Global Scientific JOURNALS

GSJ: Volume 11, Issue 4, April 2023, Online: ISSN 2320-9186
www.globalscientificjournal.com

AN EVALUATION OF BLOCK CHAIN TECHNOLOGIES: AS A PANACEA TO FINANCIAL CRIMES IN NIGERIA

FOR THE AWARD OF DEGREE OF

DOCTOR OF PHILOSOPHY

IN THE FACULTY OF INFORMATION TECHNOLOGY

CITY UNIVERSITY OF CAMBODIA

PHNOM PENH, CAMBODIA

Submitted By

Foluso Israel Taiwo

CITYU/PGS/M025

Supervised by

Professor Francis B. Osang

ABSTRACT

The usefulness and reasons for the adoption of Blockchain Technologies in conducting modern businesses and other socio-economic engagements that affect our life are gaining momentum, along with these are the challenges pose by the Internet and the Cyberspace at large, as a result of the financial wreckages usually caused by internet fraudsters, hackers, industrial espionage and cyber-warfare which made the 'Traditional' Information System (IS) a constant 'soft' target, even with the myriads of Intrusion and Detection Systems Installed to forestall attacks or prevents attack should they occur.

This paper therefore is to explore and evaluate the promising advantages of deploying blockchain technologies to fight and curb cybercrimes with the financial sector in focus.

CHAPTER ONE

1.0 INTRODUCTION

1.1 Background of the Study

The world as we know it is gradually changing from those traditional norms and processes as our daily lives is embracing the 'new normal' order as necessitated by the rapid growth of Computer Technologies and the incidence of Internet Innovations and smart services, coupled with the impacts of social media platforms that are catching the attentions of both old and young.

The usefulness and reasons for the adoption of Blockchain Technologies in conducting modern businesses and other socio-economic engagements that affect our life are gaining momentum, along with these are the challenges pose by the Internet and the Cyberspace at large, as a result of the financial wreckages usually caused by internet fraudsters, hackers, industrial espionage and cyber-warfare which made the 'Traditional' Information System (IS) a constant 'soft' target, even with the myriads of Intrusion and Detection Systems Installed to forestall attacks or prevents attack should they occur.

With this 'new normal' cultural change and e-lifestyles comes with a great price for all to be paid – Invasion of Privacy! Yes, our personal data are no longer safe as we ought to believe or think! Daily, the Internet space is bedevilled by technical miscreants often refer to as 'hackers', 'attackers', internet fraudsters, net-thieves etc and their modes of operations is central to information thefts usually perpetrated by obtaining their victims' data in a friendly and subtle manner (i.e., social engineering) or through phishing methods, which is the most

frustrating threats we face every day as cyberspace users, i.e., by claiming to be a VIP from a partner company or firm! Once the targeted victim falls into their trap – it's all over!

Bamidele (2019), reported that the Nigerian Banking Industry lost N15.15Billion to cyber-crime and forgeries in 2018 alone! This amount was astronomically higher than the N2.37Billion recorded in the year 2017 with 539%. According to Nigeria Deposit Insurance Commission (NDIC), the rising cases of fraud in the Banking System are attributable to the surge in Internet and Technological Innovation based channels and other smart instruments that are available to bankers and customer base at large. These increase in financial crimes are becoming more sophisticated day in – day out, as advanced computing techniques such as hacking, cyber tools availability in the black markets and other I.T related products and usages are now a common thing, which warranted fraudulent transfers and withdrawals, unauthorized credits accessibilities, money laundering and obtaining money by tricks (scamming) and lots more.

Recently, there are some groups of youngsters usually in their late teens and early 20s, infamously known as 'yahoo boys' that are defrauding people online (both local victims and overseas), using different types of gimmicks and subtle ways to obtain money from their unsuspecting victims. The modus operandi is not different from most business operations, but they appear legit until the last minute when the money has been carted away. The most common way of perpetrating this heinous crime is through premium dating platforms, where the perpetrator would have to subscribe for membership and looking for Information about those on the dating platforms such as suppliers of goods and services across the globe. This process always begins as follows:

1. The perpetrator will send an email (as a supplier) to a Company who is interested in that particular type(s) of product(s), having first learned about his victim's activities from the dating platform.

2. The mail server would have been hacked into for further manipulations such as attaching an invoice, catalogue, and other details as deemed fit for a legit business process.
3. The perpetrator would slightly alter the names of the supplier such that the Authorizing personnel of the paying company wouldn't noticed this difference.
4. Once payment is made, the money will be laundered by other co-perpetrators across the globe and corrupt banking personnel.
5. The Money may pass through other several connected accounts, including the accounts of individuals, thinking that they are conducting regular and genuine transactions.
6. And the eventual cashout! Pay day for these perpetrators (G-Boys or Yahoo Boys) and the spending spree will commence.

The socio-economic impact of failed monetary and fiscal

The narratives above are not too different from other types of cases reported, but the similarities point to the fact that the gullibility of the victims can be checked using Blockchain Technology**.**

The recent boom in the Cryptocurrencies adoptions on some Major Business Platforms is another concern of huge varying degree as a tool in the hands of people with fraudulent tendencies in the stock exchange market. The singular fact the Cryptocurrencies are not under the control of a Central Banking Authority makes it vulnerable to be manipulated by fraudsters or groups of organized crime associations to defraud unsuspecting investors in the Cryptocurrency market space.

In the Public Sector, the level of corruption amongst civil servants and elected or appointed political leaders are second to none – it's endemic! Contract sums are usually bloated by an average of 400% to 500% to their original costs, these

wouldn't have been possible if there is no collaboration between the civil servants and their political counterpart, who will in turn awarded the contracts to their cronies and appendages for kickbacks and returns. These proceeds are often laundered into multiple local bank accounts or starched away in foreign bank accounts or invested into real estate assets. The procurement process is flawed right from the tender and bidding exercise, which is supervised by the civil servants, who are also looking to political leaders for one favour or the other. The loopholes in the Procurement Acts are always exploited by these corrupt public servants. The EFCC and her sister Agency ICPC has been Investigating series of financial crimes, and corrupt practices perpetrated by the civil servants and political office holders, the aggregated figures are into Trillions of naira. And in most cases, these financial crimes cases linger in the Courts as perpetrators and cohorts in crime will always attempt to obstruct the course of justice and fair trials, and most cases are dismissed on the mere account of technicality.

The **Bureau of Public Procurement** (BPP) has disclosed that it saved N26.86 billion for the Federal Government in 2018, through a downward review of inflated contracts by the ministries and agencies of government.

According to the Bureau's annual report, the total amount saved stemmed from the review of contracts awarded to contractors by various Ministries, Departments and Agencies (MDAs) and the Central Bank of Nigeria before being given a certificate of "No Objection'' by the bureau.

The report shows that out of the inflated amount saved, the highest amount of N22.22 billion was recorded from the **Ministry of Power, Works and Housing**. The money was saved from an initial request of N877.40 billion.

The report also reads: *"Contracts earlier approved under the* ***Ministry of Petroleum Resources*** *was reduced from N278.91 billion to N278.64 billion, resulting in savings of about N271 million.*

*"N1.37 billion was saved on projects from the **Ministry of Transportation** from an initial request of N76.22 billion and from the **Ministry of Water Resources**, N521 million was saved out of N13.12 billion.*

"Also, from the Ministry of Finance, N143.72 million was saved from a request of N3.54 billion, while N33.65 million was saved from the Central Bank of Nigeria's (CBN) initial request of N1.47 billion."

It was further disclosed that the sum N494.96 million was saved from various military contracts from an initial request totalling N123.82 billion for the procurement of critical equipment.

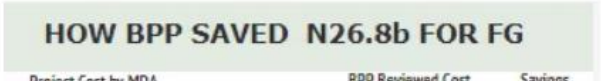
In addition, savings of about N8.04 million was made from various contracts under the supervision of the Ministry of Interior, from an initial request of N9.23 billion.

Lastly, the procurement bureau also claimed to have saved N104 million out of an initial request of N936.75 million by Federal Radio Corporation of Nigeria for the procurement of broadcast equipment for 2019 general elections.

According to the report, the public procurement activities in most MDAs are shrouded in secrecy and not in line with international best practices. "The degree of the reported cases being prosecuted in the courts by the EFCC and the ICPC are clear testimony of the breaches in the MDAs.

"As observed in most cases, the procurement officers collude with the contractors and service providers to breach certain provisions of the BPP Act for their selfish reasons. "These breaches range from faulty bid solicitation process, advance exposure of the bidding criteria to their preferred bidders and overlooking forged procurement statutory documents during technical and financial bid process.

"They also give out in-house prices of contracts to their preferred contractors and service providers which serve as an advantageous guide in their financial bidding, among other numerous breaches of the Act. "Procurement officers, who are



known to be colluding with the bidders to breach the Act, have not been reprimanded enough to deter them from their offences,'' the Bureau reports stated.

Fig. 1.0: Showing How BPP Save N26.8B for Federal Government of Nigeria in 2019

Worldwide, the global corruption and financial crimes index continue to rise as people, corporate organizations and sovereign states are always fashioning out more dubious means to legalize frauds. And it appears as if there's no way forward as effort by various organs of UN, TI, TAFT, Regional and Local Institutions to combat crimes are not yielding the expected results – a world with little crime rates.

Blockchain Technology (though not fully explored and deployed to its full potentials) appears to be the only 'alternative' to curbing and combating financial crimes in the world and Nigeria Public and Private Business Space today. The manual processes of conducting business will have to give way gradually to pave the way for the introduction and full-time adoption of Blockchain Technologies in our Public and Private Business Space.

Blockchain technology has been one of the major technological breakthroughs of this century. Bitcoin, the first Blockchain use case application, allows a network of users to perform transactions without requiring the trust of anyone on the network, or a third party. Everything is encrypted, and nobody can tamper with the Blockchain without everyone else noticing immediately. These features of immutability, amongst many other major features of Blockchain can be used to combat financial crimes and improve service delivery to the populace at large.

1.2 Statement of the Problem

The recent calls for control or total discontinuance in the use and adoption of cryptocurrencies as an alternate, genuine and valid legal tender, which are primarily powered by the Blockchain Networks by some advanced and developing economies like Nigeria have bring to the fore the concerns to evaluate blockchain technologies and to also reach a conclusion whether to reform its entirety within the ambits of the law (i.e. controlled by a Regulator) or to legislate the total discontinuance of its usage in the global and local market space.

Therefore, this research work is to evaluate the possibilities that Blockchain Technologies offer, as a tool or a means to curb financial crimes, which is the bane of its rejection by almost all Central Banks around the world despite the fact that other study in this field has investigated these claims, the main reason Nakamoto (2008) proposed a distributed ledger payment system with Bitcoin as an alternative currency was his disenchantment with the banking system for money creation. Porter & Rousse, (2016) asserted that DLT was not coincidental, as the new system was launched in the midst of the Global Financial Crisis, in 2009. Banks had taken highly risky bets in complex structured financial products that lost most of their value when it became clear that the collateral had been grossly overvalued. Inadequate research in Nigeria has left a void, which this study is attempting to address by asking, what is the importance of blockchain technologies in curbing financial crimes in the Nigeria public and private space?

1.3 Research Questions

The following research questions are designed and raise to investigate the possibilities and validity of blockchain technology use cases, as a tool in curbing and fighting financial crimes based on the above problems:

R1. What is the knowledge Background of Key Decision Makers in the Present Public-Private Sectors on The Blockchain Technologies that will likely aid its early adoption in curbing financial crimes?

R2. What are the levels of Infrastructure and State-of-the-Arts facilities available to run a parallel public-controlled blockchain networks if the open system networks of blockchain is not trusted?

R3. Can Blockchain Technological Promising Use Cases be Utilized to Curb Financial Crimes and its antecedents in the Current inefficient Nigeria Market Space?

1.4 Objectives of the Study

The Main objective of this study is to explore and evaluate the extent at which blockchain technologies can be used to curb financial crimes in Nigeria while the specific objectives are to:

1. examine the effects of the adoption on blockchain on timeliness and convenience in which business will be conducted in Financial and Non-Financial sectors in Nigeria.
2. ascertain the effect of blockchain adoption will have on quick detection that a financial crime has been committed in the Nigeria Public-Private Space.

3. investigate the effect of blockchain adoption, delay or total rejection of its usage will impact on the value-add as a new normal way of securing financial assets of all sorts.

4. will conclude with an assessment of the scope and likelihood of monetary reform as a consequence of DLT applications by central banks.

1.5 Hypothesis of the Study

To achieve the above objectives, the following hypotheses stated in null form were tested:

H_{01}: There is no significant relationship between blockchain technology and ease of conducting business in the Nigeria Public-Private Space.

H_{o2}: There is no significant relationship between blockchain technology and quick financial crimes detection and prevention in the Nigeria Public-Private Space.

Ho_3: There is no significant relationship between blockchain adoption, delay or total rejection and the value-add as a new normal way of securing financial assets of all sorts.

1.6 Significance of the Study

The study's significance is that it will serve as a framework for policy maker, management, society, students and other researchers in related subjects who may perform or embark on similar investigations on this topic in the future. Investors, shareholders, policymakers, regulatory agencies, and academics around the world will benefit from the conclusions of this study. This research will add to the body of knowledge on blockchain technology adoption and the validity of its used cases. Furthermore, because of the empirical nature of this study, researchers will be able to identify topics for future research that will assist

to explain the relationship between blockchain technologies and the fear factor surrounding one of its prominent used cases – cryptocurrency.

1.7 Scope of the Study

This study is centred on the validity claims of blockchain technologies as a panacea to financial crimes in the Nigeria Public-Private Space on the Whole. The study will also look into the effect of one of the early used cases of blockchain in the area of cryptocurrency, which has created a negative impact on the usefulness of blockchain as a whole. It's worth noting that the blockchain literature covers a wide range of creative and strategic sub-topics that explained the concept in-depth. Data will be gathered from some financial institutions operational and management staff, senior civil servants in the procurements and finance departments with a questionnaire.

1.8 Definition of Terms

Distributed Ledger Technology

Distributed Ledger Technology (DLT) refers to the technological infrastructure and protocols that allows simultaneous access, validation, and record updating in an immutable manner across a network that's spread across multiple entities or locations. DLT, more commonly known as the blockchain technology, was introduced by Bitcoin and is now a buzzword in the technology world, given its potential across industries and sectors. In simple words, the DLT is all about the idea of a "decentralized" network against the conventional "centralized" mechanism, and it is deemed to have far-reaching implications on sectors and entities that have long relied upon a trusted third-party.

Monetary Reform

Monetary reform is any movement or theory that proposes a system of supplying money and financing the economy that is different from the current system. As used in this research work, it is the liberalization of the current system and the need to introduce Crypto-Currency into the equitable redistribution of wealth.

Money

Money is an economic unit that functions as a generally recognized medium of exchange for transactional purposes in an economy. Money provides the service of reducing transaction cost, namely the double coincidence of wants. Money originates in the form of a commodity, having a physical property to be adopted by market participants as a medium of exchange. Money can be: market-determined, officially issued legal tender or fiat moneys, money substitutes and fiduciary media, and electronic cryptocurrencies.

Banking

Banking is defined as **the business activity of accepting and safeguarding money owned by other individuals and entities**, and then lending out this money in order to conduct economic activities such as making profit or simply covering operating expenses.

Bitcoin

Bitcoin is a decentralized digital currency created in January 2009. It follows the ideas set out in a white paper by the mysterious and pseudonymous Satoshi Nakamoto. The identity of the person or persons who created the technology is still a mystery. Bitcoin offers the promise of lower transaction fees than traditional online payment mechanisms do, and unlike government-issued currencies, it is operated by a decentralized authority.

Cryptocurrency

A cryptocurrency is a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. Many cryptocurrencies are decentralized networks based on blockchain technology—a

distributed ledger enforced by a disparate network of computers. A defining feature of cryptocurrencies is that they are generally not issued by any central authority, rendering them theoretically immune to government interference or manipulation.

Fiat Money

Fiat money is **a government-issued currency that is not backed by a commodity such as gold**. Fiat money gives central banks greater control over the economy because they can control how much money is printed. Most modern paper currencies, such as the Naira, Pound Sterling U.S. dollar, etc are fiat currencies.

Centralized System

Centralized systems are systems that use client/server architecture where one or more client nodes are directly connected to a central server. This is the most commonly used type of system in many organizations where a client sends a request to a company server and receives the response. The central owner stores data, which other users can access, and also user information. This user information may include user profiles, user-generated content, and more. A centralized system is easy to set up and can be developed quickly. But this system has an important limitation. If the server crashes, the system no longer works properly and users cannot access the data. Because a centralized system needs a central owner to connect all the other users and devices, the availability of the network depends on this owner. Add to that the obvious security concerns that arise when one owner stores (and can access) user data, and it's easy to understand why centralized systems are no longer the first choice for many organizations.

Decentralized System

Decentralized systems don't have one central owner. Instead, they use multiple central owners, each of which usually stores a copy of the resources users can

access. A decentralized system can be just as vulnerable to crashes as a centralized one. However, it is by design more tolerant to faults. That's because when one or more central owners or servers fail, the others can continue to provide data access to users. Resources remain active if at least one of the central servers continue to operate. Usually, this means that system owners can repair faulty servers and address any other problems while the system itself continues to run as usual.

Distributed System

A distributed system is similar to a decentralized one in that it doesn't have a single central owner. But going a step further, it eliminates centralization. In a distributed system, users have equal access to data, though user privileges can be enabled when needed. The best example of a vast, distributed system is the internet itself. The distributed system enables users to share ownership of the data. Hardware and software resources are also allocated between users, which in some cases may improve the performance of the system. A distributed system is safe from the independent failure of components, which can improve its uptime considerably. Distributed systems have evolved as a result of the limitations of the other systems. With increasing security, data storage, and privacy concerns, and the constant need for improving performance, distributed systems are the natural choice for many organizations.

It's no surprise then, that technologies using the distributed system – most notably the blockchain – are changing many industries.

SHA-Algorithm

In cryptography, **SHA** (**Secure Hash Algorithm**) is a cryptographic hash function which takes an input and produces a hash value known as a message digest – typically rendered as a hexadecimal number, 40 digits long. It was designed by the United States National Security Agency, and is a U.S. Federal Information Processing Standard. SHA-1 is no longer in use to some extent and

we have SHA-2 and SHA-3 now, as the Industry Standard for Cryptographic Functions.

Message Digest

Is a cryptographic hash function in a mathematical algorithm that maps data of an arbitrary size to a bit array of a fixed size. It is a one-way function, that is, a function for which it is practically infeasible to invert or reverse the computation. A message digest can be encrypted, forming a digital signature.

CHAPTER TWO

2.0 LITERATURE REVIEW

2.1 Introduction

This chapter will systematically review the two broad concept behind this research work (i.e., Blockchain and Financial Crimes), historical development of these concept, trends and future relevance. And the relevant works by some authors on the subject matters will be reviewed and their outcome will be briefly stated.

2.2 Conceptual Definition: What is Blockchain?

Blockchain is a system of recording information in a way that makes if difficult or impossible to change, hack or cheat the system. A Blockchain is essentially a digital ledger of transactions that is 'duplicated' and 'distributed' across the entire network of computer systems on the blockchain.

According to Treiblmaier (2018), blockchain is defined as a "*digital, decentralized, and distributed ledger in which transactions are logged and added in chronological order with the goal of creating permanent and tamper-proof records."* A specific blockchain represents a configuration of multiple technologies, tools, and methods that address a particular problem or business use case (Keogh et al., 2020a; Keogh et al., 2020b; Rejeb, 2018b; Rejeb et al., 2019a; Rejeb et al., 2018). Decentralized ledger-based currencies and systems are commonly used as payment instruments to purchase goods and services, exchanged and traded in marketplaces either for fiat currencies or other cryptocurrencies (Drašković, 2018).

The concept of blockchain was a socio-economic response to the corrupt banking systems that led to the global financial meltdown of major world economies in 2008. The main reason for proposing a distributed ledger payment system with Bitcoin as an alternative currency is the disenchantment of Nakamoto (2008) with the banking system for money creation (Porter& Rousse, 2016). Not coincidentally, the new system was launched in the midst of the Global Financial Crisis, in 2009. Banks had taken highly risky bets in complex structured financial products that lost most of their value when it became clear that the collateral had been grossly overvalued. The ensuing crisis of confidence that unfolded after 2009 in the financial system and credit rationing in turn led to negative effects, which were more severe than in previous banking crises Claessens, Ayhan Kose, & Terrones, (2010) such as substantial decreases in real GDP, Barro & Lee, (2003); Demirguc-Kunt, Detragiache, & Gupta, (2006); Hanna & Huang, (2002), corporate profits, Boyd, Gomis-Porqueras, Kwak, & Smith, (2014), and welfare losses. Aziz, Caramazza, & Salgado, (2000); Bordo, Eichengreen, Klingebiel, & Soledad Martinez-Peria, (2001); Boyd, Gomis-Porqueras, Kwak & Smith, (2005); Cecchetti, Kholer, &Upper, (2009); Hoggarth, Reis, & Saporta, (2002) all backed these claims that banking institutions and the regulators failed abysmally to 'protect' deposits in their care and failed to give returns to the depositors (owners of the funds). In addition, the massive use of public funds to bail out failed financial institutions and the close entanglement between the banks and the political system attracted attention not only of the press but also of academia Biondi, (2016); Blau, Brough, & Thomas, (2013); Reinke, (2016). The incidence and intensity of banking crises also led to the re-examination of the way money was created by the banking system. The focus of contention was the monopoly to create money granted by the state to commercial banks with a profit motive (Werner, 2014; Biondi, 2018). Critics like Porter & Rousse, 2016, have argued that banks could not be trusted with the governance of the monetary system which provided the infrastructure that was critical to the functioning of

our society at large. In proposing the alternative distributed ledger driven currency, Nakamoto (2008) argues: “Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.” Nakamoto (2008) designed the payment and money creation system of Bitcoin that “Blocks” on the blockchain are made up of digital pieces of information. Specifically, these blocks have three parts:

1. Blocks store information about transactions like the date, time, and naira amount of your most recent purchase from a store or online e.g. jumia.com (NOTE: This Jumia example is for illustrative purchases; Jumia retail does not work on a blockchain principle as of this writing this Thesis)
2. Blocks store information about who is participating in transactions. A block for your splurge purchase from Jumia would record your name along with Jumia.com, Inc. Instead of using your actual name, your purchase is recorded without any identifying information using a unique “digital signature,” sort of like a username.
3. Blocks store information that distinguishes them from other blocks. Much like you and I have names to distinguish us from one another, each block stores a unique code called a **“hash”** that allows us to tell it apart from every other block. Hashes are cryptographic codes created by special algorithms. Let’s say you made your splurge purchase on Jumia, but while it’s in transit, you decide you just can’t resist and need a second one. Even though the details of your new transaction would look nearly identical to your earlier purchase, we can still tell the blocks apart because of their unique codes.

While the block in the example above is being used to store a single purchase from Jumia, the reality is a little different. A single block on the Bitcoin blockchain can actually store around 1 MB of data. Depending on the size of the

transactions, that means a single block can house a few thousand transactions under one roof and there's no limited size to how much a block can be in reality.

Nakamoto (2008) actually designed the payment and money creation system of Bitcoin that would block abuse by authorities by deliberately debasing the currency to reduce the cost of servicing public debts Aizenman & Marion, (2011).

In the Bitcoin infrastructure designed by Nakamoto (2008), trusted institutions such as banks are replaced by cryptographic techniques and an incentive system ensures that the majority of participants (nodes) behave honestly. That makes Bitcoin a peer-to-peer financial cooperative that creates and transfers currency without a central authority verification.

In the system, Bitcoins are entries in a distributed ledger called a blockchain with specific properties programmed to minimize the probability of fraud such as double-spending or outright theft. One layer of security is the hashing of all information on the blockchain. It uses the SHA-256 algorithm which is a mathematical process that takes input data of any size, performs an operation on it, and returns output data of a fixed size. This fixed string of numbers and letters, which is called the hash, is a unique representation of the input data and changes if any component of the input data is changed. This makes tampering easy to detect digitally.

Another layer of security is that each participant in the blockchain is assigned a public cryptographic key (known to all participants) and a private cryptographic key (known to only a specific participant). If an owner wants to transfer Bitcoin, he writes a check by digitally signing the hash of the previous transaction and the public key of the next owner (the payee) and adding these at the end of the coins being transferred. The check clears when the payee signs with his private key which fits the public key that was sent by the previous owner who wrote the

check. The problem is that the payee cannot verify that the owner has not already spent the Bitcoin by signing earlier transactions. The way the Bitcoin blockchain solves this, is by publicly announcing (i.e., broadcasting) all timestamped proposed transactions to all participants and by installing a system for participants to agree on a single history of the order in which transactions were received. The payee needs proof that the majority of the nodes agree that the proposed transaction was the first broadcasted.

The steps to achieve this are as follows. After new proposed transactions are broadcasted, nodes collect a number of these transactions into a block. Each node works to solve a difficult mathematical puzzle which is specific to their block. This is the proof-of-work required by the blockchain system in order to be able to propose to other nodes to add this new block to the existing chain of blocks that had been approved earlier. If the majority of the nodes accept the proposed block because they do not detect any fraud (i.e. reach consensus on the validity of all transactions that constitute it) it is added to the existing longest blockchain and they start working on the next block, using the hash of the accepted block as the previous hash.

A key element that ensures data integrity of the blockchain is the time sensitivity of the incentives for performing the proof-of-work. As only the node whose block is accepted first by the majority of other nodes obtains a reward in the form of newly issued Bitcoins, all other nodes – after checking the correctness of the proof-of-work performed and presented to them – accept that block in order to start the proof-of work for the next block hoping to be the first to get their block accepted in the next round. The blockchain system is programmed to maintain the time it takes to perform the proof-of-work to approximately 10 min. The reason for this is that – as long as the expected reward outweighs the cost of performing the proof-of-work – nodes will invest in obtaining the fastest equipment (CPU power) in order to win the race. By maintaining a constant level

of difficulty of the proof-of-work with respect to CPU power, the blockchain is protected from nodes that attempt to tamper with the blockchain by generating an alternate chain faster than the honest chain as it would take an unrealistic amount of computing power to successfully achieve this. Nakamoto (2008, p. 4): "The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth."

The promise of Bitcoin is manifold: censorship-free (no institution which is part of the system could debase the currency or block payments), no bank run risk (avoids deposit guarantee schemes, bank regulation and too-big-to-fail cost), greater security (more difficult to hack than centralized payment system which saves cost of maintain security apparatus and compensating fraud victims), borderless (no cross-border restriction), fast (especially for cross-border payments) and cheap (infrastructure light without banks, payment terminals connected to a dedicated servers and network). Correspondingly, since the launch of Bitcoin in 2009, the total amount of money invested in the cryptocurrency has grown to almost USD 2.29 Trillion (https://coinmarketcap.com/ accessed October 7, 2021).

2.1.1 CLASSIFICATION OF BLOCKCHAINS

Based on their mode of operation and characteristics, blockchains are classified as public, private and consortium (hybrid) blockchains.

Features	Public	Private	Consortium
Participation	Without permission	By permission	
Centralisation	None	Partial	
Member	Anyone	By invitation	Membership with partial access
Ledger	Open	Selective openness	
Security	Weak	Controlled by administrator	
Consensus	Proof of work	Proof of work	
Legal ownership	None	Owner	Selected nodes
Tampering	None	Members can collaborate to alter ledger	None
Computation	High	Medium	Medium
Network dimension	Large	Small	Medium
Examples	Bitcoin, Litecoin, Ethereum	Corda, Hyperledger Fabric, Quorum	Ripple, IBM Food Trust

Table 1. Show Classification of Blockchains

2.1.2 How Blockchain Works

Blockchain is one of the emerging technologies generating more headlines in the last years. In brief, this technology can be defined as a linked chain of data blocks that allows the creation of transaction records (financial, contractual, etc.) based on a distributed consensus protocol managed by the participants (i.e., the nodes of the network) lacking a central authority. By construction, the chain of records becomes immutable; that is, no single node can modify the content of the blocks that have been previously agreed. In other words, only insertions or aggregations of new transactions are allowed, as it is not possible to eliminate or modify existing ones. The immutability property is complemented with additional characteristics. Firstly, it must be possible to obtain a summary of the status of the entire chain at any given time, so that, if any block of the chain were manipulated, it must be possible to detect such manipulation. Secondly, it would

be desirable to have access to a simple way for verifying whether a transaction has been incorporated to the blockchain or not. Finally, the parties involved in a transaction to be included in any of the blocks should be allowed to do so in a pseudo-anonymous manner, Victor Gayoso Martinez, Luis Hernandez-Alvarez and Luis Hernandez Encinas (2020).

When a block stores new data it is added to the blockchain. Blockchain, as its name suggests, consists of multiple blocks strung together. In order for a block to be added to the blockchain, however, four things must happen:

1. A transaction must occur. Let's continue with the example of your impulsive Jumia purchase. After hastily clicking through multiple checkout prompt, you go against your better judgment and make a purchase. As we discussed above, in many cases a block will group together potentially thousands of transactions, so your Jumia purchase will be packaged in the block along with other users' transaction information as well.
2. That transaction must be verified. After making that purchase, your transaction must be verified. With other public records of information, like the Securities Exchange Commission, Wikipedia, or your local library, there's someone in charge of vetting new data entries. With blockchain, however, that job is left up to a network of computers. When you make your purchase from Jumia, that network of computers rushes to check that your transaction happened in the way you said it did. That is, they confirm the details of the purchase, including the transaction's time, naira amount, and participants. All these transactional data flow will happen in a second, If not less than!
3. That transaction must be stored in a block. After your transaction has been verified as accurate, it gets the green light. The transaction's naira amount, your digital signature, and Jumia's digital signature are all stored in a

block. There, the transaction will likely join hundreds, or thousands, of others like it.

4. That block must be and will be given a **hash**. Not that very simple though, but through an Algorithm and Cryptographic means, once all of a block's transactions have been verified, it must be given a unique, identifying code called a hash. The block is also given the hash of the most recent block added to the blockchain. Once hashed, the block can be added to the **blockchain**.

When that new block is added to the blockchain, it becomes publicly available for anyone to view—**even for the hackers to see**. If you take a look at Bitcoin's blockchain for an instance, you will see that you have access to transaction data, along with information about when ("Time"), where ("Height"), and by who ("Relayed By") the block was added to the blockchain.

2.1.3 Ownership Issue of Blockchain and Privacy

Anyone can view the contents of the blockchain, but users can also opt to connect their computers to the blockchain network as nodes. In doing so, their computer receives a copy of the blockchain that is updated automatically whenever a new block is added, like a Facebook News Feed sort of, that gives a live update whenever a new status is posted.

Each computer (usually a server) in the blockchain network has its own copy of the blockchain, which means that there are thousands, or in the case of Bitcoin, millions of copies of the same blockchain. Although each copy of the blockchain is identical, spreading that information across a network of computers makes the information more difficult to manipulate. With blockchain, there isn't a single, definitive account of events that can be manipulated. Instead, a hacker would need to manipulate every copy of the blockchain on the network. This is what is meant by blockchain being a "distributed" ledger.

Looking over the Bitcoin blockchain, however, one will notice that you do not have access to identifying information about the users' making transactions. Although transactions on the blockchain are not completely anonymous, personal information about users is limited to their digital signature or username.

This raises an important question: if you cannot know who is adding blocks to the blockchain, how can you trust blockchain or the network of computers upholding it?

2.1.4 How Secured Is Blockchain Network Infrastructure?

An essential characteristic of decentralized ledgers in blockchain networks is the system participants' financial incentives in exchange for their concerted efforts to verify and record transactions on the ledger. The interest in the finance applications and other smart contract of decentralized ledgers has significantly increased because of the immutable financial transactions registered in the system, the strong governance, and the system's resiliency against security threats such as the DDoS attacks and single point of failure Tasca and Tessone, (2018).

Blockchain technology accounts for the issues of security and trust in several ways. First, new blocks are always stored linearly and chronologically. That is, they are always added to the "end" of the blockchain. If you take a look at Bitcoin's blockchain, you'll see that each block has a position on the chain, called a "height." As of October 10th 2021 the block's height had topped 360,000,200,000bytes (360.02 Gigabytes).

After a block has been added to the end of the blockchain, it is very difficult to go back and alter the contents of the block. That's because each block contains its own hash, along with the hash of the block before it. Hash codes are created

by a math function that turns digital information into a string of numbers and letters. If that information is edited in any way, the hash code changes as well.

Here's why that's important to security. Let's say a hacker attempts to edit a transaction from Jumia Platform so that the buyer actually has to pay for the purchase twice. As soon as the hacker edit the naira amount of the transaction, the block's hash will change. The next block in the chain will still contain the old hash, and the hacker would need to update that block in order to cover their tracks. However, doing so would change that block's hash. And the next, and so on, thereby making it extremely difficult to perpetrate a fraudulent act.

2.2 A Gradual Departure from the Centralized Systems

The primary difference between a blockchain and a database is **centralization**. While all records secured on a database are centralized, each participant on a blockchain has a secured copy of all records and all changes so each user can view the provenance of the data. The Traditional Database System represents the Information System (IS) of an organization. Information systems are an integral part of an organization, regardless of its size or industry. These systems typically hold and control the data that the organization needs, such as data about services, products, clients, transactions, suppliers and many more. Most, if not all, employees operate these information systems and spend many hours interacting with them at work.

Over the past few decades, these systems have been constantly upgraded. Newer systems are able to handle transactions quicker and more accurately compared to previous iterations. **Imran Khan Azeemi, et. Al.,** (2013) asserted that graphical user interfaces have become the norm and replaced clunky text terminals that lack data. Thanks to changing design approaches, developing these newer systems is done faster than ever. However, they still carry specific characteristics that haven't evolved:

- These systems contain a wealth of information about employees, customers, purchases, suppliers and many more. Many systems are able to report this data in a format that humans can understand; however, these systems are unable to adapt or improve how they behave based on this data. They can't learn from the information or events that have already happened.
- Many information systems are unable to act on their own or on the behalf of their users. They stop operations and wait until a human can instruct them on what their next action should be.
- These systems tend to be difficult to understand for non-technical staff and too rigid to change or improve. Many changes have to be coursed through the IT department, which makes improvement costly and slow.
- Most information systems don't allow comprehensive access to their daily, regular users. They usually need approval from supervisors and require them to log in and approve requests. When requiring support from outside sources, it's a common occurrence that the first point of contact is also unable to tell the system what it should do and instead asks the users to refer to a senior employee.

There are notable exceptions that perform better than these traditional information systems. In recent years, many organizations have developed Decision Management Systems to improve upon the listed limitations, creating systems that are more adaptive, analytic and agile, while the advent of Artificial Intelligence (AI) has made machine learning to be possible in business environment in the management of knowledge, the more recent blockchain technological potential used cases in business world would definitely bring about a paradigm shift to a more secure, robust and smart Information Systems.

2.3 Some Potential Blockchain Used Cases

Clearly, blockchain is emerging as a very viable technology when it comes to protecting businesses and other entities from cyber-attacks. Here are five promising use cases, moving from the labs to real life:

2.3.1. Decentralized Storage Solutions

Data is becoming a more valuable currency, than well...currency. Your business accumulates tones of sensitive data about your customers. Unfortunately, this data is also quite attractive to hackers. And one of the most convenient things you do for cyber criminals is store all of it in one place. It's a bit like storing all of your cash and jewellery in a shoe box at home, then being shocked when a burglar walks off with the entire thing.

Unfortunately, businesses are still using centralized storage when it comes to data. However, this appears to be changing slowly. Blockchain-based storage solutions are gaining popularity. For instance, The Apollo data cloud (developed by Apollo Currency team) allows users to archive data on the blockchain and grant permission for accessing to third-parties. The cryptographic access key can be revoked at any time, further reducing the risk of a breach. Thanks to the decentralized nature of blockchain technology, hackers no longer have a single point of entry, nor can they access entire repositories of data in the event that they do get in. This feature is one of the main reasons why enterprises are now considering blockchain as data privacy solution.

2.3.2 IoT Security

Hackers often gain access to systems by exploiting weaknesses in edge devices. These include routers and switches. Now, other devices such as smart thermostats, doorbells, even security cameras are also vulnerable. Simply put, the

rigorousness is often not applied when ensuring whether these IoT devices are secure.

Blockchain technology can be used to protect systems, and devices from attacks. According to Joseph Pindar, (2018) co-founder of the Trusted IoT Alliance, blockchain can give those IoT devices enough "smarts" to make security decisions without relying on a central authority. For instance, devices can form a group consensus regarding the normal occurrences within a given network, and to lockdown any nodes that behave suspiciously.

Blockchain technology can also protect all the data exchanges happening between IoT devices. It can be used to attain near real-time secure data transmissions and ensure timely communication between devices located thousands of miles apart. Additionally, blockchain security means that there is no longer a centralized authority controlling the network and verifying the data going through it. Staging an attack would be much harder (if even possible).

2.3.3. Safer DNS

DNS is largely centralized. As a result, hackers can break into the connection between website name and IP address and wreak havoc. They can cash websites, route people to scam websites, or simply make a website unavailable. They can also pair DNS attacks with DDoS attacks to render websites utterly unusable for extended periods of time. The current most effective solution to such issues is to tail log files and enable real-time alerts for suspicious activities.

A blockchain-based system can take security one step further. Because it's decentralized, it would be that much more difficult for hackers to find and exploit single points of vulnerability. Your domain information can be stored immutably on a distributed ledger, and the connection can be powered by immutable smart contracts.

Blockstack (2016) a provider of blockchain infrastructure is proposing the use of blockchain technology to decentralize the Domain Name System (DNS) and make it more secure. According to the proposal, the Bitcoin blockchain would be used to register and cryptographically protect domain names by using distributed ledger technology. DNS root servers would be replaced with a blockchain for storing information on registered domain names. This is expected to make the DNS more secure (as there would be no central points of trust or failure), to facilitate the administration of domain names by the registrants, and to make obsolete any censorship attempts (as domain names could not be seized from owners without getting access to their private keys).

2.3.4. Implementing Security in Private Messaging

As conversational commerce becomes more popular, a lot of meta data is collected from customers during these exchanges on social media.

While many messaging systems use end-to-end encryption, others are beginning to use blockchain to keep that information secure. At the moment, most messaging apps lack a standard set of security protocols and a unified API framework for enabling "cross-messenger" communications. The emerging secure blockchain communication ecosystems tackle this issue and work towards creating a new system of unified communication. Blockchain is a great solution for that as it secures all data exchanges and enables connectivity between different messaging platforms.

No matter where or how it's applied, the key factor in using blockchain as a cybersecurity method is decentralization. When access control, network traffic, and even data itself is no longer held in a single location, it becomes much more difficult for cyber criminals to exploit. This has the potential to mean more security, and less vulnerability.

2.3.5 Bank Use

Perhaps no industry stands to benefit from integrating blockchain into its business operations more than banking. Financial institutions only operate during business hours, five days a week. That means if you try to deposit a check on Friday at 6 p.m., you likely will have to wait until Monday morning to see that money hit your account. Even if you do make your deposit during business hours, the transaction can still take one to three days to verify due to the sheer volume of transactions that banks need to settle. Blockchain, on the other hand, never sleeps.

Blockchain promises to change forever the way we manage information in the digital world. It allows data and funds to be transferred in a fully secure manner thanks to sophisticated coding and encryption. Santander is a pioneer in the implementation of blockchain in its services, improving customer service and efficiency, Santander (2019).

By integrating blockchain into banks, consumers can see their transactions processed in as little as 10 minutes, basically the time it takes to add a block to the blockchain, regardless of the time or day of the week. With blockchain, banks also have the opportunity to exchange funds between institutions more quickly and securely. In the stock trading business, for example, the settlement and clearing process can take up to three days (or longer, if banks are trading internationally), meaning that the money and shares are frozen for that time.

Given the size of the sums involved, even the few days that the money is in transit can carry significant costs and risks for banks. European bank Santander and its research partners put the potential savings at $15 billion to $20 billion a year. Capgemini, a French consultancy, estimates that consumers could save up to $16

billion in banking and insurance fees each year through blockchain-based applications.

2.3.6 Healthcare Uses

Health care providers can leverage blockchain to securely store their patients' medical records. When a medical record is generated and signed, it can be written into the blockchain, which provides patients with the proof and confidence that the record cannot be changed. These personal health records could be encoded and stored on the blockchain with a private key, so that they are only accessible by certain individuals, thereby ensuring privacy

Deloitte, (2016) concluded that Blockchain technology has the potential to transform health care, placing the patient at the centre of the health care ecosystem and increasing the security, privacy, and interoperability of health data. This technology could provide a new model for health information exchanges (HIE) by making electronic medical records more efficient, disintermediated, and secure. While it is not a panacea, this new, rapidly evolving field provides fertile ground for experimentation, investment, and proof-of-concept testing.

Blockchain technology presents numerous opportunities for health care; however, it is not fully mature today nor a panacea that can be immediately applied. Several technical, organizational, and behavioural economics challenges must be addressed before a health care blockchain can be adopted by organizations nationwide.

2.3.7 Use in Smart Contracts

A smart contract is a computer code that can be built into the blockchain to facilitate, verify, or negotiate a contract agreement. Smart contracts operate under

a set of conditions that users agree to. When those conditions are met, the terms of the agreement are automatically carried out.

Say, for example, I'm renting you my apartment using a smart contract. I agree to give you the door code to the apartment as soon as you pay me your security deposit. Both of us would send our portion of the deal to the smart contract, which would hold onto and automatically exchange my door code for your security deposit on the date of the rental. If I don't supply the door code by the rental date, the smart contract refunds your security deposit. This eliminates the fees that typically accompany using a notary or third-party mediator.

2.3.8 Bitcoin Used Case in Blockchain Network

Bitcoin is the 1st successful used case of the Blockchain Network. Satoshi Nakamoto (2008) created the framework for bitcoin using the blockchain network infrastructure in his design. He intended that the crypto-currency should be the first successful peer-to-peer payment platform.

According to the Bitcoin Foundation, the word "Bitcoin" is capitalized when it refers to the cryptocurrency as an entity, and it is given as "bitcoin" when it refers to a quantity of the currency or the units themselves. Bitcoin is also abbreviated as BTC.

Bitcoin as a form of digital currency, is also known as a type of cryptocurrency because it uses cryptography to keep it secure. There are no physical bitcoins, only balances kept on a public ledger that everyone has transparent access to (although each record is encrypted). All Bitcoin transactions are verified by a massive amount of computing power via a process known as "mining." Bitcoin is not issued or backed by any banks or governments, nor is an individual bitcoin valuable as a commodity. Despite it not being legal tender in most parts of the world, Bitcoin is very popular and has triggered the launch of hundreds of other cryptocurrencies, collectively referred to as altcoins. Bitcoin offers the promise

of lower transaction fees than traditional online payment mechanisms do, and unlike government-issued currencies, it is operated by a decentralized authority.

2.3.9 Flaws Possibilities in Bitcoins

Just like all other systems are not always free from flaws or a possibility that they can be prone to known and unknown errors, the Bitcoin concepts as developed by Nakamoto (2008) seems a perfect ideal for our possible financial woes however, the Bitcoin has a number of flaws that have prevented it from becoming widely used money. These shortcomings originate from the egalitarian and unstructured character of the Bitcoin's blockchain. Nakamoto (2008, p. 8): "The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and re-join the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism." This makes the Bitcoin type of blockchain permissionless: individuals do not need permission to perform proof-of-work to verify the addition of new data.

These established shortcomings will be categorized with respect to the three primary functions of money: it is a unit of account, a store of value, and a medium of exchange. Nakamoto (2008, p. 6) designed the Bitcoin system so that participants stay anonymous: "The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking

the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape," is made public, but without telling who the parties were. As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner." There is no need to reveal one's legal identity to own and transfer Bitcoins. Only a set of private and public keys is needed. And even the publicly known keys are not traceable to legal identity provided the user does not register at an exchange and leaves no traces on the Internet. The anonymity that the Bitcoin system offers has invited illicit transactions to be paid in the cryptocurrency. Bohr and Bashir (2014, p. 97) document that over a third of the Bitcoin holders used the currency to purchase illicit goods such as narcotics and gambling services. In addition, they report that: "Several other variables were statistically significant in predicting the accumulation of Bitcoins. Controlling for other factors, the marginal effect of spending Bitcoins on illicit goods (narcotics, gambling services, or other illegal goods) predicted that those users had about 25–45% more Bitcoins (within the 95% confidence interval) than those who had not spent Bitcoins on illicit goods."

In any case, we must not forget that the non-traceability of a cryptocurrency is a problem when examined under the lens of the laws against money laundering. In the real world, the exchange of money in electronic transfers takes place between the owners of bank accounts, which are completely identified by financial institutions. Contrary to this model, in payments with cryptocurrencies, the transfer of value flows from a pseudo-anonymous identity to another pseudo-anonymous identity. Bitcoin proposes a protocol that allows monetary transactions between users using fiat money based on a limited resource. In the case of bitcoin, the limited resource is the resolution of a computationally difficult mathematical problem. In other words, with bitcoin technology, cryptocurrencies are minted by software computing a hard-to-solve problem, which has a high energy expenditure associated. Indeed, the protocol associated to bitcoin works

through a Peer-to-Peer (P2P) network, so that all nodes can access a copy of the bitcoin blockchain, but only certain users can write on it, Victor Gayoso Martinez, Luis Hernandez-Alvarez and Luis Hernandez Encinas (2020).

As the challenges enumerated above are becoming a common norm within our society, technology managers must equally upscale their operational skills and expertise in handling people's fund and other financial instruments across the globe within and outside the cyberspace. In keeping up with the ever fast and dynamic business environment with the myriads of evolving technological solutions, coupled with the birth of the Fourth Industrial Revolution, exploring the blockchain digital solutions and platform is now more than necessary for any business who wants to stay afloat and maintain its competitive edge!

Unfortunately, businesses are still using centralized storage when it comes to data. However, this appears to be changing slowly. Blockchain-based storage solutions are gaining popularity. For instance, The Apollo data cloud (developed by Apollo Currency team) allows users to archive data on the blockchain and grant permission for accessing to third-parties. The cryptographic access key can be revoked at any time, further reducing the risk of a breach. Thanks to the decentralized nature of blockchain technology, hackers no longer have a single point of entry, nor can they access entire repositories of data in the event that they do get in. This feature is one of the main reasons why enterprises are now considering blockchain as data privacy solution.

2.4 A Distributed Ledger Technology for Secured Financial Services: R3 Corda

Financial institutions have traditionally been early adopters and intensive users of information and communication technology (ICT) in order to maximize the efficiency of their main activity: verifying, recording and transferring digital information.

The benefits of implementing DLT are most pronounced for network activities that are complex, protracted and include verification of information supplied by different parties that do not necessarily trust each other such as clearing and settlement of trades in financial instruments9 (Probst, Frideres, Cambier, & Martinez-Diaz, 2016; World Economic Forum, 2016). The resulting disintermediation as well as increased transparency led to significant cost reductions, especially in regard to transaction or monitoring costs (Pinna & Ruttenberg, 2016).

In the years after the launch of Bitcoin and before the publication of the seminal study by the World Economic Forum (2016), a significant volume of venture capital was invested in projects aiming to find business applications for blockchain. One of these investors was David Rutter, who started R3CEV in early 2013 with Jesse Edwards and Todd McDonald where the R represented Rutter's name, the three represented the three partners and CEV stood for crypto, exchanges, and ventures. Rutter had established a reputation as a creative thought leader in the implementation of innovative solutions to financial markets. After over 30 years of experience gained at various financial institution, including 10 years as CEO of ICAP, he decided to dedicate his time fully to developing an application of the emerging blockchain technology. Rutter and his two R3CEV partners met with more than 20 blockchain companies, mostly based in Silicon Valley, California but could not find companies

that they considered a good investment. They were disappointed with the lack of understanding of how financial institutions actually worked and the bravado of the persons looking for funding of their ideas. Despite the fact that the aspiring entrepreneurs were not able to explain how they would actually disrupt incumbents such as J.P. Morgan or the Depository Trust & Clearing Corporation, many were able to raise millions of venture capital. As these investments did not generate the promised disruption (Fico, 2016; Peters & Panayi, 2016), this led to doubt as to whether the potential of DLT was grossly overestimated and the

situation had evolved into a tech hype comparable to the dot-com bubble that burst in 2000 (Evans-Greenwood, Hillard, Harper, & Williams, 2016; Valenzuela, 2016). Rutter had built up some experience with the actual implementation of blockchain as a seed investor in Align Commerce (later renamed Veem) the first global payments company that used blockchain, and the distributed ledger company Digital Asset Holdings. During the latter half of his career his focus had been tedious process of clearing, settlement and record keeping of traded financial instruments could lower costs significantly. A key insight was that institutions had a common problem and that they were per definition their mirror image as (the agent for) the purchaser and the seller of a financial instrument.

Based on this insight, he decided that the best way to develop a solution was to invite the parties involved to participate in a series of roundtable meetings in order to reach agreement on the best IT architecture for a collective problem. His track record for actually solving IT problems and saving time and money for banks, helped convincing these banks to spend time on a technology that many did not understand and many suspected it to be a hype with limited practical use, if any. Rutter on the goal of the three roundtable sessions held in 2014 and 2015: "We held several roundtables […] to deeply consider what the possible implications of the blockchain were, and what it could possibly do to save money, and time, and to create a better paradigm for the world of Wall Street and finance."

The outcome of the roundtables was a joint venture with nine global banks: Barclays, BBVA, Commonwealth Bank of Australia, Credit Suisse, Goldman Sachs, J.P. Morgan, State Street, Royal Bank of Scotland, and UBS. The banks committed

both capital and assigned their in-house experts to working groups of the joint venture. The membership of the collaborative network grew to 42 banks by December 2015. In an interview with the Wall Street Journal, Rutter explained the three project phases and the corresponding objectives of the consortium. The

objective of the first phase was to design the different ledger architectures which could handle the billions of dollars of diverse and complex transactions of financial instruments that the banks traded amongst each other, similar to the settlements made in a payment system such as DLT-driven Bitcoin system. The second goal was to experiment with different ledger designs in order to determine their potential and limitations. The third goal was to learn from the experiments what worked best and had a high probability of adoption amongst most banks.

In the first phase, three type of ledgers were identified: the centralized, decentralized, and the distributed ledger. A ledger is a record of asset ownership. Before the digital age, a ledger typically would be a book where the bookkeeper would make entries whenever ownership of an asset changed as result of a transaction. When computers became widely available, the ledgers were changed into digital records.

A centralized ledger is a single and complete overview of ownership that is maintained by one trusted third party. In the capital markets this party is known as the central securities depositary. These institutions are organized on a national level (e.g. the US Depositary Trust Company) or internationally (e.g. Euroclear of Clearstream). The shortcoming of this arrangement is that it can be accidentally or maliciously shut down, tampered with or destroyed. It is vulnerable to a single point of failure.

A decentralized ledger is a network of sub-ledgers which – when aggregated, would make up the complete centralized ledger. An example is a retail network where the stores send the ledger containing their inventory status to their head office at the end of the business day. The head office would have a complete record of the inventory by combining the information contained in the received decentralized ledgers. This system has multiple sources of potential error or points of failure.

A distributed ledger is a complete record of ownership and transactions with multiple identical copies distributed over different locations, thereby avoiding the risk of single point of failure. There are three essential differences between a decentralized and a distributed ledger. First, in a decentralized ledger there is a master–slave relationship between the sub-ledgers and the ledger in which the information from the sub-ledgers is aggregated. Second, a distributed ledger is programmed to resolve potential conflicts in simultaneous updates of the ledger.

Third, a distributed ledger allows for the incorporation of self-enforcing contracts (a.k.a. smart contracts) to be programmed to update the ledger (Peters & Panayi, 2016). Smart contracts are lines of code which are stored on a blockchain and automatically execute when predetermined terms and conditions are met. However, the distributed ledger requires a continuous effort to ensure there are no difference between de the ledgers in different locations. Traditionally, this had been prohibitively time-consuming. With the advent of cryptography and the blockchain verification protocol, the implementation of DLT to produce a shared ledger across locations containing up-to-date secure and transparent information became feasible.

The banks that formed the R3 consortium identified a shared problem for which DLT is a likely candidate to provide a solution: clearing and settlement of financial instruments that are traded amongst themselves. The majority of these instruments are agreed to verbally by trading floor professionals working for financial institutions each of which maintained their own ledger. Subsequently the agreed trade needs to be formalised, recorded, and the settlement of obligations need to be consummated on an agreed date. In practice, frequent human errors, disagreements between counterparties that did not trust each other and reconciliation of disputes prove to be highly labour-intensive and costly

(World Economic Forum, 2016). In addition, identifying and structuring trading data for risk and compliance purposes add to the costs of securities trading. Analysis of data from the World Bank, the World Federation of Exchanges; Oxera; Financial Times and Oliver Wyman by Santander InnoVentures, in collaboration with its partners Oliver Wyman and Anthemis Group, concludes: "Our analysis suggests that distributed ledger technology could reduce banks' infrastructure costs attributable to cross-border payments, securities trading and regulatory compliance by between $15 and 20 billion per year by 2022".12 R3 member were convinced it made economic sense to pool their resources to collectively develop an encrypted distributed ledger to reap these benefits rather than each bank trying to streamline the clearing and settlement process individually.

In the second phase, experimentation was initiated with different ledger designs in order to determine their potential and limitations. Two working groups were formed from personnel of the 42 R3 consortium banks: the Lab and Research Centre (LRC) based in New York and the Architecture Working Group (AWG) in London. With the functional requirements of the banks in mind, the LRC focused on testing existing DLT and the AWG began developing DLT from scratch. In the first quarter of 2016, the LRC tested DLT solutions from five vendors: IBM Hyperledger, Intel Sawtooth, Ethereum, Eris Industries, and Chain. The financial transactions were recorded on distributed ledgers hosted on the cloud computing services of Microsoft Azure, IBM Cloud, and Amazon AWS. While the experiments showed that the existing DLT showed potential, none of them provided the complete solution that satisfied the R3 banks. Especially, the privacy and scalability requirements of the banks were not met.

The lead was taken by AWG to develop a proprietary DLT. From the work done at LRC, it was clear that a permissionless and public blockchain like Bitcoin was

not appropriate for the banks given the banks' requirement concerning, respectively,

scalability and privacy. Existing DLT did not meet the requirements either. Richard Gendal Brown, who had been recruited from IBM to lead the team at AWG was very specific in his approach to come up with a solution: "The reality is that solutions based on selecting the design first and then trying to apply it to arbitrary problems never work out well. Every successful project I've worked on started with the requirements, not some cool piece of technology, and I was determined to bring that discipline into our work at R3."13 He summarized the requirements in nontechnical terms as follows: "The financial industry is pretty much defined by the agreements that exist between its firms and these firms share a common problem: the agreement is typically recorded by both parties, in different systems and very large amounts of cost are caused by the need to fix things when these different systems end up believing different things. Multiple research firms have postulated that tens of billions of dollars are spent each year on this problem. In particular, these systems typically communicate by exchanging messages: I send an update to you and just hope you reach the same conclusion about the new state of the agreement that I did. It's why we have to spend so much money on reconciliation to check that we did indeed reach the same conclusions and more money again to deal with all the problems we uncover. Now imagine we had a system for recording and managing financial agreements that was shared across firms, that recorded the agreement consistently and identically, that was visible to the appropriate regulators and which was built on industry-standard tools, with a focus on interoperability and incremental deployment and which didn't leak confidential information to third parties. A system where one firm could look at its set of agreements with a counterpart and know for sure that: "What I see is what you see and we both know that we see the same thing and we both know that this is what has been reported to the regulator." **That's Corda**." In November 2016 Corda was made available as an open source

DLT platform that did not group transaction in blocks but instead recorded agreements (transactions) individually, speeding up process time. Scalability was also increased by using so called notary nodes that were authorized to update the permissioned ledger. The ledger was also private, where information was disclosed on a need-to-know basis. Consensus occurred only between the two counterparties to a transaction and not between all members of the network. Clearly, the private and permissioned blockchain has made serious compromises to the idealistic public and permissionless system that was conceived by Nakamoto (2008) in order to make DLT practically useful for financial institutions.

2.5 Hyper Ledger Critique

Hyperledger Fabric is an open source, permissioned blockchain framework, started in 2015 by The Linux Foundation. It is a modular, general-purpose framework that offers unique identity management and access control features, which make it suitable for a variety of industry applications such as track-and-trace of supply chains, trade finance, loyalty and rewards, as well as clearing and settlement of financial assets, AWS-AMAZON, 2021.

A Hyperledger Fabric network is comprised of unique organizations (or members) that interact with each other on the network. For example, an organization could be a bank in a network comprised of financial institutions or a shipping partner in a supply chain network. From a Fabric component perspective, each organization has a Fabric certificate authority and one or more peer nodes. A Fabric network also has an ordering service shared by all organizations in the network, and this component helps process transactions for the network. We will share more details about each of these concepts and components below:

An organization in a network is defined by a root certificate specific to that organization. Users and other components (like peer nodes – see below) in that organization are also identified by certificates, and these certificates are derived from this root certificate, ensuring other organizations in the network can relate a user to their organization. These certificates also specify the permissions for each entity on the network, like read-only versus full access on a channel.

A root certificate for an organization is stored in the Fabric certificate authority (CA). The Fabric CA also issues certificates for users in an organization and handles other related operations. An enterprise-grade Fabric CA utilizes a variety of components and can deployed in a variety of ways using a Hardware Security Module (HSM) for root certificate protection.

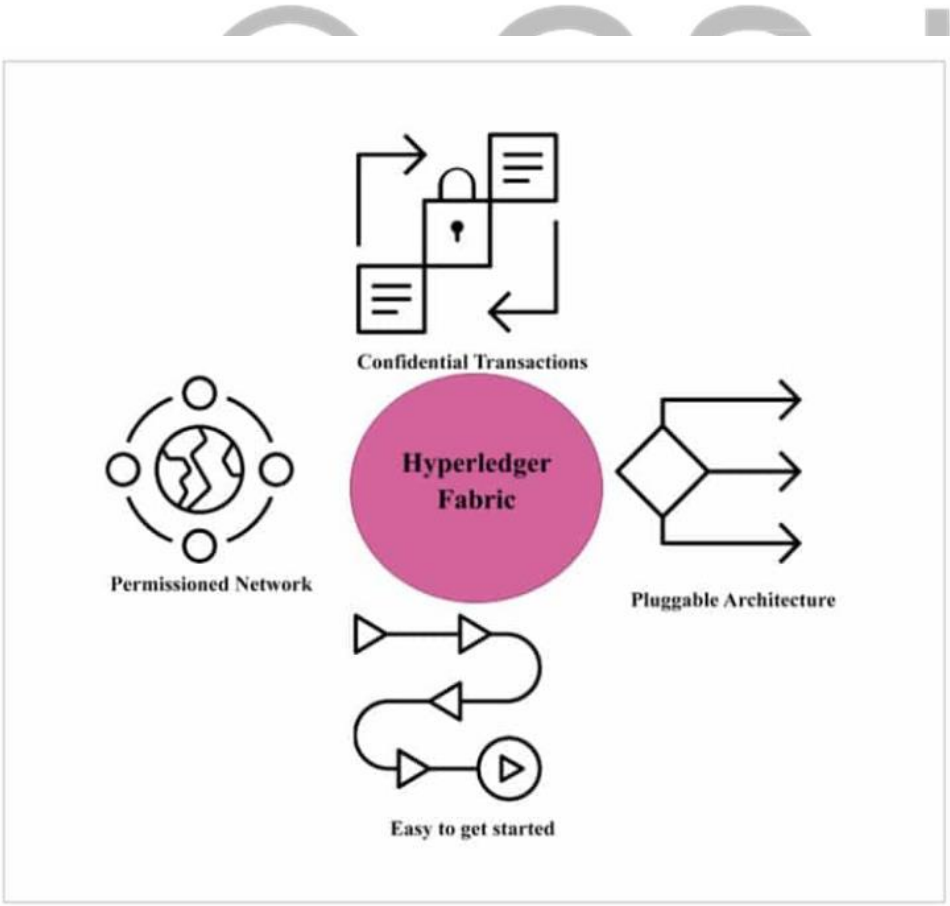


Fig. 2.0 Factors driving Hyperledger Fabric

An organization also creates one or more peer nodes as components to carry out operations on behalf of that organization. Specifically, a peer node endorses transactions proposed on the network, stores and executes smart contract code (known as chaincode in Fabric), and stores a local copy of the ledger for access. Fabric clients typically interact with peer nodes to read the ledger, add new chaincode to the network, or propose a new transaction. A peer node typically runs on its own computer, like an Amazon EC2 instance.

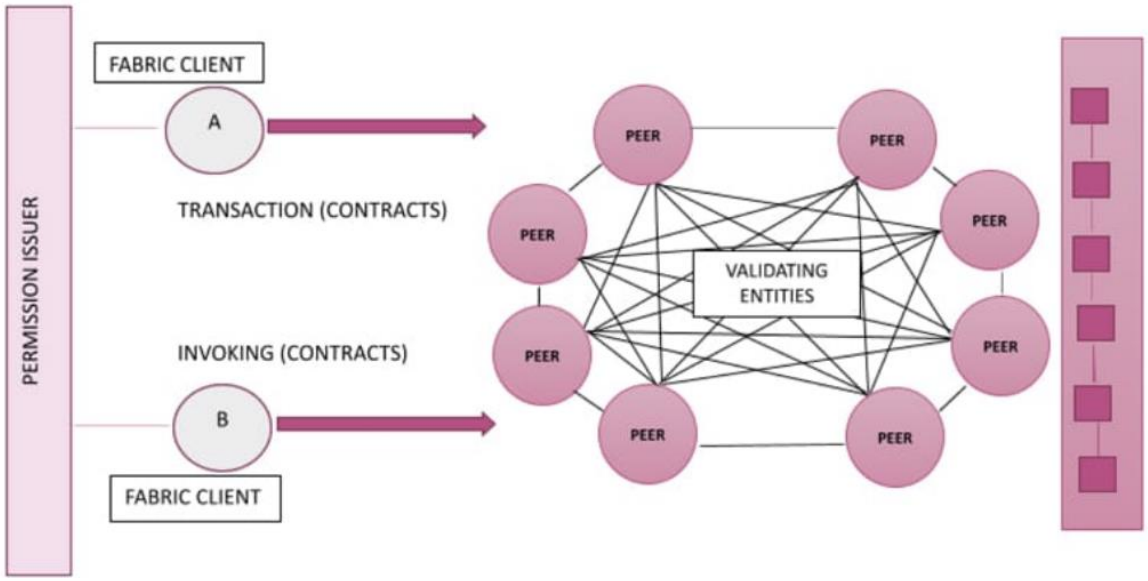


Fig. 2.1 Hyperledger Fabric Model

Finally, a Fabric network also includes of an ordering service shared by all members of the network. The ordering service makes sure new transactions on the network are properly ordered in new blocks and have the proper endorsements. The ordering service then broadcasts a new block of transactions to peer nodes in each organization. Peer nodes update their local copy of the ledger with this new block.

As per the 2020 Blockchain Global Patent Authorization report, 3924 blockchain technology patents have been filed, with the US leading at 39 per cent, Korea at 21 per cent and China at 19 per cent. Alibaba leads with 212 blockchain patents, followed by IBM’s 136.

IBM has been an initiator in so many ways – hiring the first disabled employee way back in 1914, building the IBM baseball team in 1929, hiring women systems service professionals in 1935, developing the commercial electronic multiplier in 1946, setting up its first office in India in 1951, and so on. Inspired by the success of blockchain and just a decade and a half into the 21st century, IBM has contributed to Hyperledger Fabric.

2.5.1 Industry Use Cases for Hyperledger Fabric

Supply Chain

Supply chains are global, distributed webs of suppliers, manufacturers, and retailers. Hyperledger Fabric networks can improve supply chain processes by increasing transparency and traceability of transactions within the network. On a Fabric network, companies with access to the ledger can view the same immutable data, which enforces accountability and reduces the risk for counterfeiting. In addition, production updates are added to the ledger in real time, which makes tracking provenance faster and simpler during events like product recalls or food contamination outbreaks.

Trading and Asset Transfer

Trading requires many organizations such as importers, exporters, banks, shipping companies, and customs departments, to work with one another. Using Hyperledger Fabric, financial and trading consortiums can easily create a blockchain network where all parties can transact and process trade-related paperwork electronically, without the need for a central trusted authority. Unlike other processes that require trade-related paperwork to go back and forth between the stakeholders, taking 5-10 days to complete, transactions in a Hyperledger Fabric network built using Managed Blockchain can process instantly.

Insurance

Insurance fraud costs the insurance industry billions of dollars a year, but with Hyperledger Fabric, insurance companies can reference transaction data stored on the ledger to identify duplicate or falsified claims. Blockchain can also make multi-party subrogation claims processing faster by using smart contracts to automate repayment from the at-fault party back to the insurance company. In addition, insurers can use Hyperledger Fabric to streamline Know Your Customer (KYC) processes by storing customer data on a distributed ledger and automating the verification of their identity documents with smart contracts.

2.6 Is there not a weakness in Blockchain?

There's no one nor system under the sun without an Achilles heel, blockchain weakness(s) lies right there in its colossal strengths! For the most part, the real challenges for blockchain adoption are political and regulatory, below some of the contending ones will be briefly explained:

2.6.1 Hack Susceptibility

If a hacker wanted to coordinate an attack on the blockchain, they would need to control more than 50% of all computing power on the blockchain so as to be able to overwhelm all other participants in the network. Given the tremendous size of the Bitcoin blockchain, a so-called 51% attack is almost certainly not worth the effort and more than likely impossible!

Newer cryptocurrencies and blockchain networks are susceptible to 51% attacks. These attacks are extremely difficult to execute due to the computational power required to gain majority control of a blockchain network, Joseph Bonneau, (2017) said that might change, estimating that 51% attacks were likely to

increase, as hackers can now simply rent computational power, rather than buying all of the equipment to perpetrate the actual hack of the blockchain network.

2.6.2 Central Banks Concerns

Several central banks, including the Federal Reserve, the Bank of Canada and the Bank of England, have launched investigations into digital currencies. A June 2020 paper from the Federal Reserve Bank of Philadelphia said the creation of a central bank digital currency (CBDC) would put the Federal Banks in direct competition with private banks. "Besides its potential role in eliminating physical cash, a CBDC will allow the central bank to engage in large-scale intermediation by competing with private financial institutions for deposits (and, likely, engaging in some form of lending of those deposits)," the paper said. "In other words, a CBDC amounts to giving consumers the possibility of holding a bank account with the central bank directly.

2.6.3 Illegal Activity

While confidentiality on the blockchain network protects users from hacks and preserves privacy, it also allows for illegal trading and activity on the blockchain network. The most cited example of blockchain being used for illicit transactions is probably Silk Road, an online “dark web” marketplace operating from February 2011 until October 2013 when it was shut down by the FBI.

The website allowed users to browse the website without being tracked and make illegal purchases in bitcoins. Current U.S. regulations require financial service providers to obtain information about their customers when they open an account, verify the identity of each customer, and confirm that customers do not appear on any list of known or suspected terrorist organizations. Here in Nigeria, the yahoo boys always use the ‘unchecked’ bitcoin platforms to exchange their illicit monies.

2.6.4 Technology Cost

Although blockchain can save users money on transaction fees, the technology is far from free. The “proof of work” system that bitcoin uses to validate transactions, for example, consumes vast amounts of computational power. In the real world, the power from the millions of computers on the bitcoin network is close to what Denmark consumes annually. Assuming electricity costs of $0.03~$0.05 per kilowatt hour, mining costs exclusive of hardware expenses are about $5,000~$7,000 per coin. But the increasing rates of blockchain technologies will see the energy consumption rate soar high beyond energy generation of some countries in the immediate future.

2.7 What's Next for Blockchain?

First proposed as a research project in 1991, blockchain is comfortably settling into its late twenties. Like most millennials its age, blockchain has seen its fair share of public scrutiny over the last two decades, with businesses around the world speculating about what the technology is capable of and where it’s headed in the years to come.

With many practical applications for the technology already being implemented and explored, blockchain is finally making a name for itself at age twenty-seven, in no small part because of bitcoin and cryptocurrency. As a buzzword on the tongue of every investor in the nation, blockchain stands to make business and government operations more accurate, efficient, and secure.

As we prepare to head into the third decade of blockchain, it’s no longer a question of "if" legacy companies will catch on to the technology—it's a question of "when."

2.8 Historical Trends of Corrupt Practices and Financial Crimes in Nigeria

EA Owolabi (2007) in his reviewed of the Transparency International Report on the Nigeria Corruption Perception Index in 2004 report on worldwide corrupt practices through a survey which covered 146 countries, posited that in that report, Nigeria was rated the third most corrupt country, beating Haiti and Bangladesh to the second and last positions respectively. The report was an improvement over that of 2000 when Nigeria was reported as the most corrupt country in the world. Statistically, Nigeria's Corruption Perception Index (CPI) was 1.2 in the year 2000, contrasting those of Finland (10.0), Denmark (9.8) and New Zealand (9.4). Expectedly, Nigeria rose up stoutly to criticize the 2004 T. I. report, pointing out serious defects in the manner the results were arrived at. These included the following in the T.I. Report (2004):

(i) Only the bribe takers, not givers or abettors, are punished, while the CPI ignores the origin of the bribes from western companies;

(ii) Irregular and uncontrolled country coverage, the list of countries changes from year to year;

(iii) Biased sample: more than 90.0 per cent of the world is missing; the sample is private sector oriented, overwhelmingly male and the well-off;

(iv) Imprecise and sometimes ignorant sources — some sources are used that do not measure corruption levels at all;

(v) Far too narrow and imprecise definitions of corruption are used, couched entirely in terms of public extortion, with the private sector as its victim;

(vi) Does not measure trends and therefore, cannot reward genuine reformers, even if the reforms are making a difference; and

(vii) The index is misused by development agencies in making decisions as to which countries to "reward" with aid or not.

The focus of the T. I. 2004 report was, however, more on the oil sector as a revenue source for most oil producing countries. The sector was seen as a continuous source of corruption around the world. Peter Eigen, Chairman of T. I. Board of Directors, (2004) observed that, "In these countries, public contracting in the oil sector is plagued by revenue vanishing into the pockets of western oil executives, middlemen and local officials." He suggested that oil companies could help fight corruption by making public details of payments made to government and state-controlled oil firms.

Access to vital information, according to him, will minimize the opportunity for the payment of kickbacks to secure oil tenders, a practice that has blighted the oil industry in transition and post-war economies. Reconstruction will be wrecked by a wasteful diversion of resources to corrupt elites unless there are strict anti-bribery measures. (Eigen, 2004).

According to Gray and Kaufmann (1998), in practice corruption may be well organized or chaotic. When well organized, the required amount of bribe is well known, and the payment guarantees that the desired favour will be obtained. Under chaotic corruption, however, the bribe offerer needs to bribe several officials with no guarantee either that he will not face further demands for bribes or that the favour being sought will actually be given. Both types exist in Nigeria. Corruption is a universal disease and every country is making effort to fight it. The fact that much corruption in developing countries has important industrial countries' participation is commonplace knowledge. The frequent accusations against multinational oil mining companies in their corrupt practices for bribing government officials, local chiefs and elites of the Niger Delta region of Nigeria are a testimony to the truth. This often results in social discontent and violence, when the poor masses have no other option of seeking redress for not having their own fair share of the commonwealth extracted from their ancestral lands.

As already pointed out above, the T.I report (2004) was solely based on Oil Sector and its antecedent activities which are marred by corrupt practices that are

monetarily induced, but there are other corrupt practices in the country's financial institution and the recent concerns about some of our youth that are involved in internet fraud which shall also be reviewed herein below:

2.8.1 Corruption and Financial Crimes

Corruption is like tango; it is a dance for two. If there is a corrupt custom official, it is because there is a businessman who is rewarding him; if there is a tax evader, it's because there is a bureaucrat who is being bribed! President of Paraguay Nicanor Duartor Frutos, (2006).

Although it is very difficult to define corruption, some attempts have been made at some descriptions, which would communicate the meaning of the concept. The International Monetary Fund (IMF) defined corruption as "abuse of authority or trust for private benefit: and is a temptation indulged in not only by public officials but also by those in positions of trust or authority in private enterprises or non-profit organizations" (IMF, 2000).

To the United Nations Convention Against Corruption (UNCAC), however, in 2002, the only option open in attempting to define corruption was to mention specific acts of corruption. This is the approach adopted in the ICPC Act where it merely states that "Corruption includes bribery, fraud and other related offences". According to Justice Emmanuel Olayinka Ayoola, Chairman ICPC, "the commonest form of corruption in Nigeria used to be bribery but in recent years this has been overtaken in level of prevalence by embezzlement and theft from public funds, extortion, abuse of discretion, abuse of public power for private gain, favouritism and nepotism, conflict of interest, extortion and illegal political party financing".

It had been the general opinion that corruption and governance cannot be measured in quantitative terms; but in recent years organizations and nongovernmental organizations (NGOs) such as Transparency International and the World Bank have been able to produce/construct adequate indicators on these.

The World Bank has such indicators covering more than 200 countries, on six dimensions, namely, voice and accountability; political stability and absence of major violence and terror; government effectiveness; regulatory quality; rule of law; and control of corruption. Paolo Mauro (1998), mentioned three principal causes of corruption, which are:

(i) Government restrictions and intervention, which lead to excessive profits. These include trade restrictions (tariffs and import quotas), favourist industrial policies (subsidies and tax deduction), price controls, multiple exchange rate practices, foreign exchange allocation schemes, government-controlled credit;

(ii) Natural resources, e.g., (crude) oil whose supply is limited by nature where huge profits are available to those who extract it; officials who allocate extraction rights are likely to be offered bribes;

(iii) Where civil servants are paid low wages and have to resort to collect bribes in order to feed their families;

(iv) And to this we may add, lack of adequate and sustainable retirement benefits, under which serving officials would want to provide for their future through corruption and fraudulent practices.

Financial crimes may be traceable to some of the enumerated aspects of corruption, e.g., embezzlement, theft from public funds, abuse of discretion and abuse of public power for extortion. Usually, huge amounts stolen from these sources, which cannot be legitimately explained as earnings, are siphoned and hidden across the borders to foreign banks regarded as safe haven. The correct term for moving money in this manner is **money laundering**. In other words, money laundering is defined as "the conversion of criminally obtained money into apparently lawfully obtained money by re-cycling the tainted money through banks and other legitimate financial institutions" NEPAD, (2003).

The amount of money laundered every year is not exactly known but informed guesses estimate that it could amount to from about 2.0 to 5.0 per cent of world

Gross Domestic Product (GDP) IMF, (2004). Several international conventions, standards, best practices and resources to address money laundering have been and are being developed. These efforts have been expressed in United Nations conventions, reports, and programmes, with support from various regional organizations.

In 1989, the G-7 of the most advanced countries in its Economic Summit Group established the Financial Action Task Force (FATF) to develop and promote policies to combat money laundering. The FATF has come up with its "Forty Recommendations" dealing with legal requirements, financial and banking controls. Other measures introduced by the international community include the Statement on Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering by the Basel Committee on Banking Regulations and Supervisory Practices, the IMF's and World Bank's Financial Sector Assessment Programme (FSAP) and the Fund's Offshore Financial Centre (OFC) initiative.

The terrorist attack on the United States of America on September 11, 2001 made the fight against money laundering and financing terrorism and other crimes a top priority for the international community. In this connection, FATF served notice on Nigeria in 2002 warning that it would blacklist the country unless significant steps were taken to address the deficiencies in its fight against financial crimes. It was threatened that on October 31St of that year FATF would impose the sanctions.

2.8.2 HISTORY OF CORRUPTION IN NIGERIA

Corruption or corrupt practice has a long history in all human societies. It does in Nigeria. This section attempts to trace the historical periods through which Nigeria has passed with corruption. The section benefits substantially from the paper of Justice Ayoola referred to earlier:

(i) Colonial Period: Colonialism, western education, the development of urbanization and monetization of the economy were all attended by growth of individualism. All these brought dramatic changes in relationship and the way of

doing things. The consular court system disrupted the traditional administration, which the white colonialists met. In its place was appointed the highly flawed indirect rule under which appointment of personnel was arbitrarily made. Oftentimes, appointees were unknown people, different from the traditional heads and chiefs. Many of the appointed people were of questionable character who often became intoxicated by power, leading them to abuse and misuse of office, including showing favours to criminals. Corruption in the Indirect Rule system soon got to the attention of the colonialists, as most of the warrant chiefs prospered materially through the proceeds of bribery and corruption. Also, the local councils established by them were fertile grounds for corruption.

(ii) Late and Post-Colonial Period: The nationalists who took over the government from the colonialists before full independence was attained exhibited corruption. The Foster-Sutton Commission of Inquiry set up to look into the management of the African Continental Bank owned by the Eastern Region government in the mid-1950s? and the Coker Commission of Inquiry in the early 1960s which considered the affairs of some Western Region Government corporations found the conduct of the key actors of government as falling short of high ethical standards expected of public office holders. Also, at the Federal government and regional levels corruption characterized the First Republic (1960-1966). There were electoral corruption and malpractices involving the use of money to buy votes, employment of thugs to intimidate political opponents, hiring of assassins to eliminate opponents, hijacking of electoral boxes and materials, and the printing of fake voting cards. Naturally, those who attained power through corrupt means had no other ambition than to serve self and promote ulterior interests at the disadvantage of the larger society. The once cherished culture of probity in public affairs soon yielded place to a culture of graft and the standard of public morality continued to deteriorate.

(iii) The Military Periods (1966-1979; 1983-1998): Corruption was widespread among the political class before the military struck in January 1966. Although the military gave prominent position to corruption as the reason for staging the coup and the subsequent coups, unfortunately, military regimes tended to be more corrupt than the regimes they seemed to have come to correct. Despotism, which inevitably characterizes military regimes destroyed a culture of accountability. Characteristically, military regimes upon taking power, in fighting against corruption, would remove from office or dismiss some individuals allegedly for corrupt practices; forcibly seize corruptly acquired property; confiscate property through legislation (decree), directed against particular individuals; and ban and disqualify persons from holding public office. The credibility of such actions was, however, put in doubt for any durable culture of probity. Ethical programmes such as WAI-C (War Against Indiscipline and Corruption) and MAMSER (Mass Mobilization Socio-Economic Reconstruction) introduced against corruption were short-lived and largely ineffectual.

Moreover, the efforts were largely seen to be insincere as a result of the perceived life-style and sudden inexplicable acquisition of wealth by serving service personnel, their relatives and their contractor friends and accomplices, because of their own lack of transparency in governance. In later years, military regimes were seen as institutionalizing corruption and corrupt practices and enthroning a culture of graft.

The relatively brief intervening four years of civilian administration, 1979-1983, was a disappointment because the confidence the populace had placed on it was badly shattered. It turned out, however, in the words of Mallam Nuhu Ribadu, Executive Chairman of EFCC, that the regime was “characterized by gross financial indiscipline and profligacy, wanton waste, political thuggery, disrespect for the rule of law, and bare-faced free-for-all looting of public funds through white elephant projects” Ribadu, (2006).

2.8.3 The Costs of Corruption

Transparency International considers the cost of corruption as four-fold: economic, social, political and environmental. Economically, corruption ranks highest in the construction industry and in the provision of infrastructure; mostly because it is difficult to standardize, and so benchmark costs in this sector.

This is why for instance, budget decision-makers are constantly tilting the budgets towards infrastructure spending, thus increasing the opportunities for corrupt enrichment. If one looks at the bigger picture one is appalled at the multiplier effects of this selfish act — if roads are more "lucrative" than say, education or health, then there will be more funds allocated to road construction. And, if there is more gain in road construction than in road maintenance, then surely, roads will be constructed, allowed to disintegrate and the same roads will be reconstructed from scratch! This can happen at the expense of less spectacular, but basic projects like schools, hospitals, water and sanitation. S. 0. Olatunde, (2007).

In economic and moral terms, corruption is very costly. It undermines confidence in the government, whose moral authority is diminished. Economically, misallocation of resources is worsened by corruption, and government officials will not press for change in the regulations from which they enrich themselves. In fact, officials may press for more of such regulations and license procedures, hoping for more bribes. EA Owolabi (2007).

Corruption aggravates income inequalities and poverty; those who benefit from bribery, kickbacks and preferential deals are not likely to be among the poorest. Corruption adversely affects economic growth, as it acts as additional tax on enterprises, raises costs and reduces incentives to invest. "Informal payments" on public projects may be many times their actual cost.

Corruption imposes a heavy burden on small and medium-sized enterprises, and tends to shift government spending away from socially beneficial investments,

such as health, education, roads and communications towards unneeded "white elephant" projects, or lower quality infrastructure.

Corruption discriminates against honest foreign businesses as a result of lack of transparency in most acts of corruption. In this process, beneficial direct investments often pull out of the country.

Corruption reduces domestic savings and investment and stimulates capital flight, as it weakens domestic banking system. Corruption is one of the most important inhibiting forces on investment and growth, thereby lowering the living standards of the people. Pervasive corruption often discourages donors from providing more aid, which harms opportunity for economic growth. From the above-enumerated costs of corruption, we can summarize some of what corruption has done to Nigeria in a few statements, in the words of Justice Ayoola:

(i) The long duration of corrupt practices in Nigeria has sadly changed people's moral orientation. Corruption is now described in euphemistic terms, e.g., "the Nigerian factor," "egunje" etc., and the corrupt is honoured in the society by reason of his affluence.

(ii) Mismanagement and assault on public treasury and the general decay in ethics and values have had devastating consequences on the economy and resulted in the impoverishment of the people at all levels.

(iii) Nigeria's GDP per capita fell from US $1,010.00 in the early 1980s to US $300.00 in 1999. From recent reliable surveys, above 70.0 per cent of the population lives below poverty line, less than US $1.00 per day.

(iv) Currently, the sixth largest crude petroleum producer in the world, Nigeria still imports most of the refined products consumed domestically. Curiously, recently the Trade Minister of Indonesia, an oil rich country itself, announced that an agreement would soon be signed to make Indonesia import crude oil from Nigeria. This is easily understandable by the fact that Indonesia has a large capacity to refine its crude while Nigeria does not. And the greatest advantage is derived from refined products rather than crude.

(v) Over the years, corruption has become so widespread, enabling economic and organized crimes to flourish. Nigeria was condemned to the status of a pariah state and consistently rated as one of the most corrupt countries in the world.

(vi) Foreign investors may be reluctant to invest in Nigeria for fear of losing their money to swindlers and fraudsters.

(vii) By far the most tragic cost of corruption is the way it spreads and perpetuates itself from generation to generation. A youth who sees his parent's prosperity through corrupt practices, which might have included the child's admission to school, will invariably be convinced that corruption is the best means to "make it in life". At adulthood, while in position of authority he would invariably know no other way of life. Many of our present-day leaders may have been brought up this way. The virus of corruption is like a malignant cancer whose growth is very tough to control, unless the patients are personally convinced of its dangers and have a radical change of life-style and culture.

2.8.4 SOME INITIATIVES AND MEASURES TAKEN TO FIGHT CORRUPTION AND FINANCIAL CRIMES IN NIGERIA

Especially during the years of military rule, Nigeria made an impressive body of laws and took other initiatives in the war against corruption and financial crimes. These are in addition to the criminal and penal codes that have existed since the colonial period, under which official corruption and other offences were tried. The laws and decrees include the following:

- Investigation of Assets (Public Officers and Other Persons) Decree of 1968
- The Corrupt Practices Decree 1975
- Public Officers (Special Provisions) Decree 1976
- Recovery of Public Property Decree 1984
- National Drug Law Enforcement Agency (NDLEA) Act, 1990. This was the first law made in Nigeria to make money laundering a criminal offence.

• The promulgation of the Mutual Assistance in Criminal Matters within the Commonwealth (Enactment and Enforcement) Act No. 13 of 1988, designed to bring Nigeria's municipal law in line with the Harare Scheme. The scheme contains provisions on how to deal with the proceeds of crime and laundering of such money.

• The Public Complaints Commission Act Cap 377, Laws of the Federation 1990

• The Code of Conduct Bureau and Tribunal Act Cap, Laws of the Federation 1990.

• The Criminal Code Act Cap 77, Laws of the Federation 1990

• The Penal Code, Northern States Federal Provisions Act —Cap 345, Laws of the Federation 1990

• Banks and Other Financial Institutions Act 1990

• Recovery of Public Property (Special Military Tribunal) Act Cap 389, Laws of the Federation 1990

• The Failed Banks (Recovery of Debts) and Financial Malpractices Act No. 18 of 1994

• Failed Banks Act No. 16 of 1996

• Advance Fee Fraud and other Related Offences Act No. 13 of 1995, intended to deal with the menace of the so-called "Nigerian fraud letters" or "419"

• The Foreign Exchange (Miscellaneous Provisions) Act No. 17 of 1995

• The Money Laundering Act No. 3 of 1995 All these together with the existing Criminal and Penal Codes Nigeria were before the first term of President Obasanjo. Regardless of these plethora of anti-corruption legislations, corruption and corrupt practices grew increasingly. This was perhaps why the international community saw Nigerian laws as grossly inadequate in dealing with these crimes. There are significant gaps in terms of the coverage of the laws and the adequacy of penal and forfeiture provisions and enforcement procedures. Odozi, (2002) concludes that, the laws lacked diligence in implementation, which was attributable to reasons including the following:

(i) Inadequate resources for designing and implementing various anticrime measures;

(ii) Impediment imposed by the laws on bank secrecy which shielded the criminals and/or allowed them to frustrate prosecution;

(iii) Large and growing unregulated informal sector with varying degrees of opacity and criminality;

(iv) Fragmentation of legal provisions and arbitrage opportunities for criminals;

(v) Poverty in the country which provides excuse, if not justification for various forms of economic crimes;

(vi) Cross-border porosity and protection for criminals;

(vii) Lack of political will to resolutely implement tough anti-crime measures.

Consequently, only very few offenders have been successfully prosecuted and tried for corruption as the technicalities of the laws were exploited by defence lawyers to their great advantage. In addition, most of the agencies charged with enforcing the laws were not faithful in keeping abreast of the dynamics and changes of a modern society, especially the intrigues of corrupt people and their accomplices.

All these formed the background to the Obasanjo administration's determination to combat corruption head-on from 29th May, 1999.

2.8.5 INCIDENCE OF ADVANCE FEE FRAUD: TYPES, VICTIMS AND PREVENTIVE MEASURES

Corruption, especially in the public sector and economic crimes, including money laundering and advance fee fraud have dominated public discussions in Nigeria in the last few decades because of the serious negative image they create and the harm they cause to the economy.

Fraud is a crime that involves the use of deceit to obtain pecuniary advantage. It is not a new phenomenon. However, the most disturbing aspect of fraud is the alarming proportion, its sophistication, notoriety and intensity worldwide and the fact that it does not respect the niceties of international borders makes it a major concern for any right-thinking society and it should be nipped as it buds.

According to Schneider, S. (2019), **Advance fee fraud**, type of fraud in which businesses or individuals are required to pay a fee before receiving promised stocks, services, money, or products, which ultimately are never given. The targets of the fraud—which include businesses and individuals—receive a solicitation (by letter, fax, or e-mail) from someone posing as a business representative or government official promising that a large sum of money (often in the tens of millions of dollars) will be deposited into the target's bank account. To ensure this, the recipient of the letter is asked to pay a percentage of the total amount that purportedly will be wired or transferred. Advance fee fraud scams originate in a number of countries and may use internal conflicts or other circumstances specific to that country as a pretence under which funds must be transferred abroad.

The solicitation will ask its prospective victim to respond to the correspondence, including name, address, phone number, and banking information. Subsequent correspondence will ask for a processing fee from the target before the money can be transferred. This fee is often in the tens of thousands of dollars. The letter will often provide specific directions on how this fee should be paid (usually a wire transfer to an overseas bank account). Once the processing fee is deposited, the funds are quickly withdrawn, and the perpetrators either disappear or attempt to coax even more money from the victim. Some schemes have gone so far as to have victims fly to a country, where they are extorted for even more money through intimidation and violence. No funds are ever transferred to the target.

The funds that are purportedly to be deposited in a target's account are frequently described as money that must be quickly and surreptitiously transferred out of a country due to a number of reasons, such as a civil war, bankruptcy fraud, an unclaimed bank account or inheritance, or the embezzlement of money from a government or business. Regardless of the specific claim, the source of the funds is frequently held out as illegally derived. This tactic is used to increase the credibility of the offer and to deter any victims who accept the offer from going to police, due to their own perceived complicity in an illegal action.

Advance fee fraud has existed in various forms since at least the 18th century, though the modern concept dates to the 1920s. In the 1980s, advance fee fraud became closely associated with African-based criminal groups, Nigerian criminal enterprises in particular. It was sometimes called 419-fraud, after the relevant section of the Nigerian criminal code. The 419-fraud scheme was a variation of the confidence swindle, which preys on peoples' greed and naïveté.

According to the Securities and Exchange Commission, Advance Fee Fraud gets its name from the fact that an investor is asked to pay a fee up front or in advance of receiving something of greater value. This type of scam has been around for quite some time. Over 100 years ago, the "Spanish prisoner letter" scam was used, where scammers contacted businessmen via letter alleging that someone connected to a wealthy family in Spain was in prison, and in exchange for a small fee to help smuggle them out, the wealth would be shared. The fee was paid, there was no prisoner, and no wealth shared. During the 1980's, variations of these letters starting coming from Nigeria. They began as letters mailed to potential victims and evolved into e-mail scams, as it drastically cut the cost of sending.
Advance Fee Fraud (AFF), on the other hand, is a class of fraud usually perpetrated by deliberate distortion and misrepresentation of facts of a matter with the aim of deriving financial benefits from unsuspecting, greedy, corrupt and

gullible individuals. AFF is usually non-violent in nature. However, event may turn violent when the victim attempts to track the perpetrator who may also devise the means of avoiding prosecution, including elimination of the victim. Owolabi E. A. (2007).

AFF proposals have some common elements. The first is that the proposals are usually unsolicited. The victims may not even be aware of the possibility of the deal. It is usually the fraudster who will do everything to convince the victim of the benefit and feasibility of the deal. Second, the fraudster will usually stress the urgency and need for confidentiality of the deal. Third, the victim will need to make advance payment. Finally, the fraudster must have a good knowledge of the victim whereas the victim does not usually know the fraudster well.

2.8.6 Different Forms of Advance Fee Fraud

Different countries have had several versions of this crime perpetrated by their nationals and foreign collaborators. What determines the type that is prevalent in any country depends on level of efficiency in government procurement, structure of the economy and macroeconomic stability, the ease of foreign exchange transfer, the level of corruption in the country, etc. The most notable versions of Advance Fee Fraud relate to:

a) Transfer of funds from over invoiced contracts: - In this case, proposals are made for the victim to part with some money to

facilitate the transfer of an excess payment on a contract already executed by a contractor who apparently is unaware of the excess payment. The fraudster pretends to be either the Minister, the Permanent Secretary or a Director who awarded the purported contract, for say N65.00 million, while, the actual project cost was N50.00 million. The balance of N15.00 million is what he wants his victim (usually a foreigner) to receive into the latter's account on his behalf and the sum will be shared with the victim in certain proportions, sufficiently attractive to the victim. The second stage after the victim would have consented

and forwarded his account number, is to ask him (the victim) to make some advance payments to enable him meet some Transfer charges, bribe some officials, including the Governor of the Central Bank, etc. Such payment eventually becomes substantial and normally represents the loss to the victim as the transfer itself will not take effect.

b) Benefactor of a Will: - This type is usually targeted at churches and non-governmental organizations purported to be beneficiary of a rich man's will in another country. In this case, the organization is written and informed of what has been assigned to it in the will which is ready for collection. However, before the fund or property is released to the beneficiary, certain conditions, including payment of some charges, must be fulfilled. To accept the deal is to become a victim.

c) Lifting of Crude Oil at a Relatively Low Price: - In this case the fraudster claims to be in position to grant licence to lift crude oil at a price far below the market price. However, certain down payment has to be made to settle the Minister or other top government officials he represents as well as other incidental expenses prior to oil lifting.

d) Contract Fraud: - Here the victim is assured of payment on delivery of goods without proper documentation or with fake documentation and address. Once the victim delivers, no payment follows. Another variant is for the supplier to be convinced on the need for him to pay local registration for his goods to be introduced to local market. Forged documents could be presented to make it look as if local regulations dictate that. Once such money is paid the victim is short-changed.

Yet another variant is for the fraudster to pay for one or two previous orders only for a large order to be placed and for the payment not to be made by the fraudster when the third but large order has been delivered.

e) Real Estate Purchases: - In this case, partial advance or full payment is made for rental or purchase of properties. The fraudster may in fact not have lien over the property. He disappears after receiving the money.

f) Currency Conversion: - The victim is promised a more attractive rate of exchange than prevails officially to convert dollar to local currency or vice versa. Once the remittance is made in advance, the transaction becomes hooked with the victim losing his deposit.

g) Beneficiary fund scam – The scammers often present some type of story about needing your help to get money from a bank in another country. The story will usually involve someone who has died and the perpetrator alleges that if they do not act quickly, the money will be turned over to the government.

h) Lottery scam – Scam claims that you have won money in an overseas lottery. The letter or e-mail will usually ask for personal information to confirm your identity so you can collect your winnings.

i) Investment scam – An investment company contacts you and needs your assistance in investing money overseas. The letter or e-mail will look as though it is coming from a reputable investment firm or government official. The letter will ask you to contact the company, where you will be asked to pay some sort of fee up front in return for a hefty profit that does not exist.

j) Romance scam – Scammers pull at the heart strings of those on internet dating websites and chat rooms by asking for money for sick relatives, or money for a plane ticket to meet you in person. This type of AFF is very rampant now in the Nigerian Cyber Space especially amongst the youth who are infamously referred to as Yahoo-Boys, G-Guys, Sase Boys who often engaged unsuspecting victims on premium dating site and claimed to be just anybody while defrauding their would-be lover or supposedly fiancé or fiancée several thousand of USD overtime.

Techshielder (2021) analysed international and domestic reports to find the place one is most likely to fall victim to a dating scam, as well as the monetary loss per victim. The analysis also revealed where the biggest fraudsters live, the cities with

the highest number of victims and how much money is lost to find the places you should avoid when looking for love. The research revealed that last year - 2020, dating scams cost the world a massive $218million, which works out to be an average loss of $17,661 per victim.

It turns out that the Philippines is responsible for the highest number of dating scam cases. Over 1,300 romance fraud cases have been reported against the country, and they are responsible for a whopping $4 million in financial loss. Ranking in second place is Nigeria. With a population of 201 million, Nigeria has accounted for 1,129 reports of scams. The total amount of money lost due to Nigerian dating scams is a staggering $16.8 million, this totals to an average loss per victim of $14,892. Rounding off the top three is Canada. The world's second-largest country has taken $7.8 million out of love-seekers pockets and has broken 1054 hearts due to catfishing.

At the other end of the scale, we have the European country of Iceland. The nation has only accounted for a total of 1 case of dating scam and has stolen no money at all. The study also revealed that the United Kingdom has scammed the most amount of money with romance scams. Nigeria is third on the money scale.

An article recently published in the New York Times described an advance fee fraud scheme that carried on for years, claiming almost 2,000 victims and $26 million. The Company appealed to people looking for investors for their businesses. During a time when job insecurity was high, bank requirements for loans were strict, the Company provided high hopes for those just trying to make a living by making them believe they would invest in their business or find investors for them. The hopeful entrepreneurs only needed to pay up-front fees of between $10,000 and $40,000. Unfortunately, the Company did nothing with the money. When clients started complaining and asking for their money back, phone calls were not returned and files were transferred to someone else. One victim, who felt as though he was fairly business savvy, looked to the Company to help him find investors for a multi-use development project. After paying

$15,000 in “due diligence” fees and over $1,000,000 in pre-development costs, the victim was forced to declare bankruptcy on one of his businesses. Because the Company worked diligently to make their business appear legitimate, they were able to de-fraud even the smartest of business owners. Sadly, the money lost by victims is generally very difficult to recover. Companies like this word their contracts to make it almost impossible for victims to sue for fraud. Therefore, it is imperative to understand the warning signs of a suspicious business opportunity.

2.8.7 The Victims of Advance Fee Fraud

Experience from the cases of AFF that have been blown open shows that victims are characteristically the corrupt and gullible individuals who want to be rich quick and with the tendency to be fraudulent. The victims are usually of age 45 years and above in the middle or the upper class in the economy. They are usually perceived to be strong financially and have flair for quick money. Most of the time, the fraudsters have information about the victims and must have undertaken some research about them. Details regarding their life styles, telephone numbers, business interests, etc, of the victims are usually available to them.

Honest citizens also bear the cost of this crime. This comes in the form of man-hour lost by witnesses during investigation and trial appearances. Similarly, consumers sometimes pay higher prices in crime-affected businesses since such extra cost involved in such AFF deals are often passed on to the products. In the same way, tax evasion by fraudsters results in higher tax burden for honest citizens as government activities have to be financed with tax revenue.

2.8.8 Cost of Advance Fee Fraud

The cost of Advance Fee Fraud to an economy is enormous. This cost manifests in the following forms among others:

a) Discourages investments, particularly foreign investment inflows and inhibits economic growth;

b) Brings loss of confidence in the economies of the countries of the perpetrators;

c) Reduces the confidence of the citizens in the capacity of its government to protect them from fraudsters;

d) Leads to high cost of crime prevention and detection where it is prevalent;

e) Distorts the flow of trade as confidence level falls;

f) Undermines the stability of banks and other financial institutions;

g) Increases inflationary pressures; and

h) Makes a country a candidate for listing as a non-cooperating country and territory by the **Financial Action Task Force** on Money Laundering and Financing of Terrorism.

i) Untimely death of the victims if they cannot pull it through and great sorrow and psychological trauma for the families left behind, which can also lead to untold hardships for the bereaved families.

2.8.9 Some Necessary Precautions and Warning Signs

The starting point is for all countries to ensure good governance, accountability and transparency in its activities. A country where all of these are absent is usually a fertile ground for fraudsters to exploit. Given the methods generally adopted by the perpetrators of Advance Fee Fraud, the following warnings, precautions and signs should be observed in order not to be a victim.

i) Extreme care should be taken in entertaining proposals of individuals and companies that were not previously known;

ii) Establishment of business dealings should be based on diligent search. Attempts should be made to “know your customers well”. Ensure that a company introducing a business deal is properly registered in the country of residence. This constitutes a basis for seeking redress in the court of law as an unregistered company is not a legal entity;

iii) It is necessary to examine self-role in any activity. The legality of the deal should be of interest to the potential victim. Any transaction that is not legal cannot constitute basis for seeking redress;

iv) There is the need to be suspicious when the first contact with the business partner is on phone or through a letter; Be suspicious of anyone who does not have a direct telephone line and who is not around when you call, but promises to return your call later.

v) Investigate the caller, the business he is involved in and his life style; and
vi) There is need to report suspicious cases to the law enforcement authorities. The EFCC has the primary responsibility for investigating and prosecution of all financial crimes, including AFF.

vii) Be wary of business deals that require you to sign non-disclosure or non-circumvention agreements that are designed to prevent you from independently verifying the integrity of the people with whom you intend to do business.

2.8.10 Some Measures Aimed at Curbing Advance Fee Fraud in Nigeria

The high incidence of AFF and the bad image it has created for Nigeria prompted the government to adopt some measures which were aimed at combating the activities of the fraudsters. These include:

a) The provision of section 419 of Nigeria Criminal Code, though admittedly obsolete in terms of its definition, recognized the corporate, economic and national consequences of the activities of fraudsters.

b) The "Advance Fee Fraud and Other Fraud Related Offences Act, 1995" did not only correct the inadequacies of the Criminal Code, but proscribed all forms of conduct used in advance fee fraud and other fraud schemes. The Act has extra-territorial effect in that it proscribes the conduct carried out within and outside Nigeria which results in a person or organization being defrauded. The Act makes

it possible for Nigerian and foreign syndicates to be prosecuted in Nigeria for offences committed within and outside the country. Offenders can be tried in absentia and convicted while they suffer the punishment after returning to Nigeria. There is also the severe penalty of up to 10 years imprisonment without an option of fine for convicts.

c) Enlightenment programmes for local and the international communities have also been stepped up to sensitize the public of the risk involved in unsolicited offers and advice given on what action to take when such proposals come up.

d) Investigation and enforcement of AFF are taken very seriously by the EFCC which is empowered by the provisions of the EFCC (Establishment) Act 2004. As in many countries, difficulties are often encountered in combating this crime. The problems include false identities and addresses often used by fraudsters to open accounts with banks, as well as the reluctance of victims to open up because of the fear of prosecution as accomplices. Moreover, the more the crime becomes internationalized the more difficult it is to get the culprits.

e) Deterrent and preventive measures aimed at making AFF less profitable and stopping reinvestment of proceeds of Advance Fee Fraud and other related crime are contained under Section 7 of the Advance Fee Fraud and Other Fraud Related Offences Act, 1995.

f) Anti-money laundering measures put in place and enforced through the banks are aimed at ensuring that any amount above N1.0 million for individual and N5.0 million for corporate bodies going through banks are reported and properly investigated. Proceeds of AFF and other criminal activities of an amount beyond these thresholds can easily be traced. Offenders are often prosecuted.

The CBN Anti-corruption site has provided avenue for reporting AFF cases. Such cases have often been handled in collaboration with the EFCC and other agencies of government.

2.8.11 Global Efforts to Curb - The Advance Fee Fraud Coalition

The Advance Fee Fraud (AFF) Coalition was announced on October 28, 2008 by its founding members, Microsoft Corp, Yahoo! Inc, The Western Union Company and the African Development Bank, to raise global awareness among consumers of the threat posed by lottery hoax e-mails, a common form of advance fee fraud. The collaborative effort was designed to educate internet users so they are better able to protect themselves against fraudulent activities online. Because of the international and elaborate nature of advance fee fraud, the Coalition believes that no company, no law enforcement unit, no industry can solve this problem alone. AFFCOALITION (2008)

Subsequent to its founding, the Coalition has established a broad set of goals that range from providing preventive consumer education, streamlining the process of identifying accounts used by fraudsters to communicate and obtain payments, and identifying ways of driving enforcement in the following ways:

a) Public Communication

The Coalition will work together to increase the public awareness on advance fee fraud as we realize that the more people learn about and understand this type of fraud, the fewer will be likely to fall victim to these frauds in the future. The coalitions' information will be directed both at the users of our products and services, and also to the general public-- for example, by joining hands when possible with the AFF information campaigns of other organizations and with consumer protection authorities.

The criminals have been counterfeiting the trusted brands of the coalition members to fraudulently acquire the trust of victims, and now the AFF Coalition members aim to use their trusted brands to instead publicly warn potential victims of the risk of advance fee fraud.

B) Mitigation

Each AFF Coalition member seeks to identify service accounts or transactions used by fraudsters, so that appropriate action can be taken. Members of the AFF Coalition are committed to improving their respective tools or processes for mitigating against advanced fee fraud through prevention and disruption.

c) Enforcement

AFF Coalition Members are committed to identifying appropriate enforcement opportunities, as well as to analysing fraud patterns and trends. These may include investigations, civil lawsuits, or criminal referrals, depending on the facts and circumstances of the particular case.

2.9 THE EMERGENCE OF THE ICPC. THE EFCC AND OTHER ANTI CORRUPTION AGENCIES

If the people cannot trust their government to do the job for which it exists - to protect them and to promote their common welfare — all else is lost. And that is why the struggle against corruption is one of the great struggles of our time.

President Barrack Obama as a United States Senator visiting the University of Kenya. 28 August 2006, in his attempt to charge government to be accountable and transparent in its conducts.

This issue of trust is what was lacking in Nigeria Public -Private Space at the return to civil rule in 1999, which largely marked the end of military interregnum into constitutional civilian rule, especially after the dreaded General Sani Abacha led Military Junta.

In an effort to quickly established stability and commenced a process that has morphed into the establishment of new Agencies as a central point of coordination to other existing anti-corruption agencies, policies and acts; At the

inception of the new democratic administration, President Olusegun Obasanjo declared:

“Corruption, the greatest single bane of our society today will be tackled head on at all levels. Corruption is incipient in human societies and in most human activities. But it must not be condoned. No society can achieve anything near the full-blown cancer it has become in Nigeria; the rampant corruption in the public service and the cynical contempt for integrity that pervades every level of bureaucracy will be stamped out.”

As at today the government has enacted the Corrupt Practices and Other Related Offences Act 2000 under the umbrella of Independent Corrupt Practices and Other Related Offences Commission (ICPC), and the Economic and Financial Crimes Commission (EFCC) Act 2002 as well as a thoroughly revised and updated Money Laundering Act. In these Acts, the tools for identifying, investigating and convicting offenders are enhanced.

“The use of presumptions, the reversal in the burden of proof, the seizing of assets or freezing of accounts and the establishment of specialized autonomous anti-corruption agencies apart from police are included in the Anti-corruption Acts”. Ajibola (2006).

The responsibility of the ICPC include receiving petitions and investigating them, and in appropriate cases, prosecute the offenders; studying systems and practices of government and where they aid corruption and fraud, to advise government on how to avoid and change procedures and systems; to educate the public and foster their support against corruption.

The EFCC Act was passed in 2002, which created the EFCC with the single establishment purpose of fighting crimes including Advance Fee Fraud, money laundering, fraud, and bank-related malpractices. This Act was amended by the EFCC (Establishment) Act of 2004.

Other agencies in the anti-corruption crusade include the Code of Conduct Bureau, National Food and Drug Administration (NAFDAC), Standard

Organization of Nigeria (SON), the Budget Monitoring and Price Intelligence Unit, otherwise known as "Due Process", which enforces strict adherence to probity in the award and execution of government contracts.

The Federal Government has tried to pursue the policy of transparency in revenue allocation and other public remuneration to a considerable degree in order to bring an end to abuse and waste of scarce public resources. It has thus tried to demonstrate good leadership; it, however, remains for many of the state governments to exhibit the same degree of tendency.

Some of the concrete manifestation of success in Federal Government efforts in recent years can be mentioned:

(i) Serving Ministers involved in bribery scandals dismissed and prosecuted;

(ii) Since the beginning of Obasanjo Administration in 1999, three Senate Presidents have been made to quit their positions for various offences;

(iii) An Inspector General of Police was dismissed from office, prosecuted, tried and jailed for corruption and abuse of office;

(iv) A state Governor was successfully impeached for money laundering, and he is currently being tried in the court;

(v) The culprits in the biggest international fraud involving US $242.00 million were arrested, tried and jailed;

(vi) On a positive note: NAFDAC and NDLEA have been commended in their respective areas of responsibility for effectively destroying fake and dangerous drugs and prosecution of narcotic peddlers. NDLEA received the commendation of the US President on 20th September, 2006 for its effectiveness in the war against narcotics.

(vii) Some Director-Generals of NAFDAC have received both local and international commendations for the effectiveness of the organization.

(viii) The Budget Monitoring and Price Intelligence Unit in the award of government contracts have saved over N500.00 billion of public funds.

(ix) The Treasury Single Account has equally guide against wastage associated with Staff Costs and Budgetary Utilization in Public Funds – No More Ghost Workers in Most Institutions that have been captured by IPPIS.

Recently, Nigeria subjected herself to sovereign credit rating and the country was given a B-B rating by Fitch and Standard & Poor's, placing her on a par with Brazil, Serbia, Ukraine, Philippines, and Vietnam. This will enable Nigeria to access international finance on terms equal to countries with equivalent rating. Apart from the improvement in the international debt payment to the Paris Club, the former Finance and Coordinating Minister of the Economy attributed this relatively high and favourable credit rating to the "significant achievements registered in the fight against corruption and in the improvement of transparency, notably through the work of the Due Process Office, the monthly publication of funds shared to the three tiers of government, the proactive engagement with the Extractive Industries Transparency Initiative and the first-rate efforts of the EFCC and the ICPC" Okonjo-Iweala, (2006). This is a good testimony to the progress made so far.

Corruption has grown with Nigeria as a country. It gets more and more ingrained, especially as the economy deteriorates and the rate of crime increases in more recent times in the Country. There is hardly any day a newspaper will not carry stories of corruption and/or financial crime. Corruption in Nigeria is not practised systematically; it ***is systemic***. Corrupt practices are met both at public and private places. Almost anywhere a service is to be provided the service is not freely obtained. The Chairman of ICPC was recently quoted as saying that some government institutions are the most corrupt in Nigeria, maybe because those

institutions practise their own more openly, or their services touch people more directly.

At the government sector, hardly anything, which has immediate touch on people goes on free of corruption: child education (admission, promotion), seeking employment, licensing or registration of small businesses, financial services, etc. In the private sector obtaining product distributorship, small or major contracts, provision of various needed services, etc. Common to both sectors are embezzlement, fraud and other financial crimes.

Corruption has become the second nature in most places. It is a major paralysis on the economy. Even at the highest level of governance as exemplified by the scandal between the National Assembly and the former Minister for Education, in a bid to increase the budget vote for the Ministry. This type of corrupt practice is highly injurious to the whole economy as a result of the serious distortions it introduces to planned government expenditure, which had earlier been considered and approved by the Federal Executive Council. Corrupt practices and financial crimes may not be confined to that incident only.

Although considerable improvement has been brought to anti-corruption and anti-financial crimes strategy under the Obasanjo Administration through the ICPC and the EFCC, consisting of investigation, prosecution and conviction of offenders, what has been seen so far is at best a “firefighting” operation. Only a few known cases can be treated at a given period of time. The larger parts of the system/practice remain untouched, and perhaps immediately unknown. In furtherance with this, an eminent jurist, Prince Bola Ajibola (2006), is proposing what is known as Restitution, whereby, for example, a fraudster can receive double punishment/penalty.

First, the court will try him/her and impose penalty for the crime; and secondly, the victim will sue the fraudster to court and get judgment to recover his/her loss to the fraud. But it still falls within the current system of punishing individual offenders. The ICPC Act if fully implemented seems to be a step beyond this

situation having included public education, enlightenment, and awareness of the evil and the harm, which the vice has been doing to the country and the economy. Establishment of effective watch-dogs in strategic places to nip in the bud the tendency to commit these crimes is an urgent necessity. Everything must be done through public enlightenment and mobilization to successfully fight corruption in Nigeria. Corruption is a killer, but it must be killed.

And more recently, the Federal Government of Nigeria initiated the Whistle Blower Policy. The Whistle Blower Protection Bill was proposed at the National Assembly in the past. However, the Bill only scaled the second reading in October 2016. The Policy was approved by the Federal Executive Council in December 2016. The Policy was created by the Federal Ministry of Finance for Whistle Blowers.

The Policy provides that if the government is able to recover stolen or concealed assets through information provided by a Whistle-Blower, then he/she may be entitled to between 2.5% - 5% of amount recovered.

To qualify for the reward, the whistle-blower must have provided the Government the information it does NOT already have and could not otherwise obtained the information from other publicly available source to the government. The actual recovery must also be because the information provided by the whistle-blower. The Policy does not provide ANY immunity from civil or criminal prosecution. What this means is that if during the Investigation some of the evidence links a whistle-blower to partaking in the act of corruption or a related incident, the Whistle-Blower would NOT be immune from criminal prosecution. He/She Could Technically be charged for a crime that he/she helped to blow the whistle on. This policy was also designed to give impetus to the on-going campaigns against corruption and financial crimes, however it seems not to be yielding as expected.

Nigeria lacks a designated whistleblower law that covers employees and citizens from retaliation if they report crime, corruption or public health threats. Furthermore, Nigerian law does not recognize people who make such reports as whistleblowers. Consequently, there are no legal mechanisms to protect whistleblowers from retaliation. There is no government agency that receives and investigates reports from workplace whistleblowers, lends support or legal advice to whistleblowers, or offers them protection from retaliation and adverse consequences.

2.10 CORRUPTION IN THE PUBLIC SECTOR DEFINED

While the EFCC tends to be more of curbing corruption and fighting financial crimes in the private sector, the ICPC is more focused on the Public Sector. Although corruption is a multi-hydra faceted socio-economic malaise in every human endeavour and various attempts have been made in curbing and preventing its occurrence and the how ICPC is approaching this phenomenon headlong will be reviewed below.

Corruption can be difficult to define since there is no one single definition to capture its multifarious manifestations because as Onigu Otite (2000) says: "…although the ubiquity of corruption is otherwise acknowledged, its magnitude and character are defined by different social and cultural contexts and time dimensions".

Therefore, a universally agreed definition for "corruption" that will cover the whole gamut of human behaviour may be elusive but for practical purposes, suffice it to provide one or two working definitions.

The Corrupt Practices and Other Related Offences Act 2000 says corruption **"includes bribery, fraud and other related offences"** while the Vision 2010 Committee in its report explains corruption as **"all those improper actions or**

transactions aimed at changing the normal course of events, judgement and position of trust."

The World Bank (1997) describes corruption as **"the abuse of public office for private gains. Public office is abused for private gain when an official accepts, solicits or extorts a bribe. It is also abused when private agents actively offer bribes to circumvent public policies and processes for competitive advantage and profit. Public office can also be abused for personal benefit even if no bribery occurs, through patronage and nepotism, the theft of state assets or the diversion of state revenue."**

The dynamics of corruption are aptly captured in the following formula by Cobert Klitgaard:

C (corruption) = M (monopoly power) + D (discretion) – A (Accountability).

This means that corruption thrives in situations where monopoly power exists along with large discretion without accountability. In practical terms, any socio-economic arrangement where organizations or individuals involved in the process of service delivery have monopoly power over the resource's production, allocation and utilization; have discretionary power to decide who receives or is allocated the resource and in what proportion; and where accountability is relegated to the background, will provide fertile ground for corruption.

According to Odekunle (2012) corruption can be fought with the following formula: CG+CS+VA-LI =PC {for investigation}

Where CG = Consumed Goods
CS = Consumed Services
VA = Verified Assets
LI = Legitimate Income
PC = Presumed Corruption {for investigation}

The Corrupt Elements in Nigeria live ostentatiously, have stupendous ill-gotten wealth and are shielded by the powers that be which ushers-in anger and hatred.

The police and other regulatory agencies fighting against corruption are overwhelmed, helpless and castrated. The so-called International Community is regularly conspiring with corrupt Nigerians with reckless abandon by offering looters safe haven; the punishment given to treasury looters in Nigeria is not commensurate with the gravity of their crimes. All these deprive the people required resources for a decent living. The unwanted attributes associated with corruption are veritable [remote and immediate] harbingers of conflicts and mass massacres in Nigeria which must be squarely addressed by governmental and non-governmental concrete actions.

Other socio-economic factors that can be defined as the motivators and reinforcers for corrupt practice include: extremely poor welfare and working conditions which render incomes far below escalating costs of decent living; unwieldy operational procedures that engender "the shortcut/fast-forward mentality" which triggers inducement from the public; prevalent job and social insecurity; pervasive poverty that provokes social pressure on office holders; high societal tolerance for corruption; a culture of impunity engendered by the 'sacred cow' mentality; weak enforcement mechanisms; defective leadership; low risk of penalties as against the high proceeds realizable from corruption; greed; excessive materialism; very weak ethical environment; the lust for power etc.

2.10.1 CLASSIFICATION OF CORRUPTION

Corruption can be classified using different parameters: size or amount of money involved, the degree of incidence, location of occurrence, etc. Thus, some classifications of corruption are:

Grand Corruption: occurs at the highest level of government usually in the contract process and involves enormous monetary value. It often impacts heavily on government budget and growth prospects.

Political Corruption: this involves the subversion of the political process and it is aimed primarily at capturing power for determining the rules of economic and political engagement. It also seeks illicit pecuniary benefits and is associated with Grand Corruption.

Bureaucratic Corruption: this occurs at the level of government bureaucracy and often involves perversion of laid –down rules of due process. It usually aims at private monetary gain through wrongful inducements and illicit payments for rendering public service. It can also be classified as Petty Corruption because of the usually small amount of money involved.

Judicial Corruption: this takes place when judicial officers fall short of the standard of Integrity and the course of justice is perverted for personal gains.

Moral Corruption: this covers all immoral behavior that is socially unacceptable to the generality of people.

2.10.2 CORRUPTION IN THE PUBLIC SECTOR

The Public Sector is that part of the economy that is owned and controlled by the government. It is the operational space within which the government relates to the people and delivers its obligations to them. These obligations include among others, security, welfare, education, social infrastructure, social justice, and an enabling regulatory or deregulatory framework on the economy. The Ministries, Parastatals and Agencies of government which make up the public sector and their aggregated functions form the government/people interface; the quality of which shapes assessment of governance by the public. Incompetence and corruption by public sector operatives corrode this interface, thus translating to poor governance and leading to the censure of government.

In Nigeria, the public sector is very significant because the government is the chief driver of the economy.

Everything deliberately done or not done, in order to subvert laid down procedures for official transaction in the public sector is corruption. This can be with regard to recruitment, procurement, internal staff issues such as training, promotion, welfare, policy implementation etc. As stated earlier, the incentive for corruption is always not pecuniary even though the very obvious cases have to do with monetary benefit. The private gain sought may be power, influence, ego, status, etc. Any reward or inducement that is intended to deflect a person from the honest and impartial discharge of his duties constitutes a corrupt act.

Although corruption is by no means peculiar to Nigeria or to its public sector, it had until recently, almost become a synonym of the Nigerian official environment. Various shades of corrupt practices characterize public offices e.g., embezzlement, fraud, diversion of funds, gratification, nepotism, falsification of documents, outright theft of government property, favouritism, wilful absenteeism, awarding contracts to 'front' companies, lodging public funds in private accounts, over-invoicing, approval of sub-standard projects, disregard of due process etc.

Endemic corruption in Nigeria has negatively affected the fabric of society in profound ways. It has created the sad paradox of widespread and dehumanizing poverty in the midst of abundant natural and human resources. The crippling effects of corruption are manifest in the erosion of the institutional and administrative capacity of government, the decayed infrastructure and appalling service delivery across all sectors of the economy.

The devastating consequences of corruption on the polity further include the stunted social and economic development, astronomical levels of unemployment, escalating crimes, violent ethnic and religious hostilities, moral decadence, brazen injustices, unsavoury standing in the brotherhood of nations, etc. Given the quantum of these negative effects, the unmistakable fact is that corruption is a clear danger to the corporate and individual existence of Nigerians.

President Olusegun Obasanjo captured this scenario so aptly when he declared at the inauguration of the Independent Corrupt Practices and Other Related Offences Commission (ICPC) on 29th September, 2000 that **"I have for many years held the view that corruption, in all its ramification, is the greatest single impediment to our national aspiration to enter the new millennium with confidence; corruption checkmates all vision for a morally strong and economically prosperous society. Indeed, corruption is the antithesis of development and progress …"**

2.10.3 THE ICPC AS AN INTERVENTION MECHANISM AGAINST CORRUPTION

The Independent Corrupt Practices and Other Related Offences Commission (ICPC) was inaugurated on the 29th of September 2000 on the legal platform of the Corrupt Practices and Other Related Offences Act 2000 which is the legislation that prohibits and prescribes punishment for corrupt practices. The Act came into operation on the 13th day of June 2000. Prior to its enactment, certain laws had been and are still in existence as legal instruments meant to combat corruption in the country.

These laws include: the Criminal Code; the Penal Code; the Recovery of Public Property (Special Military Tribunal Act Cap. 389, Laws of the Federation of Nigeria 1990(as amended in 1999); the Failed Bank (Recovery of Debts and Financial Malpractices in Banks) Decree 1994(as amended in 1999); the Code of Conduct Bureau and Tribunal Act (Cap 56 Laws of the Federation of Nigeria 1990); the Criminal Justice (Miscellaneous Provisions) Decree, 1966 and the Corrupt Practices Decree 1975.

In some of these laws, the offences of corruption were not comprehensively defined and classified. Their interpretations and applicability to certain situations were also rather complex. These facts, along with the ingenuity of corrupt elements in fashioning out novel methods of perpetrating their nefarious acts,

rendered the provisions of these laws inadequate in the fight against corruption. This inadequacy informed the enactment of the Corrupt Practices and Other Related Offences Act 2000.

There are certain features of the ICPC Act 2000 which make it unique and well-positioned as an effective weapon in fighting corruption in Nigeria.

Some of these features are:

a) statutory independence of the Commission - S. 3 (14)
b) the holistic, three-pronged approach to fighting corruption (enforcement, prevention and education) - S. 6 (a) - (f)
c) provision for an independent counsel to investigate allegations of corruption against officers with constitutional immunity - S. 52
d) non-admission of custom or tradition as a plea - S. 60
e) designation of Judges to hear corruption cases - S. 61 (3)
f) protection of information and informer - S. 64

THE DUTIES OF THE COMMISSION:

The duties of the Commission as stated in Section 6 (a) - (f) of the Act are, in summary, as follows:

a) To receive and investigate reports of the attempts to commit or the actual commission of offences as created by the Act and, in appropriate cases; prosecute the offender (s) (Enforcement).
b) To examine, review and enforce the correction of corruption-prone systems and procedures of public bodies with a view to eliminating and/or minimizing corruption in public life (Prevention).
c) To educate and enlighten the public on and against corruption and related offences with a view to enlisting and fostering public support for the fight against corruption (Education).

As is evident from the above, the Commission's duty is not only to investigate, arrest and prosecute people for corruption, but it is also charged with corrective,

preventive and educational responsibilities. The whole essence of the Act is not just to punish offenders but to facilitate the creation of a corruption-free society by engaging in a systemic overhaul of the machinery of the state which hitherto had sheltered administrative lacunas and thus encouraged the widespread incidence of corruption; the creation of this new society is also expected to be facilitated through the general re-orientation of the Nigerian populace.

2.11 Roles of Banks in Curbing Financial Crimes

Fighting financial crimes is not an optional action given the grave implications of these crimes on the banking sector. The fight against financial crime is vital to the stability of both domestic and international financial system. it is a fight that calls for un wavering commitment and constant re-assessment of threats and counter-measures in order to stay one step ahead of the criminals In the light of the fact that financial crime is dynamic and criminals are increasingly going into alliances, the players within the Nigerian financial system must be creative as well as make concerted efforts to put in place appropriate measures to close all the loop-holes which financial criminals have taken advantage of; Also to counter financial crimes operators in the banking sector must engage in partnership or strategic alliances with regulat ory and law enforcement agencies for effective result.

Dr Caleb M Fundanga, Governor of the Bank of Zambia (2003) asserted that differences in money laundering legislation and in the implementation of international standards such as, know your customer regulations, customer identification and secrecy laws have led to regulatory arbitrage. This has worked to the advantage of money launderers because they can move the proceeds of their activities to less regulated territories where there are lax laws. Therefore, to avoid

launderers from taking advantage of the weaknesses in the application of international law, many governments have decided to co-operate in order to combat money laundering. In this regard, the most notable international initiatives/responses to money laundering include:

First, the Financial Action Task Force (FATF). The FATF is a 26-member intergovernmental, policymaking body that was established in 1989 to guide the implementation of anti-money laundering measures in the aftermath of the 1988 UN Drugs Convention. Its membership includes the major financial centres of Europe, North America and Asia. The FATF has come up with 40 recommendations which member countries are expected to adopt. These are designed for universal application and cover the criminal justice system and law enforcement, the financial system; it's regulation and international cooperation.

Second, the Basel Committee of Banking Supervision. The main thrust of regulatory response to money laundering has been to stop dirty money from entering the banking system and to make sure that it is traceable when it occurs. The Basel Committee, a grouping of the world's leading bank supervisors has so far come up with three guidelines for banks in combating money laundering, namely: *'The Prevention of Criminal Use of the Banking System for the purpose of Money Laundering' (1988),* the *'Core Principles of Effective Banking Supervision' (1997),* and the '*Customer due diligence for banks' (2001).*

Third, the Wolfsberg Principles. The Wolfberg Principles came into force in 2000 and are an industry response to the threat of money laundering. They are an agreement among eleven major international private banks (which account for at least a third of the world private banking funds) to guide the conduct of international private banking. Essentially, the Principles seek to control money laundering by cutting across the multiplicity of jurisdictional issues and

addressing the serious reputation damage they were suffering in the media because of money laundering.

Besides the foregoing, Banks have specific roles to play to effectively contain financial crimes within their system. Some of these roles are considered below.

a) Banks should strengthen internal financial controls policies and operations. Laxness and the easing of internal controls merely because no one has ever been caught stealing has been the start of many internal crime cases. Internal controls are necessary to check the enemies within and block loopholes that may be taken advantage of. To check internal fraud and crime, banks should look out for the following indicators among employees:
   i. Staff under stress without a high workload - marked personality changes
   ii. Always working late with no apparent justification
   iii. Reluctance to take leave
   iv. Unexplained wealth or living beyond apparent means
   v. Sudden change of lifestyle
   vi. Customer complaints of missing statements unrecognized transactions.
   vii. New staff resigning quickly
   viii. Rising costs with no explanation
   ix. Key employees having too much control or authority without audit checks
   x. Employees with external business interests

2. Identification of customers: Banks should do comprehensive KYC – "Know Your Customers" before

opening account or entering into fiduciary transaction with any person(s) to avoid dealing with criminals.

3. Staff training and development; regular training for employees on money laundering issues including how to detect suspicious transactions, staff duties under the Money Laundering Prohibition Act 2004 and on other financial crimes.

4. Deployment of anti-crime prevention IT solution - When talking about security and the rising occurrence of financial crime, there are several factors to be considered, all of which are interconnected and imperative to resolve. These include understanding the changing nature of financial crimes; the technologies available to counter attacks, particularly the growing number of online incursions; and the need to educate employees and customers on this digital warfare.

5. The responsibility to authorize transactions, the responsibility for collecting or paying cash and the responsibility to maintain accountability - records must be separated within a bank.

6. Job descriptions must be clearly defined and responsibilities for each position clearly delineated.

7. Banks should maintain a strict accountability procedure related to the movement or flow of cash. Banks should not deviate or become lax in the enforcement of this protocol. The rules must apply to everyone in the bank no matter how the length of service and level of trust.

8. Banks should reconcile and audit their books regularly. Regular audits should be occasionally backed up by an unscheduled and unannounced audit.

9. Banks should ensure that passwords to computer files, pass codes to enter facilities and security protocols are frequently changed to reduce the potential for

abuse. Evaluate the necessity for someone in your bank to know certain passwords or codes. Do not permit people to use other's passwords for convenience's sake.

10. Lock up unused cheques and account for them numerically in a log. Limit access to the cheques to a limited number of authorized personnel. Bank statements should be reconciled independently and away from those employees authorized to handle accounts payable/receivable or employees recording the information.

11. Do not fail to discipline employees that deviate from the bank's policy. An atmosphere of permissiveness breeds the potential for internal corruption.

12. Banks should always beware of large-scale cash transactions, the large or rapid movement of funds, and an unrealistic net worth compared to reported income and / or employment.

13. Banks should strengthen and improve on the culture of records preservation for the purpose of audit trail and also to meet regulatory requirement.

14. Banks should strengthen existing inter-bank relationship as well as cooperate with all regulatory and law enforcement authorities in all cases relating to financial crimes. Unless. banks work together and cooperate with relevant authorities it will be difficult to achieve significant success in the fight against financial crimes within the banking sector.

2.12 Media Rights and Press Freedom on Crimes Reporting in Nigeria

In a widely published online report by Reporters without Borders in early 2021, Nigeria is now one of West Africa's most dangerous and difficult countries for journalists, who are often spied on, attacked, arbitrarily arrested or even killed. The campaign for the elections in which President Muhammadu Buhari obtained another term in February 2019 was marked by an unprecedented level of disinformation, especially on social media. The all-powerful regional governors are often the media's most determined persecutors and act with complete impunity. In 2018, one governor had part of the premises of a radio station razed

after a series of reports criticising his handling of local affairs. Online freedom is restricted by a 2015 cyber-crime law that is widely used to arrest and prosecute journalists and bloggers in an arbitrary manner. Three journalists have been shot dead while covering Islamic Movement in Nigeria protests since July 2019 without any proper investigation to identify those responsible. The police are often the direct beneficiaries of impunity and were blamed for the death of a young trainee journalist after arresting him in October 2020. The major street protests in 2020 were accompanied by violence against the media. Several news organisations were torched and many reporters were attacked. With more than 100 independent newspapers, Africa's most populous nation enjoys real media pluralism but covering stories involving politics, terrorism, financial embezzlement by the powerful or conflicts between communities is very problematic. This was seen yet again in 2020, when an investigative reporter was threatened and several of his sources died or were killed after he investigated massacres in the northern state of Kaduna.

As at the time of writing this research, Nigeria is currently ranked 120/180 in the 2021 World Press Freedom Index, this is coming as at the time FGN banned TWITTER indefinitely throughout the country after the social media platform deleted one of the President's tweets, and by the attacks and threats it poses to the media according to journalists interviewed by RSF.

The implications from this development is that Press, Media and Citizens' participations in the fighting against corruption and financial crimes will be at the lowest ebb as none want to be lynched, maimed or killed for divulging an information all in the name of public interest.

Ranking since 2013

Year	Ranking		Year	Ranking	
2020	115 / 180	↑	**2015**	111 / 180	↑
2019	120 / 180	↓	**2014**	112 / 180	↑
2018	119 / 180	↑	**2013**	115 / 180	=
2017	122 / 180	↓			
2016	116 / 180	↓			

Fig. 2.2 Showing Nigeria's Corruption Index Ranking 2013 - 2020

2.13 Globalization Concept and Implications for Nigeria as necessitated by ICT

The blockchain distributed ledger technology offers a secure, transparent, verifiable, democratic, decentralised, efficient, and tamper-resistant way to record and transfer data across international boundaries that are not bound by physical or geographical demographics. The incidence of globalization as necessitated by the emergence of Internet and now one of its major antecedents – blockchain networks, will definitely makes the world witness a rapid deployment of services that are hitherto impossible to achieve.

Joel Oluwatobi, (2020), asserted that Blockchain technology can help to improve globalization by enabling transparency as well as the faster movement of goods and services. The birth of blockchain technology and its quick adaptation have left many people stunned, with famous CEOs, investors, entrepreneurs and financial experts often talking about how it will change the way we go about our daily financial activities.

One of the most important aspects to consider in blockchain technology is how this relatively new technology can help improve globalization — i.e., the process of interaction and integration of people, companies and governments worldwide.

He further stressed that One of the most important things in the global economy is the movement of goods and services. Currencies are used to facilitate these movements, but issues such as high inflation rates and currency manipulation techniques are making a lot of people worried about the validity of traditional currencies.

Immutability could make cryptocurrencies the right tool to facilitate the movement of goods and services. Even though some government officials argue that the speed and network congestion of cryptocurrencies are hindering them from being adopted as a tool for globalization, many projects have started to disprove these assumptions. This is making cryptocurrency a globalization tool that people can trust. For an instance **QtumX**, an Open-Source Project has claimed to be able to do 10,000 Transaction Per Second far better than the Visa Network that All Financial Institutions are using that is reputed to make 1,700 Transaction Per Second.

James Manyika, Jacques Bughin, and Jonathan Woetzel, (2016) concluded that though it seems globalization is rescinding due to the economic melt-down that happened in 2008 rather, it is entering a new phase defined by soaring flows of data and information.

Remarkably, digital flows—which were practically non-existent just 15 years ago—now exert a larger impact on GDP growth than the centuries-old trade in goods, according to a new McKinsey Global Institute (MGI) report, *Digital globalization: The new era of global flows*. And although this shift makes it possible for companies to reach international markets with less capital-intensive business models, it poses new risks and policy challenges as well.

The world is more connected than ever, but the nature of its connections has changed in a fundamental way. The amount of cross-border bandwidth that is used has grown 45 times larger since 2005. It is projected to increase by an

additional nine times over the next five years as flows of information, searches, communication, video, transactions, and intracompany traffic continue to surge. In addition to transmitting valuable streams of information and ideas in their own right, data flows enable the movement of goods, services, finance, and people. Virtually every type of cross-border transaction now has a digital component.

Trade was once largely confined to advanced economies and their large multinational companies. Today, a more digital form of globalization has opened the door to developing countries, to small companies and start-ups, and to billions of individuals. Tens of millions of small and midsize enterprises worldwide have turned themselves into exporters by joining e-commerce marketplaces such as Alibaba, Amazon, eBay, Flipkart, and Rakuten. Approximately 12 percent of the global goods trade is conducted via international e-commerce. Even the smallest enterprises can be born global: 86 percent of tech-based start-ups surveyed by MGI report some type of cross-border activity. Today, even the smallest firms can compete with the largest multinationals.

Individuals are using global digital platforms to learn, find work, showcase their talent, and build personal networks. Some 900 million people have international connections on social media, and 360 million take part in cross-border e-commerce. Digital platforms for both traditional employment and freelance assignments are beginning to create a more global labor market.

In this increasingly digital era of globalization, large companies can manage their international operations in a leaner, more efficient ways. Using digital platforms and tools, they can sell in fast-growing markets while keeping virtual teams connected in real time. This is a moment for companies to rethink their organizational structures, products, assets, and competitors.

Global flows of all types support growth by raising productivity, and data flows are amplifying this effect by broadening participation and creating more efficient

markets. MGI's analysis finds that over a decade, all types of flows acting together have raised world GDP by 10.1 percent over what would have resulted in a world without any cross-border flows. This value amounted to some $7.8 trillion in 2014 alone, and data flows account for $2.8 trillion of this impact. Both inflows and outflows matter for growth, as they expose economies to ideas, research, technologies, talent, and best practices from around the world.

Although there is substantial value at stake, not all countries are making the most of this potential. The latest MGI Connectedness Index—which ranks 139 countries on inflows and outflows of goods, services, finance, people, and data—finds large gaps between a handful of leading countries and the rest of the world. Singapore tops the latest rankings, followed by the Netherlands, the United States, and Germany. China has grown more connected, reaching number seven, but advanced economies in general remain more connected than developing countries. In fact, each type of flow is concentrated among a small set of highly connected countries.

Lagging countries are closing the gaps with the leaders at a very slow pace, and their limited participation has had a real cost to the world economy. If the rest of the world had increased its participation in global flows at the same rate as the top quartile over the past decade, world GDP would be $10 trillion, or 13 percent, higher today. For countries that have been slow to participate, the opportunities for catch-up growth are too substantial to ignore.

An analysis by PwC (2020) shows blockchain technology has the potential to boost **global gross domestic product (GDP) by $1.76 trillion** over the next decade. That is the key finding of a report assessing how the technology is being currently used and exploring the impact blockchain could have on the global economy. As organizations grapple with the impacts of the COVID-19 pandemic, many disruptive trends have been accelerated. The analysis shows the potential

for blockchain to support organizations in how they rebuild and reconfigure their operations underpinned by improvements in trust, transparency and efficiency across organizations and society.

The major take-aways from this analysis are:

a) The report identifies five key application areas of blockchain and assesses their potential to generate economic value using economic analysis and industry research. The analysis suggests a tipping point in 2025 as blockchain technologies are expected to be adopted at scale across the global economy.
b) Tracking and tracing of products and services – or provenance – which emerged as a new priority for many companies' supply chains during the COVID-19 pandemic, has the largest economic potential ($962bn). Blockchain's application can be wide ranging and support companies ranging from heavy industries, including mining through to fashion labels, responding to the rise in public and investor scrutiny around sustainable and ethical sourcing.
c) Payments and financial services, including use of digital currencies, or supporting financial inclusion through cross border and remittance payments ($433bn).
d) Identity management ($224bn) including personal IDs, professional credentials and certificates to help curb fraud and identity theft.
e) Application of blockchain in contracts and dispute resolution ($73bn), and customer engagement ($54bn) including blockchain's use in loyalty programmes further extends blockchain's potential into a much wider range of public and private industry sectors.

Blockchain's success will depend on the general understanding of the concept and contextual essence of it, the supportive government policy environment, a

business ecosystem that is ready to exploit the new opportunities that technology opens, and a suitable industry mix.

2.14 The Nigeria Government Fear in the Acceptance of Blockchain

The Central Bank of Nigeria's Onslaught against Bitcoin (One of the very first used cases of The Blockchain Network Platform) seems not to be effective as the Nigeria's Cryptocurrency Ecosystem appeared to be undaunting of the sudden ban on all crypto-exchanges from all possible channels of the Financial Institutions in the Country, this was a similar move to some other Countries like China who also put a peg on Crypto Markets in the Asian Markets.

In February, the Central Bank of Nigeria ordered banks to "identify persons and/or entities" who were conducting transactions in crypto or running crypto exchanges and "ensure that such accounts are closed immediately." But that ban didn't stamp out bitcoin in Nigeria. Rather, the crypto community turned to peer-to-peer trades, or sending payments directly to each other. Coindesk (2021).

Crypto communities world-wide have always found ways around government bans, and Nigeria is no exception. In a recent blockchain research conducted by Chainalysis, (2021) the dollar volume of crypto received by users in Nigeria has been consistently growing in 2020 and 2021, which may be partly related to this year's bull market. In May, Nigeria received $2.4 billion worth of crypto, compared with $684 million last December, the analytics firm said.

While that kind of geographical data comes with caveats, it's clear that crypto is alive and well in Nigeria.

According to **Katharina Buchholz (2021)** in a survey from Statista, 32% of respondents in Nigeria use crypto. Nigeria also ranked eighth in Chainalysis' 2020 report on cryptocurrency adoption around the world. The interest in crypto

surged last fall, when activists with the "EndSARS" movement, protesting against police brutality in Nigeria, used bitcoin to raise funds.

Economic factors also appear to spur adoption.

"Recently, the devaluation of our local currency encouraged people to start saving in crypto assets like Bitcoin and Ethereum," said Udeaja Kingsley, CEO of the BiTA crypto startup, adding that the crypto users are "mostly the youths that believe in it and are trading it via the means of P2P."

So far in 2021, the Nigerian naira has been losing value with the country's inflation rate at 18%. While U.S. dollars might be hard to obtain in Nigeria, bitcoin sometimes serves as a proxy for the dollar, allowing people to hedge against naira's inflation. Because most of the goods Nigerians buy are imported, U.S. dollars are in high demand and there is often not enough of them available on the market.

Cryptocurrencies like bitcoin highlight the potential of money's digital future despite being created outside the confines of the traditional global banking system. And its sharp rise in adoption has led to a scuffle with legacy institutions in determining the future of money.

The argument against cryptocurrencies has typically focused on concerns around fraud and volatility. That hasn't stopped some countries, like El Salvador, from using bitcoin as a legal tender. For others that see bitcoin and cryptocurrencies as a threat to their national banking and financial systems, Central Bank Digital Currencies act as direct replacements for rising interest in something other than fiat.

Chimezie Chuta, founder and coordinator of Blockchain Nigeria User Group, told TechCrunch recently that "The concept of CBDCs has become a necessity for central banks. Money is a tool for controlling people. They do not want to allow

the primary tool of control to be eroded because the entrance of privately issued cryptocurrencies like bitcoin and Ethereum is a direct challenge to central banks' authority everywhere in the world. CBDCs come in as their response, albeit weak ones,"

2.15 Effects of Central Bank Crackdown on Cryptocurrency in Nigeria

Vice President Yemi Osinbajo, (2021) in a response to a question asked by of the Journalist on the Central Bank Onslaught on ALL Cryptocurrency Services and Exchange by All Nigeria Bank and other Financial and Security Firms in the Country…he said the Regulator should research and reviewed the cryptocurrency value in its entirety and possibly comes up with a mechanism for checking abuse, rather than outright reject as most of our youth are trading genuinely on the Blockchain Platforms. This should have been the initial position of all CBN in the world – especially for those who feel threatened by the disruptive tendencies the Blockchain Technology brings to the Financial Markets. Amongst other things the following are the immediate noticeable effects of the CBN ban on cryptocurrency:

a) **Providers Account are Frozen & Suspension of Service to Users:** The Federal Government of Nigeria and with a particular reference to the Central Bank of Nigeria has asserted that they do not 'banned' cryptocurrencies in the country per se. Only that Banks and other Financial and Security Exchange Firms will no longer offered nor provide any services to their numerous customers/clients on cryptocurrencies and other related service, said Adamu Lamtek, the Deputy Governor of CBN in the wake of the controversial ban on crypto business in Nigeria. However, the fallout truth and reality from the Service Providers are far from what the CBN said as one of the leading firm in crypto-business - Luno, the crypto wallet owned by Digital Currency Group (also CoinDesk's parent company), has had fiat deposits and withdrawal frozen since February, it said in a recent statement by the CEO Marcus Swanepoel. Although the company

managed to get its bank account in Nigeria unfrozen in June, users still can't move their fiat funds to and from the platform, Swanepoel said, adding that the company "intensified regulatory lobbying" to get the issue sorted out. "We are negotiating day and night with the relevant stakeholders in Nigeria to get them to collectively work with the government to find a solution that works for everyone," he added. "This includes the CBN and other crypto platforms, and allowing people to withdraw is the main priority."

In report by Coindesk, (2021) Chike Okonkwo, sales and partnerships lead in Africa for an asset manager Thresh0ld, and also a member of the Stakeholders in Blockchain Technology Association of Nigeria (SiBAN), said the crypto community has been trying to talk with the central bank, but hasn't heard back so far.

He says SiBAN, along with other two organizations, Blockchain Nigeria User Group and Cryptography Development Initiative of Nigeria, has been working to get on the same page with regulators for a while.

"We have been having meetings with the [Securities and Exchange Commission, the country's securities regulator] before the CBN ban news but due to the fact that the CBN did what they did, the SEC had to pause their own plans," Okonkwo said.

In February 2021, just as a response to the Central Bank of Nigeria's ban on crypto-business, the Security and Exchange Commission – now called The Exchange Group halted her plans to 'regulate' crypto-business activities in Nigeria – which could have been the first of its kind in the world. The decision to ban crypto-business in Nigeria is not in its entirety taking in the public interest as the Apex Regulator didn't research well on the incidence and phenomenal of the blockchain network technologies and weigh the benefits for the teeming Nigeria Populace, especially the youth. The End Sars Protest in October 2020 right after the relaxation of Covid-

19 Lockdowns has shown that Cryptocurrency Adoption is not coming – its already here and I don't see it being stopped.

b) **Alternative Channels for Cross-Border Wealth Creation:** CoinDesk, (2019) pointed out that, some of Nigeria's importers already switched to crypto as a payment method, says Keith Mali Chung, president and co-founder of Loopblock Network, an African blockchain firm. "Over 70% of all that is being consumed in Nigeria is imported, and with financial restrictions, bitcoin is gaining all the attention it deserves," he said. Chinese merchants selling clothing and electronics in Nigeria are using crypto as a means of exchange, Chung said. The pattern is similar to the one in Eastern Europe, where Chinese merchants might be sending tens of millions of dollars in crypto across the border daily. "A lot of people are taking advantage of the [decentralized finance] industry right now, it's giving equal financial opportunities for all, irrespective of nationality or whatsoever," Chung said. "A lot of people are jumping into different yield farming programs, I know quite a number of people who got DeFi loans to run their businesses," he added. It's hard to estimate how much money is moving from Nigeria to China this way, Chung said, but he has some anecdotal evidence. "I know of individual [merchants] who transact over $2 million to $5 million daily, and they are countless, and the numbers are rapidly increasing," he said.

From the foregoing, one could easily deduce why it is not total correct for CBN to crackdown on crypto-business and the Exchange Group halting their initial lucrative plans to provide security mechanism for crypto- trade, because that move would have provided the platform and yardstick for measurement and analytic controls as well.

c) **Peer-to-Peer Trade Volume Boom:** As a general norm world over, the survival instincts of any social animal are always measured by its intuitiveness and innovative thoughts to steer and sail out of the storm; the

crypto ecosystem has been demonstrating that in all the countries where government have been attempting crackdowns. Crypto communities world-wide have found ways around government restrictions, and Nigeria is no exception. According to Paxful's (Paxful a service that enables users to buy and sell bitcoin in a peer-to-peer fashion,) Youssef, (2021) after the Central Bank of Nigeria banned crypto-related bank transfers in February Nigerians sent even more bank wires purchasing bitcoin than before. Paxful is “on pace” to have 23% more trades funded with bank transfers in Nigeria than last year, and 36% more in terms of volume, Youssef said. According to UsefulTulips, in the first half of 2021 the volumes of two major P2P platforms in Nigeria, Paxful and LocalBitcoins, were the largest in Africa, totalling over $200 million.

During the first five months of 2021, Nigerians traded 50% more than the same period last year on LocalBitcoins, said Jukka Blomberg, LocalBitcoins’ chief marketing officer, adding that new registrations have also increased this year. That activity may be at least partly explained by the fact that P2P trades are not easy for government officials to trace. When people send money directly from one personal account to another, without channelling it through a third party, it’s hard to see how exactly individuals are using the money. It could be for bitcoin they purchased from someone, their apartment’s monthly rent or paying back a debt to a friend. It would thus be difficult, if not impossible, for banks to "ensure that such accounts are closed immediately,” as the Central Bank of Nigeria ordered.

Nigeria is the largest market for the company, with around 1.5 million users and over $1.5 billion trading volume, according to Paxful.

According to Yele Bademosi, CEO of the Africa-focused crypto app Bundle, turning to peer-to-peer transactions might actually make the crypto

ecosystem in Nigeria healthier and more resilient. “In my opinion, we (Nigerians) got too comfortable about the fact that we were relying on centralized rails and channels to on/off ramp crypto,” Bademosi told CoinDesk. “In the ethos of bitcoin, P2P methods are more resilient as they don’t have a central point of failure.”

d) **The Entrepreneurship of Some Youth is Growing and Developing:** Ray Youssef, CEO of Paxful believes the biggest factor of crypto’s popularity in Nigeria has been “the intense drive and business aptitude of the Nigerian youth.” The Spirit of Entrepreneurship is baked into their DNA,” Youssef asserted. According to Chung in the CoinDesk report, some young Nigerians view bitcoin and smaller, newer cryptocurrencies as a way to make some money as the traditional economy lags because of the dire socio-economic situation which is now aggravated by the Covid-19 pandemic.

In an online survey conducted by Statista (a Data Platform) in 2020, Reliance on remittances and the prevalence of peer-to-peer phone payments have led to a steep rise of cryptocurrency use in Africa's largest economy. Out of 74 countries in the Statista Global Consumer Survey, Nigerians were the most likely to say they used or owned cryptocurrency. About a third of those who took part in the survey are Nigerians – with age demographic within the range of 18years – 45years.

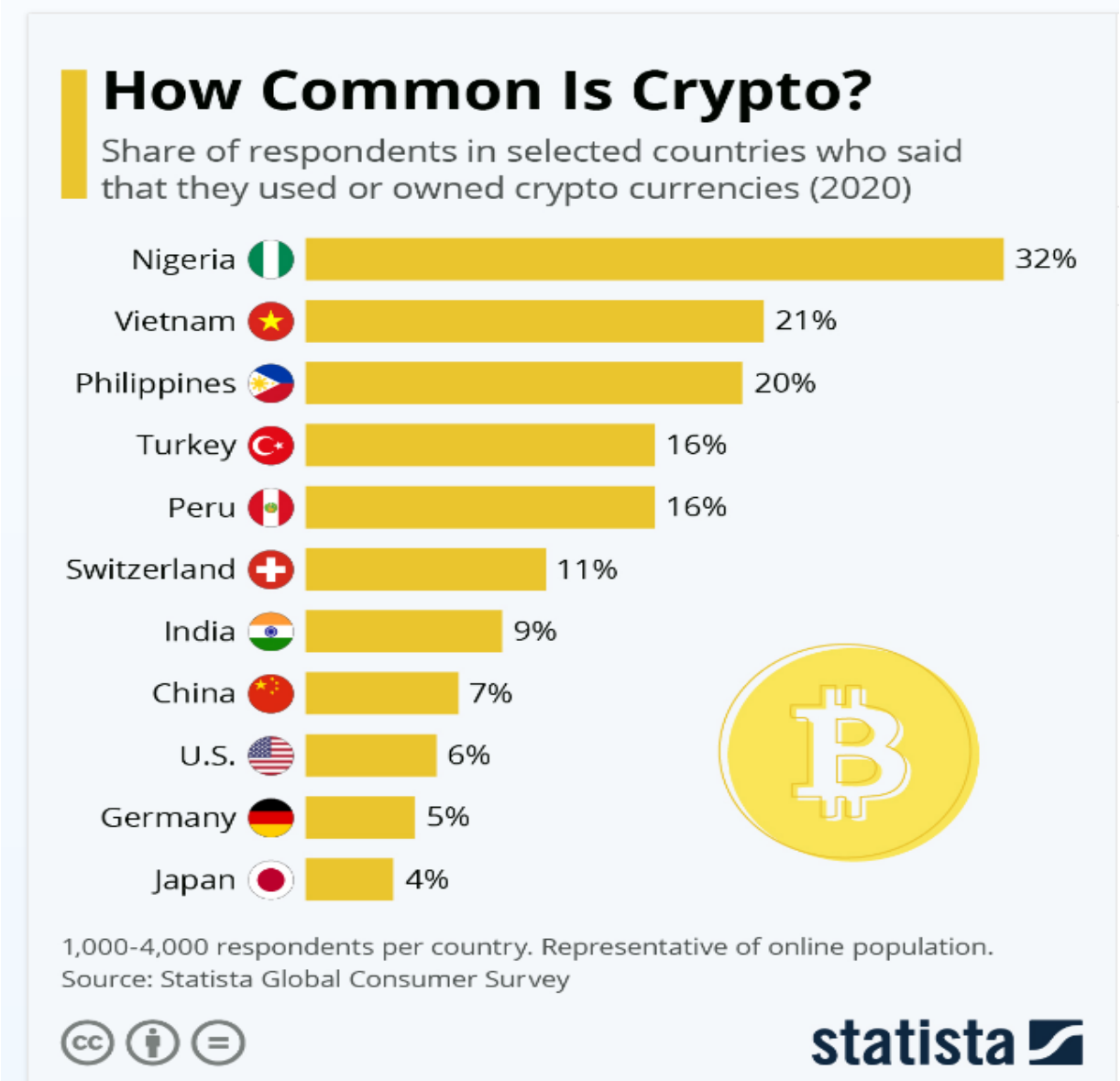


Fig: 2.3 Showing How Common is Bitcoin in the World

The reason(s) for this position is not far from the fact that the economic situation in the Country is dire and the youth can't just be waiting endlessly for a government that would turn the tides! This lack of trust in the policies of government has been unabated far too as Elites and Political Leaders amass wealth wantonly – an incidence that leads to hatred and casting aspersion on the Leadership and the System.

e) **Introduction of Central Bank Digital Currency:** The announcement of Central Bank of Nigeria to introduce a Digital Currency termed "e-Naira' (CBDC) and it subsequent launched on 25th October 2021 recently could be said to be false hope. Because the released framework and mode of operations of the e-Naira is not a novelty approach to what an ordinary banking App would have done with ease! And it doesn't do anything different from the existing Fiat Money.

The e-naira is based on the Hyperledger Network Infrastructure – a permissioned open-source network where members are 'admitted' and granted some levels of privileges – which means some nodes on the network has more capabilities than the others and not to mention that your membership rights and privileges can be revoke by the administrator(s) of the platform.

The Hyperledger Platform is also costly to run and managed unlike the Distributed Ledger of the Blockchain Network.

Hyperledger Fabric is an enterprise-grade open-source platform that is maintained by IBM and Linux Foundation. Unlike Bitcoin and Ethereum, Hyperledger Fabric does not have any cryptocurrency, where the access to the network is restricted to the network members only, and not anyone can join the network. The mechanism used to validate the transactions and create blocks in Hyperledger Fabric is Practical Byzantine Fault Tolerance (PBFT) protocol, M. Castro and B. Liskov, (1999). The transactions are controlled in Hyperledger Fabric using chaincode (smart contract), which is a program code that provides the ability to write and design the applications to interact with the network. The privacy of the transactions between the participant in the network can be obtained using an isolation mechanism known as channel. The channel ensures that the

transaction and data are available only to the nodes that are members in the channel.

2.16 RELATED RESEARCH WORK ON BLOCKCHAIN

The only seemingly challenge for the global adoption of Blockchain into the Business and Financial Mainstream appears to be the inability to outperform the VISA Network which is reputed to be 1700TPS. Therefore, in this section, the research and experimental works done to enhance and evaluate the performance of some blockchain platforms and their protocols are briefly highlighted in this section:

Bartoletti et al., (2017) proposed a framework that supports data analytics only on Bitcoin and Ethereum platforms. The proposed tool permits relative blockchain data to be integrated with data from external sources. The framework also allows it to organize the data in a database.

Xu et al, (2017) classified the blockchain implementations and compared them with the blockchain-based frameworks to study the impact of the blockchain architecture on software architectures. The introduced classification highlights major blockchain platforms architectural characteristics and the impact of the blockchain design on the quality of the blockchain-based software, such as performance and scalability.

B. Koteska, E. Karafiloski, and A. Mishev, (2017) identified the quality attributes for the blockchain technology and investigated the quality issues, solutions, and requirements for blockchain implementation. The results show that the blockchain platforms need to be improved in many aspects, such us security, scalability, privacy, and performance, in terms of latency, cost-effectiveness, etc.

Yasaweerasinghelage et al, (2017) proposed the use of simulation framework and performance modelling to predict the latency of blockchain-based systems. Most

of the predicted results have a relative error of less than 10%. This approach also aims to help in evaluating different blockchain design options.

Kocsis et al, (2017) proposed a performance evaluation model for blockchain technology, which was used to evaluate Hyperledger Fabric v0.6. The main purpose of the model is to evaluate the software design in its early stages, where changing the requirement of the software will not have a big impact on the overall cost and time.

Croman et al, (2016) studied the challenges in blockchains scalability, especially Bitcoin. The results showed that, to get significant throughput and latency improvements, reparameterization of the Bitcoin's interval and the block size is suggested.

Jermy Rubin, (2015) introduced an open-source software "BTCSpark" for analyzing Bitcoin and building blockchain analysis tools. The tool provides an environment that is easy to use with good performance.

In a recent study by H. Sukhwani, J. M. Martínez, X. Chang, K. S. Trivedi, and A. Rindos, (2017) designed a performance model for the Practical Byzantine Fault Tolerance (PBFT) consensus mechanism which is used in Hyperledger Fabric. The study studied the possibilities for performance bottlenecks in networks that have large numbers of nodes.

Kokoris-Kogias et al, (2016) introduced a scalable consensus protocol for public blockchain platforms called ByzCoin. The proposed protocol provides better security and performance when it was tested on Bitcoin platform.

Behl et al. (2014) presented a parallelization approach to scale BFT systems and increase their performance. The evaluation results showed that using this approach will increase the throughput of the system compared to the throughput achieved with the traditional approach.

Eyal et al, (2015) proposed Bitcoin-NG protocol to address the scalability of Bitcoin. The paper also addressed the security and efficiency of similar protocols. The evaluation results of the protocol demonstrated that Bitcoin-NG with limited bandwidth provides optimal scalability.

Vuckolic et al, (2016) compared between proof of work based blockchains and those based byzantine fault tolerance in terms of scalability and performance. The paper showed that the performance of bft based blockchains (such as Hyperledger) is better compared to those that are based on PoW (such as Bitcoin). On the other hand, PoW based blockchains provide better scalability than bft based blockchains.

Aniello et al, (2017) presented implementation and evaluation for a two-layered blockchain platform for a federated database. The proposed architecture provides high performance and data integrity but is weak in terms of scalability and data availability.

Aniello et al. (2017) also investigated different consensus mechanisms to overcome the current issues in architecture, such as Byzantine Fault Tolerant (BFT) and Distributed Hash Table (DHT).

Suankaewmanee et al, (2017) proposed Mobichain which is a mobile commerce application that uses blockchain as a core technology. The aim of this application is to make the transaction in m-commerce more secure. The paper also conducted performance evaluation for the Mobichain application, which showed that the proposed module is efficient solution for m-commerce applications.

A recent study by S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, (2017) measured the performance of two permissioned blockchain implementations: Ethereum and Hyperledger Fabric, by varying the number of transactions (from 1 to 10000 transactions). This methodology was used on simple cash transfer applications, with three major functions: Create Account,

Issue Money, and Transfer Money. The Create Account function is used to create new users, while the other two functions issue and transfer money and are used, respectively, to issue money into an account and transfer money from one user to another. The results for this experiment showed that the Hyperledger outperforms Ethereum in all specified evaluation metrics, which are execution time, throughput, and latency, as shown in Figure 1.

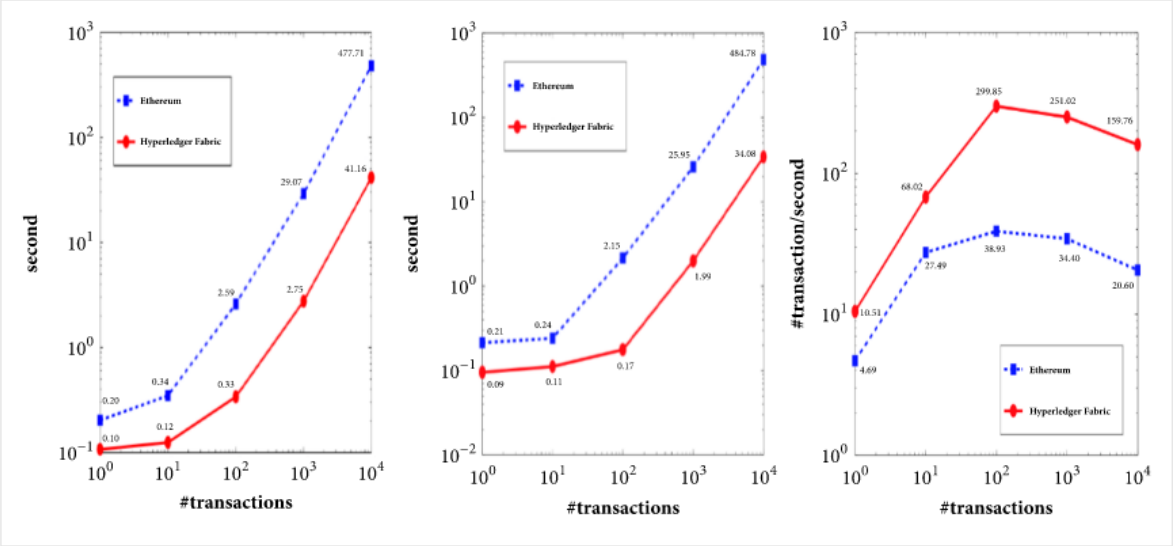


Fig 2.4 Execution time, latency, and throughput of Ethereum and Hyperledger Fabric, respectively.

Another recent experiment studied the scalability of three blockchain platforms, Hyperledger, Ethereum, and Parity by T. T. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K. Tan, (2017) and D. T. T. Anh, M. Zhang, B. C. Ooi, and G. Chen (2018). The scalability is analysed by setting the transaction rate at constant and changing both the number of users and the number of servers. The experiment showed that the throughput and latency of the Ethereum platform reduced almost linearly beyond 8 servers. On the other hand, the Hyperledger Fabric platform stops responding beyond 16 nodes due to the overhead of communication between nodes in the consensus protocol (see Figure 2).

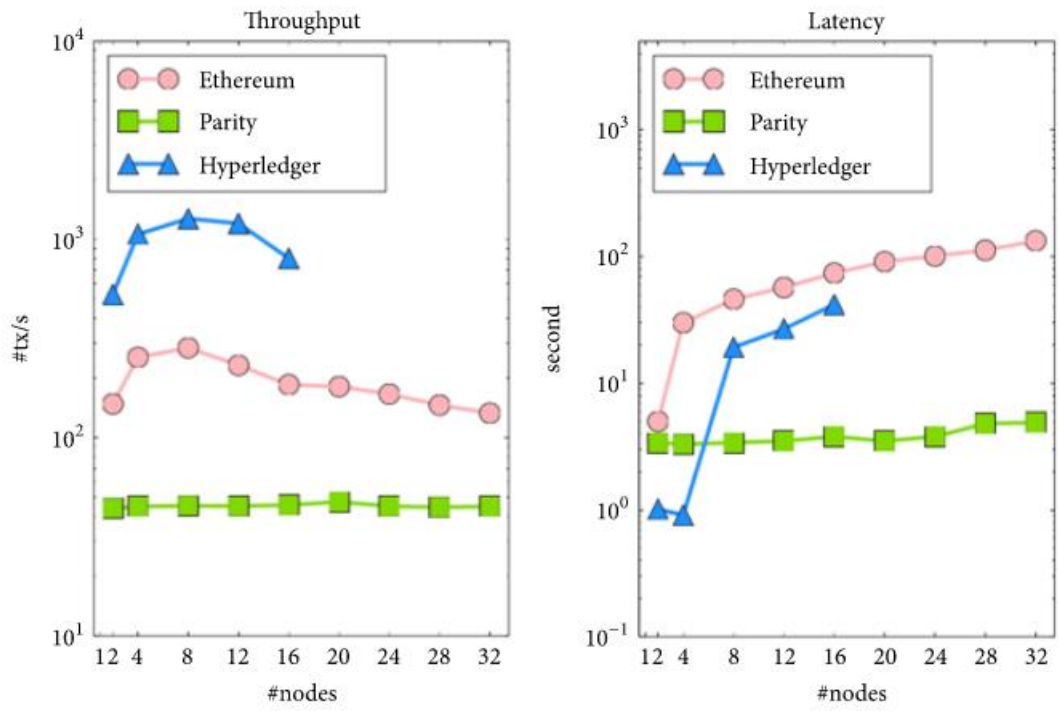


Fig 2.5 Showing Scalability for Hyperledger Fabric, Ethereum, and Parity

CHAPTER THREE

METHODOLOGY

This chapter covers the research design, source of data, population of the study, sample size and sampling technique, model specification, measurement of variables and data analysis technique.

3.1 Research Design

Ex-post facto research design will be used in the course of this research. The basis for this choice of design is because the study intends to use data that are in existence (Secondary data) already and there will be no effort to control or manipulate these existing data. The works of some authors (Fred Huibers, (2021), Distributed Ledger Technology and the Future of Money and Banking; Victor Gayoso Martinez, Luis Hernandez-Alvarez and Luis Hernandez Encinas (2020), Analysis of the Cryptographic Tools for Blockchain and Bitcoin; Abderahman Rejeb, Karim Rejeb and John G. Keogh (2021), Centralized vs. decentralized ledgers in the money supply process: a SWOT analysis), on some of the core elements of blockchain network technology will be used as the source of data on which ex-post facto design will be applied.

3.2 Sources of Data

The study will rely on secondary data. A thorough investigation of the previous literature was carried out using sources extracted from various academic databases. Ex-post facto design analysis based on an integrative literature review methodology was conducted to synthesize various research contributions and analysed relevant information related to centralized, decentralized and distributed ledgers in deep consonance with Blockchain Technology and its usefulness as an enabler of secured service delivery in the combat against financial crimes in the public and private sector.

3.3 Population

All the population of this research comprises of six (6) financial behemoths (JPMorgan, Citi Bank, Wells Fargo, US Bancorp, PNC, Fifth Third Bank and Signature Bank some of these banks are listed on the Nigerian Exchange Group as at 31st December 2020. It should be noted that as at the time of commencing this research none of the Nigeria Banks is using the blockchain network in its operation, except for CBN who is plaining to launch an Open-Source blockchain to run a digital currency pilot on October 1st, 2021 using the Hyperledger Fabric Blockchain, which has been criticised for not been able to provide the level of security offerings that the distributed ledger offers and its more expensive solution.

3.4 Sample size and Sampling Techniques

The sample size of this study are the six (6) financial institutions from the listed banking organizations on the NYQ and Nigerian Exchange Group using purposive sampling technique. The study purposively selected financial institutions that have been involved with uninterrupted business activities deployed by blockchain networks between 2017–2020. The sample size represents 75% of the population of those banks using blockchain technologies in one way or the other or as major operational core and backbone.

3.5 Model Specification

In sequence to the main objective of this study, which is to explore, examine and evaluate the applicability of blockchain technologies as a means and tool for curbing and preventing financial crimes which are normally perpetrated as a result of the present infrastructure configurations and industry-wide mode of operations of the banks, the clearing institutions and the regulator, which has led to the privatisation of profits and socialization of losses arising from the mismanagement, malpractices, fraudulent act and actual theft by an outsider (hackers) and staff of such institutions themselves. This study will adapt the model of Victor Gayoso Martinez, Luis Hernandez-Alvarez and Luis Hernandez Encinas (2020), in Analysis of the Cryptographic Tools for Blockchain and Bitcoin. In this research, the most elementary cryptographic concepts that are necessary to understand the fundamentals of blockchain technology will be reviewed. The main tool used for ensuring the integrity of information are the hash functions; the verification that a piece of information comes from the legitimate sender is carried out through digital signature schemes (some of them using elliptic curves) and Merkle trees. Thus, the concepts of hash functions, digital signatures, elliptic curves, and Merkle trees will be presented.

3.6 Method of Data Analysis

The data will be examined by using descriptive and panel regression analysis in order to meet the study's objectives. The Pearson’s Chi-Square will be use in this investigation. This is because it takes into account the variable characteristics of individual businesses. The rationale for this was because these methodologies will assist in determining and test the effect of the dependent variables on the independent variables, as well as demonstrating the degree of link between the variables in this study. The analysis will be directed by the hypothesis's described model. The heteroskedasticity test and Auto-Correlation

will be used to see if the data was multicollinear. The validity and reliability of the data will be further tested using the Hausman Specification, LM test, and Shapiro-Wilk W test for normality before regression analysis will be performed to evaluate the hypotheses presented.

The methodologies to be used to analysed the study's specific objectives are explained below. Because of their capacity to forecast the link between the variables, several strategies were applied. Following that, tables were utilized to present the results.

Objective One

The degree of impact that blockchain application used case has on the ease of conducting business in the Nigeria Public-Private Financial Space will be examined using regression techniques.

This objective will be achieved through the measurement of speed and timeliness of financial services deliveries by the Traditional Banking Institution which is controlled through corporate governance, and the Non-Financial Institutions that offers Banking Services.

Objective Two

It is more appropriate to examine the effect of blockchain adoption will have on the quick detection of fraudulent activities, prevention of it or total absence financial crimes in Nigeria, although it’s widely established that there’s no system without flaws. But this objective will be achieved through the measurement of reduction in crime index and the likelihood of its occurrence if Blockchain Technology is used to power financial service using regression techniques.

Objective Three

It is more appropriate to examine the effect of total rejection of its usage will impact on the value-add as a new normal way of securing financial assets of all sorts, using regression techniques. This objective will be achieved through the measurement of success rates index of companies who deployed it and those who are conservatives.

Objective Four

It is more appropriate to evaluate the need for over hauling of the resent banking systems – Banking is necessary and banks are not, Bill Gates (2004) This will conclude with an assessment of the scope and likelihood of monetary reform as a consequence of DLT applications by central banks using descriptive analysis of the global trends in conducting business using Information Technology Data-Driven Systems.

CHAPTER FOUR

4.0 PRESENTATIONS, ANALYSIS AND DISCUSSIONS ON FINDINGS

In this chapter, the researcher will review the most elementary cryptographic concepts that are necessary to understand the fundamentals of blockchain technology. Also, the Analysis and Conclusion from the Hypothesis will be presented and discussed. The main tool used for ensuring the integrity of information are the hash functions; the verification that a piece of information comes from the legitimate sender is carried out through digital signature schemes (Alice send a message to Bob), some of them using elliptic curves and Merkle trees. Therefore, the concepts of hash functions, digital signatures, elliptic curves, and Merkle trees are thus presented.

4.1. HASH FUNCTIONS

Hash functions are among the cryptographic primitives that have increased their relevance in recent years. It is important to note that such functions do not encrypt or decrypt messages. However, they are an indispensable tool for verifying data integrity, apart from other applications equally interesting. Hash functions can be defined as functions that are capable of transforming any block of binary data into another fixed-size binary block, Menezes, A.J.; van Oorschot, P.C.; Vanstone, S.A (1996); Paar, C.; Pelzl, J. Understanding Cryptography (2010). The result of such a transformation is called hash or digest. The first hash functions were proposed to be used in digital signature protocols with the goal to improve their efficiency, as signatures were constructed by using the digest of data elements instead of the whole elements. Being the hash a much shorter element, the protocol was more efficient since the calculations were simpler and less bandwidth was needed when sending the signed data.

In addition to this initial use, hash functions have been applied to other areas related, in general, to the protection of information and, in particular, to its integrity. Thus, they are also used to detect corrupted data, presence of viruses, etc.

From a mathematical point of view, hash functions are created using the concept of Trapdoor One-Way Functions (TOWF), which are functions defined between the sets X and Y

$$f: X \,!\, Y, \text{ with } f(x) = y$$

that fulfil the following conditions:

1. f is a unidirectional function, thus, from a computational standpoint, it must be easy to compute f (x) = y for all elements x ϵ 2 X but, at the same time, it must be very difficult to obtain $x = f^{-1}(y)$ for a given value y ϵ Y.
2. If additional information, known as trapdoor, is learned, then it must be feasible to calculate in polynomial time an element x ϵ X so that f (x) = y.

Thus, a hash function is a unidirectional function that is applied to a message m of variable size, where the message belongs to a certain set of messages, M, and provides a digest of the message with a fixed, predetermined bit size, n. Therefore, a hash function, h, can be described as follows:

$$h: M \rightarrow \{0, 1\}^n, \text{ with } h(m) = \varkappa$$

Since hash functions transform a message of any length into a collection of n bits, the number of possible hashes is much smaller than the number of different input messages. Consequently, there will always be different messages whose digests match.

4.1.1 Properties of Hash Function

Other important properties that these functions must fulfil are presented as follows:

1. **Bit dependency**: The hash of a message, $h(m) = m$, must be a complex function dependent on all the bits of the message, so that, if a bit of the message is changed, its hash must change, approximately, half of the bits.
2. **Preimage Resistance**: Given a hash h(m), it must be computationally difficult to get a message m so that h(m) = m. In other words, from a computational point of view, any hash function must be difficult to reverse. For an instance, if a hash function h produced a hash value z, then it should be a difficult process to find any input value x that hashes to z. – This property protects against an attacker who only has a hash value and is trying to find the input that digest an expected hash(es).
3. **Second Preimage Resistance:** Given a message m_1, it must be computationally difficult to find another message, m_2, where $m_1 \neq m_2$, with the same hash. That is to say, it must not be possible to find another message such that h(m1) = h(m2).
4. **Collision Resistance:** It must be computationally difficult to find two messages m_1 and m_2, $m_1 \neq m_2$, so that h(m1) = h(m2). In other words, for a hash function h, it is hard to find any two different inputs x and y such that h(x) = h(y). – Since, hash function is compressing function with fixed hash length, it is impossible for a hash function not to have collisions. This property of collision free only confirms that these collisions should be hard to find. – This property makes it very difficult for an attacker to find two input values with the same hash. – Also, if a hash function is collision-resistant then it is second pre-image resistant.

The Bit-Dependency Property allows guaranteeing the integrity of information, since, if any number of bits are modified, the result of the function will show a great difference between the original hash and the new hash, thus trial and error attacks are not feasible. On the other hand, it is worth mentioning that, despite being similar, the last two properties are actually are different. Second Pre-Image Property considers that one of the messages is known and tries to locate

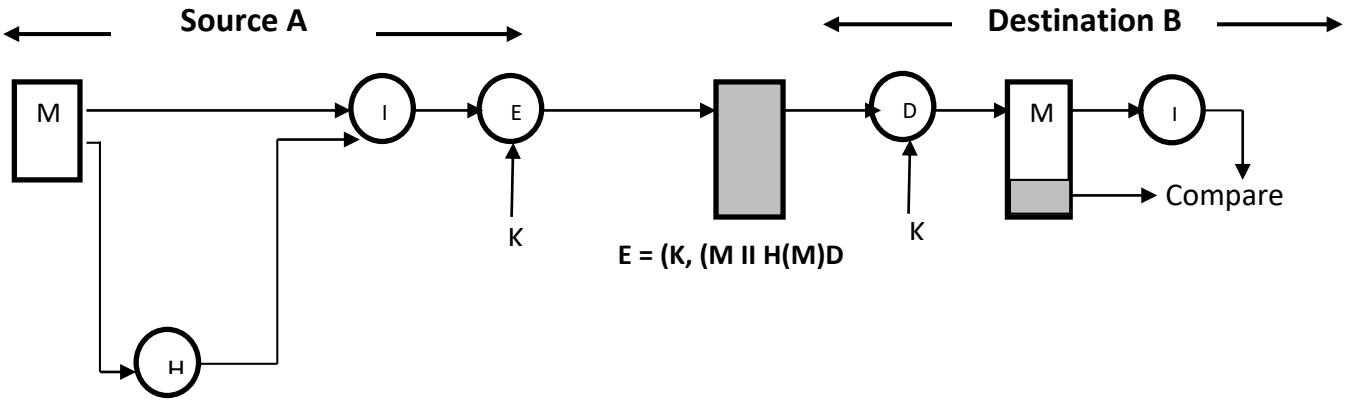
a different message with the same hash. In comparison, in Collision Resistance Property, no conditions are imposed on the messages. Based on the birthday paradox, collision resistance is a weaker condition than resistance to the second preimage. If a hash function is vulnerable to collision resistance, its use will no longer be recommended.

The compliance with the above properties guarantees, at least initially, that the functions that fulfil them are not vulnerable and prevent that, taking as input the hash of a message, the content of the message can be retrieved and that no one will be able to find another message with the same hash.

4.1.2 Application of Cryptographic Hash Function

Having established in the preceding paragraphs that the most important aspect of a hash is to ascertain data integrity, while ensuring that the bandwidth used in transmitting the message payload is efficient in the course of transfer, the following methods are how Cryptographic Hash Function is Applied in Transferring a message:

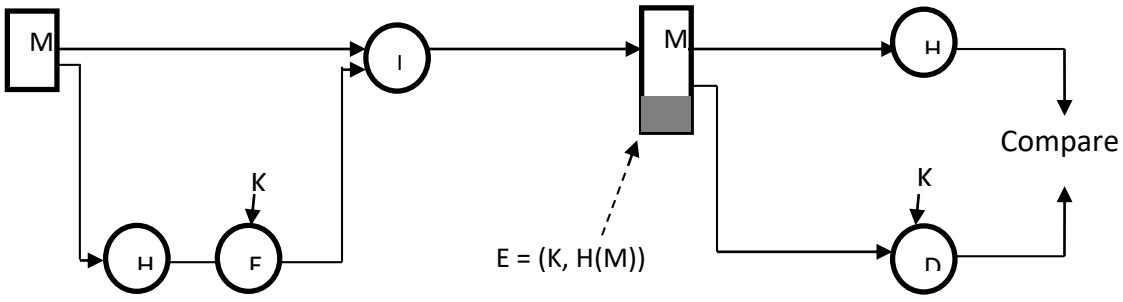
1. **Message Authentication:** Message authentication is a mechanism or service used to verify the integrity of a message. Message authentication assures that data received are exactly as sent (i.e., contain no modification, insertion, deletion, or replay). In many cases, there is a requirement that the authentication mechanism assures that purported identity of the sender is valid. When a hash function is used to provide message authentication, the hash function value is often referred to as a message digest.



Method A

Fig 4.1 Message plus concatenated hash code encrypted using symmetric encryption.

Because only A and B share the secret key, the message must have come from A and has not been altered. The hash code provides the structure or redundancy required to achieve authentication. Because encryption is applied to the entire message plus hash code, confidentiality is also provided. Only the hash code is encrypted, using symmetric encryption. This reduces the processing burden for those applications that do not require confidentiality.



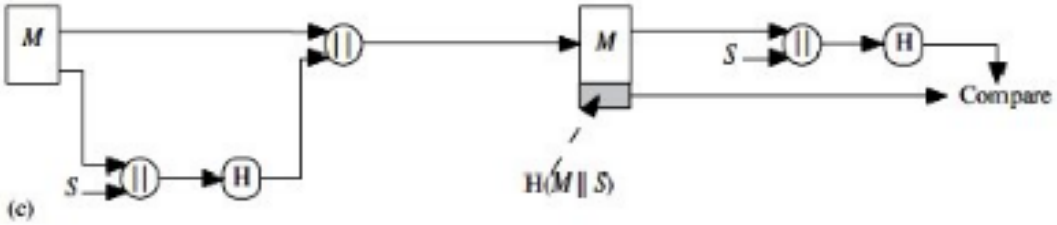
Method B

Fig 4.2 Only the hash code is encrypted using symmetric encryption. This reduces the processing burden for Applications do not need confidentiality.

It is possible to use a hash function but no encryption for message authentication. The technique assumes that the two communicating parties share a common secret value S. A computes the hash value over the concatenation of M and S and appends the resulting hash value to M. Because B possesses S, it can recompute

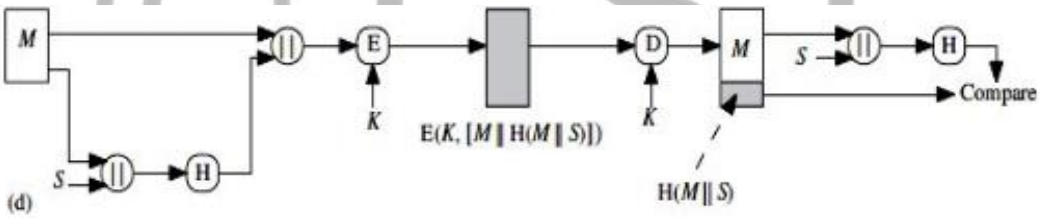
the hash value to verify. Because the secret value itself is not sent, an opponent cannot modify an intercepted message and cannot generate a false message.

Confidentiality can be added to the approach of method (c) by encrypting the entire message plus the hash code.



Method C

Fig. 4.3 No Encryption but Parties shared a Secret Value.



Method D

Fig. 4.4 Confidentiality is thus added by encrypting the message payload and the hash code.

4.1.3 Discussion on Cryptographic Hash Function Properties in Securing Financial Transaction

A hash function H accepts a variable-length block of data as input and produces a fixed-size hash value h = H(M) The principal object of a hash function is **data integrity**. A change to any bit or bits in M results, with high probability, in a change to the hash code. The kind of hash function needed for security applications in financial transaction is referred to as a cryptographic hash function, which is the key security feature of Bitcoin

on the Blockchain Network. A **cryptographic hash function** is an algorithm for which it is computationally infeasible (because no attack is significantly more efficient than brute force attack) to find either (a) a data object that maps to a pre-specified hash result (the one-way property) or (b) two data objects that map to the same hash result (the collision-free property). Because of these characteristics, hash functions are often used to determine whether or not data has changed. Therefore, in a typical financial transaction across a banking platform (not necessarily Banks), these cryptographic hash functions are the bedrocks to ensure that (a) a transactional process initiated by a buyer of a product or a user requesting a paid-service cannot be intercepted by a hacker (attacker) on the information super highway (i.e., the Blockchain Network) without knowing the Private Key and Public Key of the persons involved (b) that the Sender (or the Initiator of the process) is verified and not an imposter per se.

More commonly, message authentication is achieved using a message authentication code (MAC), also known as a keyed hash function. Typically, MACs are used between two parties that share a secret key to authenticate information exchanged between those parties. A MAC function takes as input a secret key and a data block and produces a hash value, referred to as the MAC. This can then be transmitted with or stored with the protected message. If the integrity of the message needs to be checked, the MAC function can be applied to the message and the result compared with the stored MAC value. An attacker who alters the message will be unable to alter the MAC value without knowledge of the secret key. Note that the verifying party also knows who the sending party is because no one else knows the secret key. Note that the combination of hashing and encryption results in an overall function that is, in fact, a MAC (Figure 4.3). That is, E (K, H(M)) is a function of a variable-length message M and a secret

key K, and it produces a fixed-size output that is secure against an opponent who does not know the secret key.

4.1.4 Requirements for Cryptographic Hash Function

Requirements	Description
Variable Input Size	H can be applied to a block of Data of Any Size.
Fixed Output Size	H produces Fixed-Length Output
Efficiency	$H_{(x)}$ is relatively easy to compute for any given 'x' therefore making both hardware and software implementations practical.
Pre-Image Resistant (One-Way Property)	For any given hash value 'h', it is computationally infeasible to find y, such that H(y) = h
Second Pre-Image Resistant (Weak Collision Resistant)	For any given block x, it is computationally infeasible to find $y \neq x$, such that H(y) = H(x)
Collision Resistant (Strong Resistant)	It is computationally infeasible to find any pair (x, y) such that H(y) = H(x)
Pseudo-randomness	Output of H meets Standard tests for pseudo-randomness

4.2 Digital Signature Functions in Data Security

Another important application, which is similar to the message authentication application, is the digital signature. The operation of the digital signature is similar to that of the MAC. In the case of the digital signature, the hash value of a message is encrypted with a user's private key. Anyone who knows the user's public key can verify the integrity of the message that is associated with the digital signature. In this case, an attacker who wishes to alter the message would need to know the user's private key.

The hash code is encrypted, using public-key encryption with the sender's private key (this provides authentication). It also provides a digital signature, because only the sender could have produced the encrypted hash code. In fact, this is the essence of the digital signature technique.

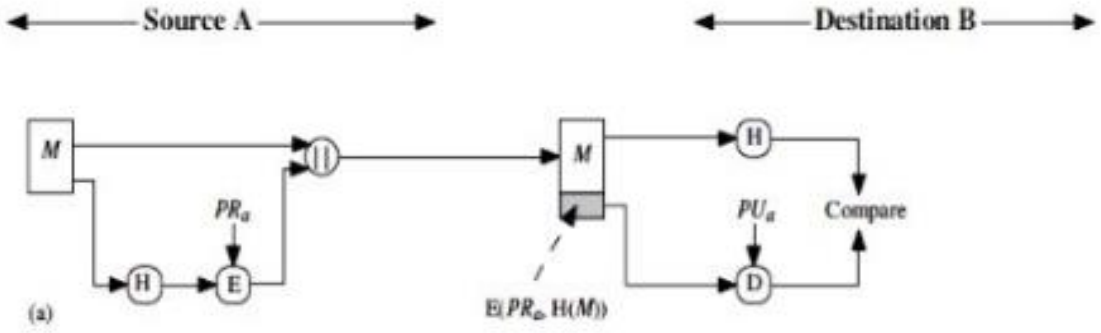


Fig. 4.5 The hash code is encrypted, using public-key encryption with the sender's private key (Authentication)

If confidentiality as well as a digital signature is desired, then the message plus the private-key-encrypted hash code can be encrypted using a symmetric secret key. This is a common technique.

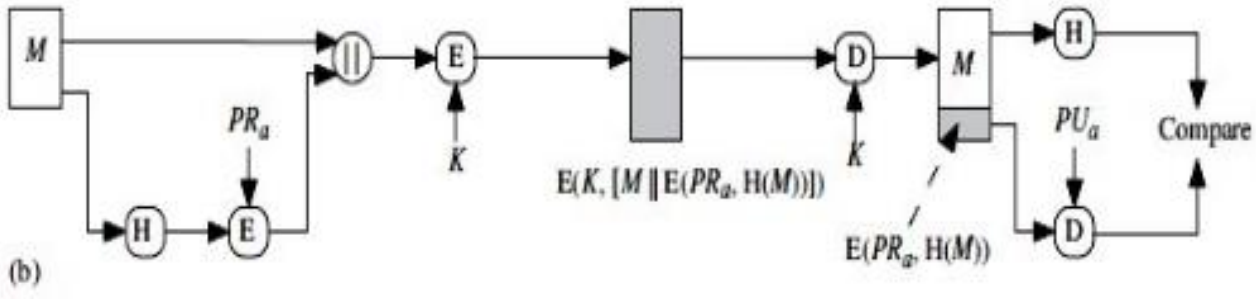


Fig. 4.6 The message plus the private-key-encrypted hash code are encrypted using a symmetric secret key.

4.2.1 DSA Operations

The DSA algorithm involves four operations: key generation (which creates the key pair), key distribution, signing and signature verification and the signing and verification will be discussed for the purpose of this research.

4.2.1.1 Signing:

A message m is signed as follows:

a Choose an integer k randomly from {1…q – 1}

b Compute r := (g^k mod p) mod q., in the unlikely case that r = 0, start again with a different random k

c Compute s := (k^{-1} (H(m) + xr)) mod q. in the unlikely case that s = 0, start again with a different random k

The signature is (r, s)

The calculation of k and r amounts to creating a new key per message. The modular exponentiation in computing r is the most computationally expensive past of the signing operation, but it may be computed before the message is known. Calculating the modular inverse k^{-1} mod q is the second most expensive part, and it may also be computed before the message is known. It may be computed using the extended Euclidean algorithm or using Fermat's little theorem as k^{r-2} mod q.

4.2.1.2 Verifying a Signature

Once there is a valid message m, the signature (r, s) can then be verified as follows:

a. Verify that 0 < r < q and 0 < s <q
b. Compute w := s^{-1} mod q.
c. Compute u1 := H(m) . w mod q.
d. Compute u2 := r .w mod q.
e. Compute v ;= (g^{u1} y^{u2} mod p) mod q.
f. The Signature is valid if and only if v = r.

4.2.1.3 Verifying the Correctness of the Algorithms

The signature scheme is correct in the sense that the verifier will always accept genuine signatures. This can be shown as follows:

First, since $g - h^{(p-1)/q} \bmod p$, it follows that $g^q \equiv h^{p-1} \equiv 1 \bmod p$ by Fermat's little theorem. Since $g > 0$ and q is prime, g must have order q.

The signer computes:

$S = k^{-1} (H(m) + xr) \bmod q$

Thus

$K \equiv H(m)s^{-1} + xrs^{-1}$

$\equiv H(m)w + xrw \pmod q$

Since g has order q we now have

$g^k \equiv g^{H(m)w} g^{xrw}$

$\equiv g^{H(m)w} y^{rw}$

$\equiv g^{u1} y^{u2} \pmod p$

Finally, the Correctness of DSA follows from

$R = (g^k \bmod p) \bmod q$

$= (g^{u1} y^{u2} \pmod p) \bmod q$

$= v$

4.2.1.4 Discussion on DSA Sensitivity to Security

With DSA, the entropy, secrecy, and uniqueness of the random signature value are critical. It is so critical that violating any one of those three requirements can reveal the entire private key to an attacker. Using the same value twice (even while keeping secret), using a predictable value, or leaking even a few bits of in each of several signatures, is enough to reveal the private key x.

This issue affects both DSA and ECDSA – in December 2010, a group calling itself ***fail0verflow*** announced recovery of the ECDSA private key used by Sony to sign software for the PlayStation 3 game console. The attack was made possible because Sony failed to generate a new random for each signature.

This issue can be prevented by deriving deterministically from the private key and the message hash, as described by RFC 6979. This ensures that is different for each and unpredictable for attackers who do not know the private key x.

In addition, malicious implementations of DSA and ECDSA can be created where is chosen in order to subliminally leak information via signatures. For example, an offline private key could be leaked from a perfect offline device that only released innocent-looking signatures.

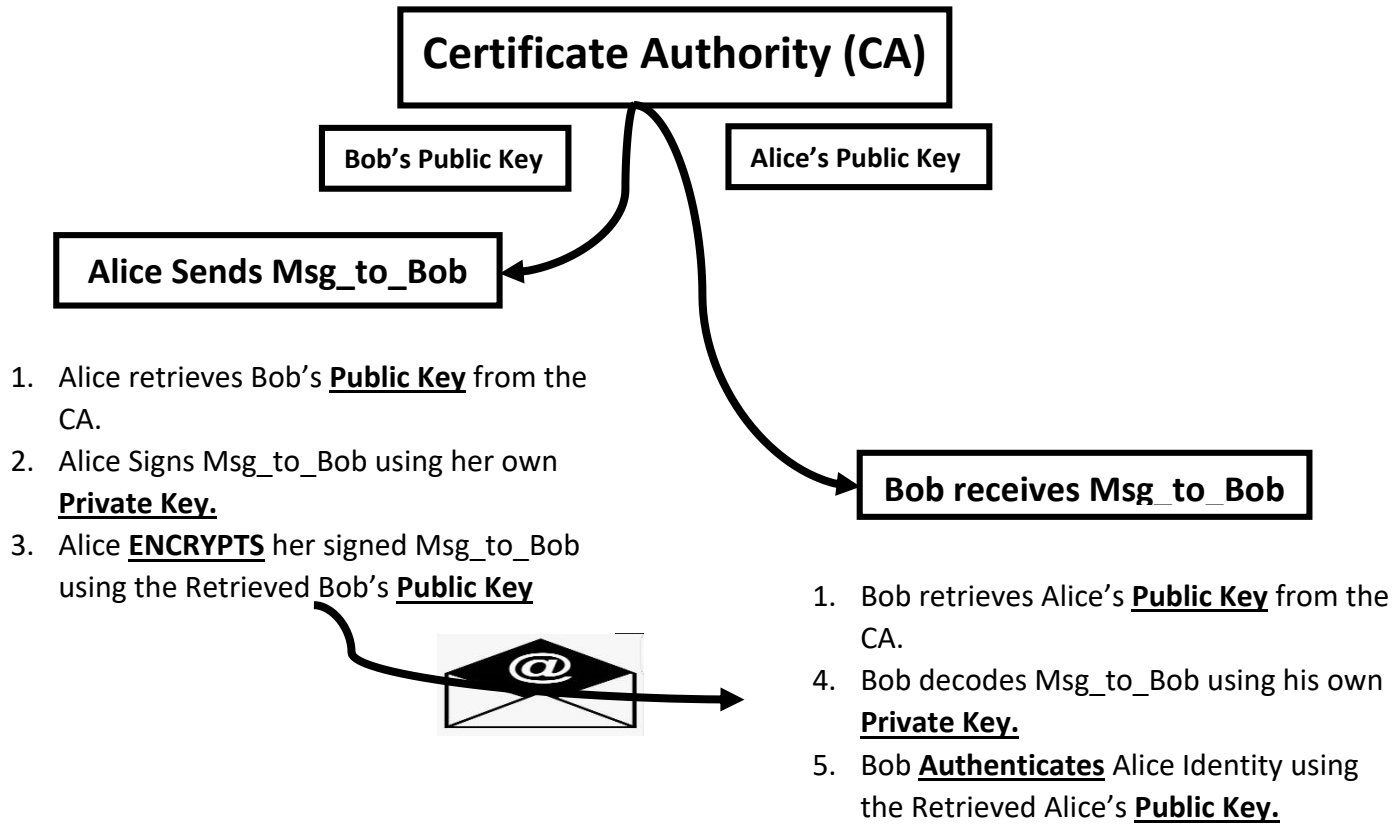


Fig 4.7 Public Key Infrastructure (PKI) Alice sends Message to Bob. Issuing Certificates and Encrypting the message using RSA Algorithm Established a Trusted Path.

4.3 Elliptic Curves

Based on the foregoing, elliptic curve signature algorithm will now be presented in this section in regards to its application and usefulness in the blockchain cryptographic functions, so that it is understood from mathematical point of view. From a mathematical perspective, an elliptic curve defined over a field F is a cubic, non-singular curve of genus one with at least one rational point. Most elliptic curves can be described as the set of points $(x, y) \in F \times F$ verifying the following equation, known as the non-homogeneous

Weierstrass equation: $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$,

where $a_1, a_2, a_3, a_4, a_6 \in F$.

An elliptic curve point is said to be singular if the partial derivatives of the curve equation are equal to zero at that point. Consequently, the curve is singular if it has at least a singular point, while it is non-singular if it does not have any singular point.

There is another way of representing the Weierstrass equation, and that is by using homogeneous variables, as expressed below, Menezes, A.J. (2006):

$$Y2Z + a1XYZ + a3YZ2 = X3 + a2X2Z + a4XZ2 + a6Z3.$$

This alternative expression is quite useful, as it allows defining a special point, which is called the point at infinity and is typically represented as O = [0 : 1 : 0]. The point at infinity cannot be obtained through the homogeneous form and is paramount when operating with the points of the curve. More specifically, for any point P on the curve, the point of infinity acts as the identity element in the point addition operation, guaranteeing that P + O = O + P = P. Figure 4.8 shows below the graphically how the addition of points P and Q produces point R when using an elliptic curve defined over the field of the real numbers.

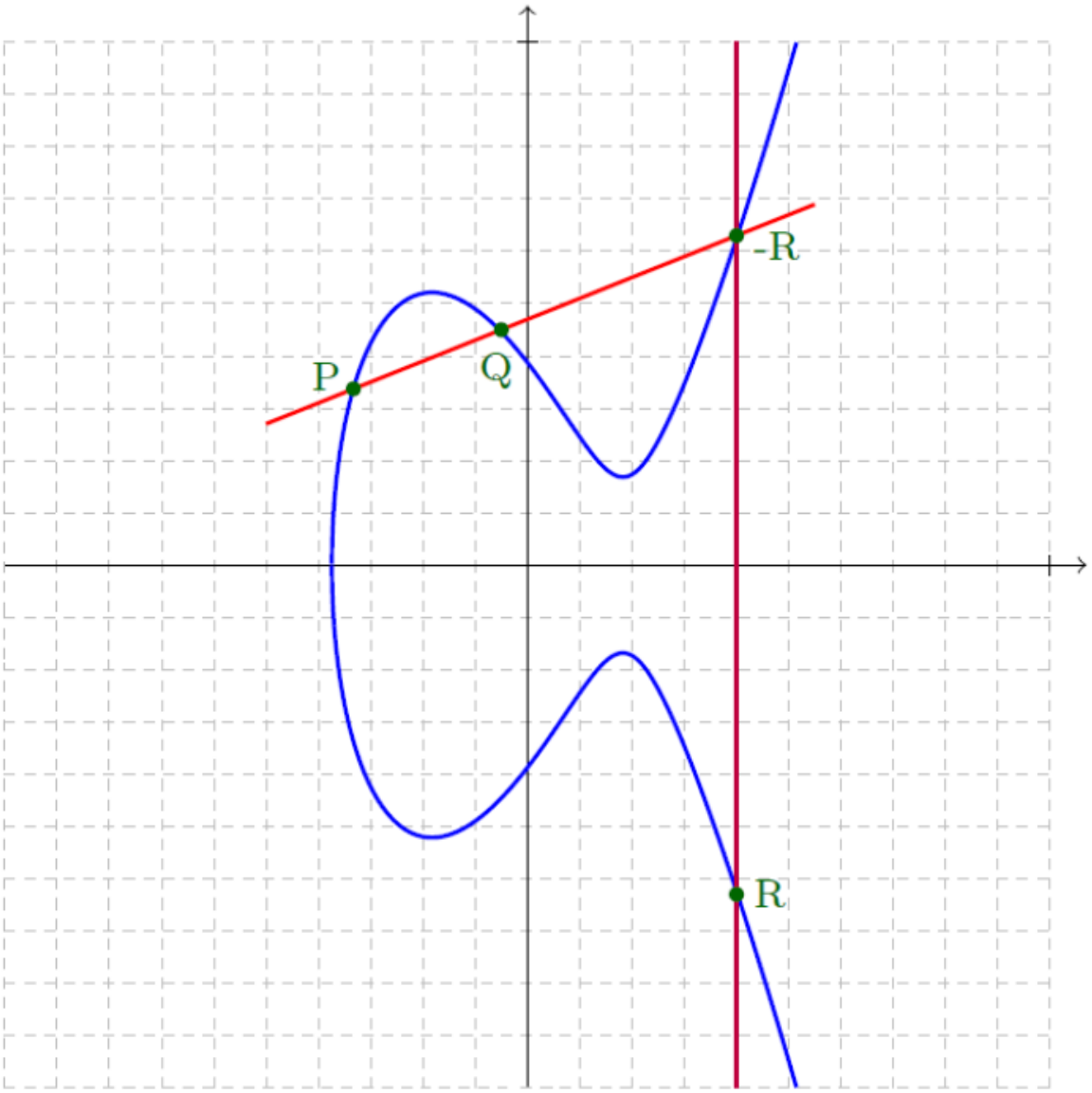


Fig. 4.8 Point addition on an elliptic curve defined over the field R

4.3.1 Elliptic Curves over Finite Fields

Most cryptosystems defined over elliptic curves use two special finite fields: prime fields F_p, where p is an odd prime number, and binary fields F_{2m}, where m can be any positive integer. Due to several reasons, including licence issues and some security weaknesses detected in curves over binary fields, prime fields are nowadays the best option when implementing elliptic curve cryptosystems (Bernstein, D.J., Lange, T. Curve25519, 2006; Lochter, M., Merkle, J. Elliptic Curve Cryptography (ECC) RFC 2010). In this type of curves, the term key

length, which is employed as a first approximation for classifying the cryptographic strength of the curves, must be interpreted as the number of bits needed to represent the prime number p.

An important concept that arises in finite fields is that of the order, which can be applied to both an elliptic curve and to its points: the order of an elliptic curve is the the number of points of the curve, while the order of a point P is the value n such that n _ P = O, where n _ P is the scalar multiplication of the point P by the number n (i.e., P + P + _ _ _ + P, where P appears n times).

A point G is said to be a generator if it is used for producing either all the points of the additive group defined by the elliptic curve or a subgroup of it. For security reasons, only generators whose order is a prime number are used in commercial deployments.

Given a curve and a generator, the term cofactor refers to the result of dividing the number of points of the curve by the order of the generator. Most standards only allow curves whose cofactor is either 1 or a small number, e.g., 2, 3, or 4.

Weierstrass Curves

The peculiarities of prime fields allow simplifying the non-homogeneous Weierstrass equation, obtaining in the process what is called the short Weierstrass form represented as $y^2 = x^3 + ax + b$, where $4a^3 + 27b^2 \equiv 0 \pmod{p}$.

Bernstein, D.J.; Lange, T. Explicit-Formulas Database. (2016) concluded that, as in the case of the general Weierstrass equation, the identity element of the short Weierstrass form is the point at infinity $\mathcal{O}$, while the opposite element of a point P = (Xp, Yp) is the point −P = (Xp - Yp). Adding two points P = (Xp, Yp) and Q = (x_Q, y_Q) such that P ≠ ±Q produces a point R = (xR, yR) whose coordinates can be computed as follows:

$$\left.\begin{aligned} x_R &= \lambda^2 - x_P - x_Q, \\ y_R &= \lambda\,(x_P - x_R) - y_P, \\ \lambda &= \frac{y_Q - y_P}{x_Q - x_P}. \end{aligned}\right\}$$

In comparison, when P = Q, it is necessary to use an alternative addition formula, thus, in this case, the point R = 2P obtained through the doubling operation has the following coordinates:

$$\left.\begin{aligned} x_R &= \lambda^2 - 2\,x_P, \\ y_R &= \lambda\,(x_P - x_R) - y_P, \\ \lambda &= \frac{3\,x_P^2 + a}{2\,y_P}. \end{aligned}\right\}$$

4.3.2 Elliptic Curve Digital Signature Algorithm (ECDSA)

In blockchain technology, the most widely used signature schemes are based on elliptic curves. National Bureau of Standards. ANSI X9.62, (2005) and Federal Information Processing Standards. FIPS 186-4. (2014) have been able to provide the Standard Framework for the adoption of ECC in the Blockchain Networks and Cross Platform Application. In this sense, the Elliptic Curve Digital Signature Algorithm (ECDSA) has become a standard.

The procedure for Alice to perform a digital signature with ECDSA is the following:

1. Alice must compute the hash of the message m in the usual way, h(m) = m.

2. She must generate a random number k, $1 \leq k \leq n - 1$ (where n is the order of the elliptic curve) and compute the point $k \cdot G = (x1, y1)$ and the value $r = x1 \pmod n$. If r = 0, then Alice must discard those elements and repeat this step.

3. Alice must determine k^{-1} (mod n) and calculate $s = k^{-1}(m + u \cdot r)$ (mod n).

4. The signature associated to the message m is the pair (r, s).

Once Bob has obtained the message m, the signature (r, s), and Alice's public key A, he must follow these steps if he wants to validate the signature:

1. Bob must compute by himself the hash h(m) associated to the message m.

2. Then, he must check that the values r and s belong to the range [1, n ─ 1].

3. Bob must compute the value s^{-1} (mod n) so he can calculate $z1 = m \cdot s^{-1}$ (mod n) and $z2 = r \cdot s^{-1}$ (mod n).

4. After that, he must determine the point of the curve $z1 \cdot G + z2 \cdot A = (x0, y0)$, where G is the generator of the curve.

5. Finally, Bob will accept the signature as valid if and only if r = x0 (mod n).

The validation process is formally correct given that, if we denote as $(P)_x$ the first coordinate of the point P € E, which can be checked by the following:

$$x_0 = (z_1 \cdot G + z_2 \cdot A)_x = \left(\hat{m} \cdot s^{-1} \cdot G + r \cdot s^{-1} \cdot A\right)_x = \left(\hat{m} \cdot s^{-1} \cdot G + r \cdot s^{-1} \cdot a \cdot G\right)_x$$
$$= \left((\hat{m} + r \cdot a)\, s^{-1} G\right)_x = (k \cdot G)_x = x_1 \pmod{n} = r.$$

In the particular case of bitcoin, the elliptic curve that is used is known as the Koblitz curve secp256k1, which is defined in the Standards for Efficient Cryptography, SECG-SEC 2 Version 2.0. (2010) and whose equation is $y2 = x3 + 7$.

This curve has
115, 792, 089, 237, 316, 195, 423, 570, 985, 008, 687, 907, 852, 837, 564, 279, 074, 904, 382, 605, 163, 141, 518, 161, 494, 337

points, considering as the base field the one with
115, 792, 089, 237, 316, 195, 423, 570, 985, 008, 687, 907, 853, 269, 984, 665, 640, 564, 039, 457, 584, 007, 908, 834, 671, 663

number of elements, which is a 256-bit integer representing the key size.

In the particular case of the keys used with the secp256k1 curve, for a user to generate his public–private key pair, he must randomly generate a collection of 256 bits and, following the protocol defined for the elliptic curves, derive the corresponding public key, which, in this case, has a length of 64 bytes as concluded by National Bureau of Standards. ANSI X9.62, (2005) and Federal Information Processing Standards. FIPS 186-4. (2014).

The public key is a point belonging to the secp256k1 curve, and thus it has two coordinates and can be represented as (x, y). Each of these numbers is encoded using the 256-bit big endian format, and the key is written down concatenating its value in hexadecimal format with the prefix 0x04. As a result, the key is encoded with 65 bytes.

If the so-called compressed format is used to represent the two coordinates of the point that constitute the public key, then only the x coordinate is encoded, since the y coordinate can only take two values, as the curve is symmetrical with respect to the abscissa axis. In this case, the public key would be written with the 32 bytes of the x coordinate together with a one-byte prefix (0x02 or 0x03, depending on the result of some computations using that coordinate). As a result, when using the compressed format, the public key is encoded with only 33 bytes.

4.4 **Hash Pointers and Merkle Trees**

4.4.1. Hash Pointers

As the researcher has already indicated, blockchains are chains of blocks of information where each block has an associated hash value. Those hashes are used for generating a data index. If each data block contains the hash of the block that has been previously added to the chain, a linked chain of blocks is obtained, where the hashes play the role of pointers.

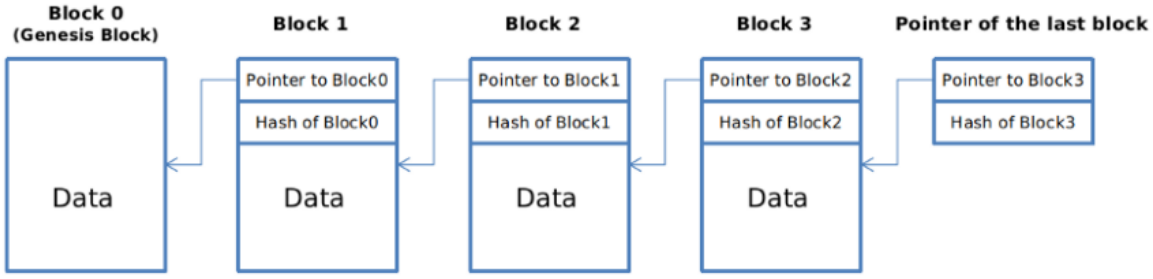


Fig 4.9 Link List also known as Blockchain

In this context, it is important to define a method that allows identifying if a certain block of information has been previously included in the chain. However, the direct search for information in lists linked by hashes is a computationally complicated task, which depends on the number of blocks included in the chain. Therefore, it is necessary to use a method that stores and manages hash pointers efficiently, and Merkle trees are one of the tools that help to achieve that goal, Merkle, R.C. (1985).

Basically, a hash pointer consists of two major parts:

- Pointer to where some information is stored
- Cryptographic hash of that information

  The pointer can be used to get the information; the hash can be used to verify that information hasn't been changed.

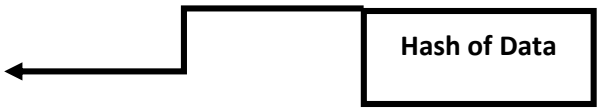


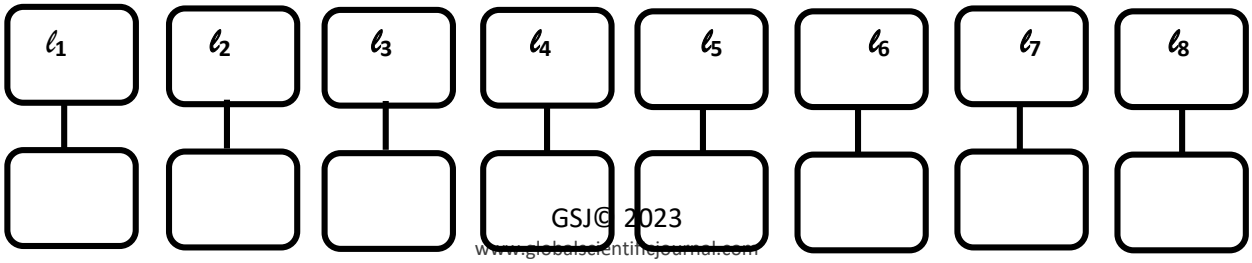
Fig. 4.10 Hash Pointer Component Parts.

4.4.2 Binary Trees and Merkle Trees

Before defining Merkle trees, it is necessary to define binary trees. A binary tree is a tree-shaped graph that contains a root, internal nodes, and leaves. If a descending order is considered, from the leaves to the root, each leaf has no predecessors and has only one child, each internal node has two parent nodes and a single child node, and the root node has two predecessors and no descendants.

In bitcoin's blockchain, a block of transactions is run through an algorithm to generate a hash, which is a string of numbers and letters that can be used to verify that a given set of data is the same as the original set of transactions, but not to obtain the original set of transactions. Bitcoin's software does not run the entire block of transaction data—representing 10 minutes' worth of transactions on average—through the hash function at one time, however, Bitcoin.org. (2020). Rather, each transaction is hashed, then each pair of transactions is concatenated and hashed together, and so on until there is one hash for the entire block. (If there is an odd number of transactions, one transaction is doubled and its hash is concatenated with itself.)

As an example, the following binary tree has eight leaves; three levels of internal nodes with eight, four and two nodes, respectively; and one root.



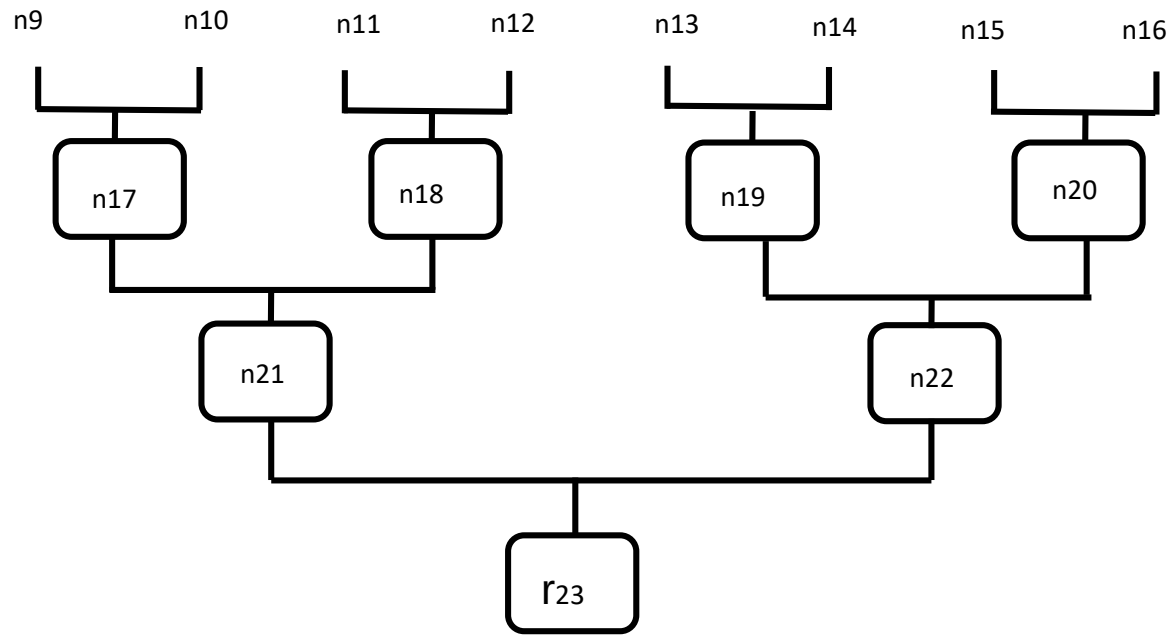
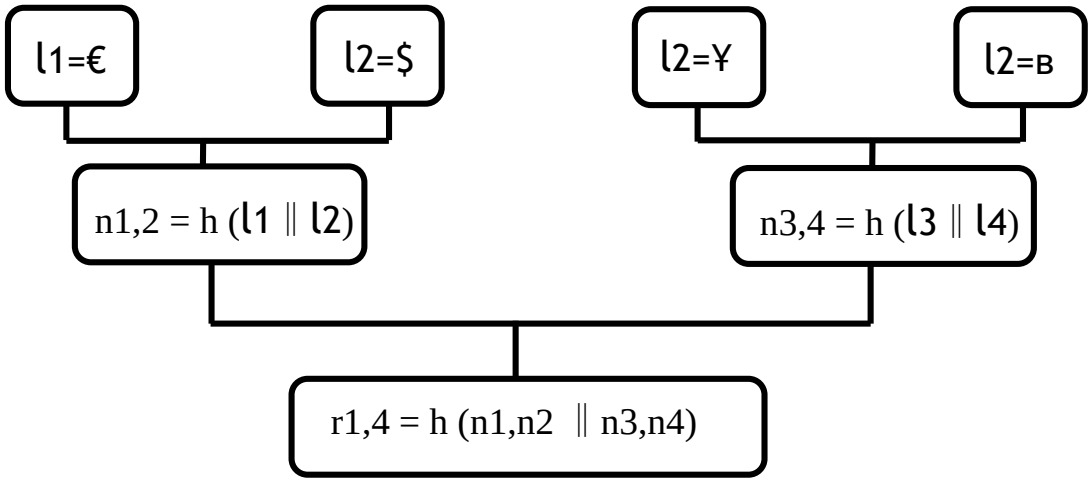


Fig 4.11 A Merkle Tree with root, node (hash) and leaves (Transactions).

Merkle trees are binary trees in which the leaves contain arbitrary data and the remaining nodes represent the output of a hash function, h, applied to the concatenation of the two preceding nodes.

As an example, the leaves of the following Merkle tree contain the characters that represent different currencies: euro (e), dollar ($), yen (Y) and bitcoin (B). For their part, the nodes are determined by calculating the output of the h function applied to the two previous nodes.



In this example, the value of the root, r1,4 = h (n1,2 ‖ n3,4) allows checking if certain data blocks were included in the tree represented by that root.

To verify if such a Merkle tree contains a certain value stored in one of its sheets, for example the bitcoin currency symbol, B, it is not necessary to know all the blocks of the tree, but a much smaller amount (approximately the logarithm of the number of leaves).

In fact, to prove that the value B was included in the Merkle tree with root r1,4, it is only necessary to know the value of the leaf l3 = ¥ and the value of the node n1,2 since the node n3,4 is computed taking as input the l3 and l4 elements. In the event that the calculated value did not match the root of the Merkle tree, r1,4, it can be stated that the value B is not part of the tree. This statement follows directly from the bit dependency property of hash functions.

Thus, it is possible to manage the integrity of the information in a blockchain if the value of the root of the Merkle tree that is associated with such data is included in the data blocks of the chain. It is not necessary, therefore, to add the values of all the data, which reduces the amount of information to be included.

4.5 Analysis, Findings and Discussion on Test of Hypothesis

As stated earlier in the course of this research work, efforts will be made to established the need for the adoption of Blockchain Technology (Distributed Network Architecture – with No Single Point of Failure and with great features of Immutability) into the Mainstream Business and Commercial Activity in Nigeria viz-a-viz the existing VISA Network (Trusted Third Party Centralized Network – with Single Point of Failure and Prone to attacks).

Considering a population of 20 number of Blockchain Transaction Per Second (TPS) and Visa ranging from the minimum of 7 to 20 of Blockchain and 380byte of Visa to 1024byte Transaction Per Second (TPS), a Systematic Sampling Selection of Size (4) four and list the possible Sample are as follows:

Solution 1

Blockchain TPS of:

7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45 respectively

Systematic Selection is given as:

$K = N/n = 20/4 = 5$

Assuming we choose 7 first, 11, 13, 15 and 21 respectively.

Solution 2

TPS – Visa Byte

380, 390, 400, 410, 490, 510, 710, 610, 800, 900, 1024, 990, 680, 950, 970, 430, 460, 550, 1000 and 420 as well.

Assuming we choose 380 first, 390, 510, 800 and 1024 as well.

The Analysis to determine the degree of impact that Blockchain Application Used Case will have on the ease of conducting business in the Nigeria Public/Private Financial Space will be examined using Pearson Correlation Coefficient, while the Chi-Square is a non-parametric probability distribution analysis will be used to determine whether there's any significant effect of blockchain adoption will have on the quick detection of fraudulent activities.

The formular for Pearson correlation is given as follows:

$$r = \frac{\sum (Xi - \bar{X}i)(Yi - \bar{y}i)}{\sqrt{\sum (Xi - \bar{X}i)^2 \sum (Yi - \bar{y}i)^2}}$$

r = Correlation Coefficient

xi = values of the x – variable

$\bar{X}i$ = mean of the values in a sample

Yi = variable

$\bar{y}i$ = mean of the values of the variable

x	(Xi - $\bar{X}$i)	(Xi - $\bar{X}$i)^2	y	(Y – $\bar{y}$)	(Y – $\bar{y}$)^2	∑ (Xi - $\bar{X}$i) (Yi – $\bar{y}$i)
7	-6.4	40.96	380	-240.8	-57,984.64	-1,541.12
11	-2.4	5.76	390	-230.8	-53,268.64	5539.2
13	-0.2	0.16	510	-110.8	-12,276.64	-44.32
15	2.6	6.76	800	179.2	32,112.64	465.92
21	7.6	57.76	1024	403.2	162,570.24	3064.32
67	1.2	111.4	3104	0.0	71,152.96	7,484

$$\bar{X}i = \frac{7 + 11 + 13 + 15 + 21}{5} = \frac{67}{5} = 13.4$$

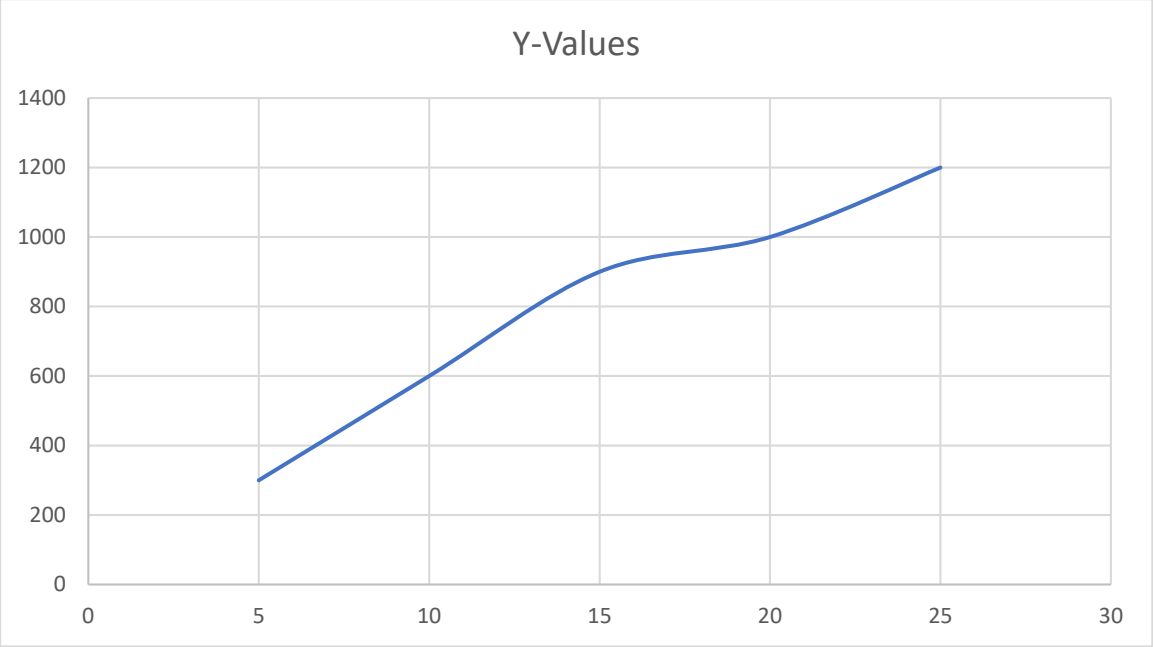
$$\bar{y} = \frac{380 + 390 + 510 + 800 + 1024}{5} = \frac{3104}{5} = 620.8$$

$$r = \frac{7572.64}{\sqrt{111.4 \times 71,152.96}} = \frac{7572.64}{\sqrt{7,926,415.816}}$$

$$= \frac{7572.64}{2815.39} = 2.6$$

The result from the above data analysis is 2.6, which indicate that there is strong correlation between the variable of interest (x and y) between the Blockchain and the Visa Byte TPS, which also implies that Blockchain Application will have strong impact of conducting business activities in Nigeria Financial Sector of the economy through the Internet.

Fig. 4.12 Showing the Graphical Illustration of Correlation of x and y



SOLUTION 2: Chi-Square $X^2 = \frac{(oi - ei)^2}{\epsilon i}$

oi = observed values

ϵi = expected values

Chi-Square Analysis for the Blockchain Data

Oi	ϵi	Oi – ϵi	$(Oi - \epsilon i)^2$	$(Oi - \epsilon i) / \epsilon i$
7	13.4	-6.4	40.96	3.057
11	13.4	-2.5	6.25	0.466
13	13.4	-0.4	0.16	0.012
15	13.4	1.6	2.56	0.191
21	13.4	7.6	57.76	0.567
				4.401

Test of Hypothesis

Ho: There is Significant effect in the adoption of blockchain to manage business in Nigeria Financial Sector.

Hi: There is Significant No effect in the adoption of blockchain to manage business in Nigeria Financial Sector.

Decision Rule

Reject Ho if X^2 calculated is greater than X^2 tabulated at 5% and 1% level of significant, with the degree of freedom (n – 1), otherwise accept Ho. Therefore, if Chi-square calculated is lesser than Chi-Square Tabulated and Conclude that there's significant effect in the adoption of blockchain in Nigeria Financial Sector.

Critical Region

Since the hypothesis of interest which Ho observed and expected frequency of blockchain adoption has no significant effect versus Hi; observed and expected frequency of blockchain adoption has significant effect from the X^2 table with (n – 1) = (5 – 1) = 4 degree of freedom. The critical value at 5% and 1% Level are X^2 tab = X^2 = (4., 0.05) = 9.49, X^2 tab = X^2 = (4., 0.01) = 13.3

CONCLUSION

Thus, we cannot reject the Ho (the null hypothesis in favour of the Hi and conclude that there is a significant effect in the adoption of blockchain at the 5% and 1% level of significant, Here X^2 cal < X^2 tab i.e. X^2 Calculated is less than the X^2 tabulated.

CHAPTER FIVE

CONCLUSIONS, SUMMARY AND RECOMMENDATIONS

5.1 Conclusions

Throughout this research work, the main cryptographic tools related to the security and reliability of blockchain which makes it suitable for combating and curbing financial crimes and other illicit acts are presented: hash functions, digital signatures, elliptic curves, and Merkle trees. Digital signatures made the proving of the authorship of a document possible and guaranteeing its integrity as well. The digital signature algorithm used by many blockchain technologies is ECDSA, a standard that uses elliptic curves. Among all the curves that can be used, secp256k1 has been selected by many implementations. SECP256K1 is a standard elliptic curve that uses 256-bit keys, a strength level similar to the AES algorithm. It should be noted that the choice for using secp256k1 is because it allows for efficient computation and was constructed in a special non-random way, while other commonly used curves have a random structure.

Hash functions appear in several places when dealing with blockchains. On the one hand, they are used as part of the digital signature algorithms. On the other hand, hash functions play an important role in the implementation of Merkle trees, a concept that allows efficiently checking if a certain block is present in a blockchain.

Through the combination of the aforementioned elements, it has been possible to create blockchain, a reliable technology with a promising future that it will be almost impossible to commit a financial crime in Nigeria if blockchain technology is adopted.

The Covid-19 pandemic outbreak in late 2019 and how it ravaged global economic activities by 2020 and still rampant with news of a delta variant lately, and the medical response which bring about ‘contactless’ socio-economic

activities and digital payments, tele-working, virtual classroom and of course the rise in crypto-business (even with all the official skepticism and denials), the blockchain technology is the only likely direction that can give the much needed impetus to sail through the current global socio-economic malaise.

5.2 Contribution to Knowledge

The main contribution of this thesis is to assert axiomatically that the applications of blockchain are not limited to cryptocurrency alone, it can be use in the financial applications by deploying it to combat financial crimes and other illicit acts as a result of its immutability features, and can also be used in non-financial applications, such as public services, reputation systems, security, and Internet of Things (IoT).

5.3 Recommendations

The following recommendations are made by the researcher based on the findings in the course of this research work:

1. Patrick Tiquet, Director of Security & Architecture at Keeper Security (2021) said he checks in to the ‘dark-web’ regularly, because it’s important for him to be on top of what’s happening in the hacker’s underground world. “He uses the dark web for situational awareness, threat analysis and keeping an eye on what’s going on,” he said “I want to know what information is available and have an external lens into the digital assets that are being monetized – this gives us insight on what hackers are targeting.”

   If you find your own information on the dark web, there’s precious little thing you can do about it, but at least you’ll know you’ve been

compromised. Bottom line: If you can tolerate the lousy performance, unpredictable availability, and occasional shock factor of the dark web, it's worth a visit. Just don't buy anything there.

Therefore, our Financial and Security Auditors, System Analysts, Cyber Security Professional and Personnel of the Agencies (like EFCC and ICPC) should as a matter of urgency commence the training of their various personnel in the Cyber-Space Security and Advance Information and Communication Skills and Techniques that would keep them at least a step ahead of crimes committed through the open web and the dark web at large – You can fight what you don't know.

2. Though mutual regulatory understanding of the technology as its still nascent is much needed; firms should collaborate with lawmakers and policymakers to create a solid regulatory framework—and perhaps look at leveraging policymakers' experimental facilities. The Nigeria Exchange Group can be encouraged to revisit their initial plans to provide Security Mechanism for the Blockchain Network and Crypto-Business as a whole.

3. Companies should look at creating an ecosystem of partners in order to derive maximum value from this collaborative technology.

4. The Covid-19 Pandemic has created the opportunity for enablement of wide range Cloud Services as a new strategy for giving access to employees to work from home for their enterprises. There is currently a surge in the demands for virtual cloud-based solution platforms. And as a result, a direct increase in the demand for Software-as-a-Service (S-a-a-S) across industries to ensure the continuity and smooth running of

operational and management activities. Blockchain-as-a-Service is an Ideal Solution to the Nigeria Small and Medium Scale Enterprises challenges that are associated with Infrastructural Acquisition or Development. SME's implementation of the distributed ledger-based services will be useful in the areas of safeguarding digital entities, authenticating human identities and increasing demand for B-a-a-S Products and Services.

5. The Banking, Financial Services and Insurance Institutions and Information Technology Companies in Nigeria should commence the adoption of cryptographic ledger solutions to combat the rise in Identity and Data Theft Incidence; Clearing and Settlements, trade finance platforms, digital identity verification exercises, credit reporting and of course cross-border transactions. In a recent report of Business Insider Magazine June 2021, India's largest public sector bank, the State Bank of India (SBI), along with ICICI Bank, Kotak Mahindra, Axis Bank, and 11 others have formed a new company called the **Indian Banks' Blockchain Infrastructure Company Private Limited (IBBIC)** that will be at the helm of this transformation.

   The move is expected to eliminate paperwork, reduce transaction processing time, and offer a secure environment. Moreover, it could be a boon for medium and small-scale enterprises (MSMEs). Using blockchain to issue Letter of Credits would potentially solve issues even elemental fraud like the issuance of two LCs on a single invoice can be easily prevented with the help of this blockchain technology. And the process time of traditional LC of four days would be reduced to four hours, the report said.

   This is a right step in a right direction, our CBN and other Major Banks should be doing same – not this frightens stance!

6. Per Fortune Business Insights report, the worldwide global market for blockchain is forecast to witness a Compound Annual Growth Rate (CAGR) of 56.1% between 2020 and 2027 and reach $69.04 billion. Further, growing usage of distributed ledger technology and rapid migration of workloads to cloud by enterprises are expected to drive the demand for blockchain as a service (BaaS) solution. Per a Mordor Intelligence report, BaaS market is projected to witness a CAGR of 15.2% between 2020 and 2025 and reach $982.8 billion. With the foregoing, it will be suicidal to deny our teeming youthful population the chance to explore their opportunities in these global arrangements. The Youth should be encouraged to participate fully in the global blockchain business, while an attempt should be made to put some checks and balance measures in place.

   Regulates, don't prohibit – Vice President Prof. Yemi Osinbajo, (2021)

7. The Rise in Digital Transformation has also led to the rise of various threats and cyberattacks globally. Nigeria has its own fair share in this menace and it tends to be unabated, even as EFCC has been making efforts to prosecute offenders. Unfortunately, there is skill shortage – lack of skilled professionals to overcome the situation and other risk factors. Therefore, the adoption of a robust policy on curriculum developments in our institutions of learning, including the Secondary Schools that will enable early exposure to IT-Skills in Cybersecurity and Industry Base Certifications for Personnel across organizations should be introduced. If this is not addressed timely, the adoption of the Blockchain Technology into the mainstream business is likely to be stagnant for more few years to come.

References

Abderahman Rejeb, Karim Rejeb and John G. Keogh (2021), Centralized vs. decentralized ledgers in the money supply process: a SWOT analysis. Pg. 4 - 28

Ajibola Bola (Prince), (2006) "Restitution: an alternative solution to the corruption issue", Paper presented at the Nigerian Institute of Town Planners, August 9, 2006, at Airport Hotel, Ikeja.

Amazon Web Services (2020) https://aws.amazon.com/blockchain/what-is-hyperledger-fabric/. Accessed August 20, 2020.

American National Standard Institute – ANSI, (2005), Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), National Bureau of Standards. ANSI X9.62. 2005. Available online: https://standards.globalspec.com/std/1955141/ANSI%20X9.62. Accessed 27th June 2020.

Andrew Arnold, (2019), 4 Promising Use Cases of Blockchain in Cybersecurity., https://www.forbes.com/sites/andrewarnold/2019/01/30/4-promising-use-cases-of-blockchain-in-cybersecurity/?sh=21aca823ac32. Accessed August 14, 2020.

B. Koteska, E. Karafiloski, and A. Mishev, (2017) "Blockchain implementation quality challenges: a literature review," in *Proceedings of the 6th Workshop on Software Quality Analysis, Monitoring, Improvement, and Applications (SQAMIA '17)*, vol. 1938, September 2017.View at: Google Scholar

Bamidele Samuel Adesoji (2019), Report on Nigeria Deposit Insurance Commission. https://nairametrics.com/2019/08/02/banks-lost-n15billion-to-fraud-cyber-crime-in-2018/#:~:text=The%20Nigerian%20banking%20industry%20lost%20N15.&text=The%20fraud%20cases%3A%20According%20to,fraud%20cases%20amounting%20to%20N12. Accessed, August 12, 2020

Bank of Canada, (2020) Digital Currencies and Fintech. https://www.bankofcanada.ca/research/digital-currencies-and-fintech/. Accessed August. 12, 2020.

Bitcoin.org. "Frequently Asked Questions." Accessed June 25, 2021.
BlockStack (2016) Proposal to use blockchain technology to decentralise the DNS and make it more secure. https://dig.watch/updates/proposal-use-

blockchain-technology-decentralise-dns-and-make-it-more-secure. Accessed 14th February 2020

Bureau of Public Procurement (2019) Annual Reports. https://dailypost.ng/2019/09/08/fg-reveals-contracts-fashola-amaechi-others-inflated-n27bn/. Accessed on 24th July, 2020.

Business Insider India, (2021) SBI, HDFC, ICICI and other Created a Blockchain Company. https://www.businessinsider.in/cryptocurrency/news/sbi-hdfc-icici-and-12-others-banks-are-joining-forces-to-use-blockchain-to-power-letters-of-credit-a-move-that-could-be-a-boon-for-msmes/articleshow/83570874.cms. Accessed August 9th 2021.

Capgemini's Digital Transformation Institute (2016), https://www.capgemini.com/news/consumers-set-to-save-up-to-sixteen-billion-dollars-on-banking-and-insurance-fees-thanks-to/. Accessed August 21, 2020

Central Bank of Nigeria, (2004), A review of Economic and Financial Crimes Legislation. (A paper presented at Legal Services Division of the CBN In-House Seminar), 26th November, 2004.

Coindesk (2019) Millions in Crypto is crossing the russia-china border daily. Tether is king https://www.coindesk.com/business/2019/07/30/millions-in-crypto-is-crossing-the-russia-china-border-daily-there-tether-is-king/. Accessed in August September 1st 2019

Coindesk (2021) Thriving Under Pressure: Why Crypto Is Booming in Nigeria Despite the Banking Ban https://www.coindesk.com/markets/2021/07/06/thriving-under-pressure-why-crypto-is-booming-in-nigeria-despite-the-banking-ban/. Accessed on August 8th, 2021.

D. T. T. Anh, M. Zhang, B. C. Ooi, and G. Chen, (2018) "Untangling Blockchain: A Data Processing View of Blockchain Systems," *IEEE Transactions on Knowledge and Data Engineering*, 2018.

DMS TEAM, (2015) The Disadvantages of Traditional Information Systems, http://www.decisionmanagementsolutions.com/14831/. Accessed August 21, 2020

E. A Owolabi (2007) Corruption and financial crimes in Nigeria: Genesis, trend and consequence. http://citeseerx.ist.psu.edu.viewdoc/download?doi=10.1.1.590.2899&rep=rep1&type=pdf. Accessed on November, 2020

E. Kokoris-Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford, (2016) "Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing," 2016.View at: Google Scholar

Eigen, Peter, Chairman, Board of Directors, (2004) Comments on T. I. Report on the Corruption Perception Index, Transparency International, Report on CPI, 2004

Ekpenkhio, S. A. (2003), "Public Procurement Reforms; The Nigeria Experience": A paper presented during Regional Workshop on Procurement Reforms and Transparency in Procurement for Anglo-phone African Countries, Tanzania, l6th January, 2003.

Federal Bureau of Investigation, (2015), Ross Ulbricht, the Creator and Owner of the Silk Road Website, Found Guilty in Manhattan Federal Court on All Counts. https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/ross-ulbricht-the-creator-and-owner-of-the-silk-road-website-found-guilty-in-manhattan-federal-court-on-all-counts. Accessed August. 31, 2020.

Federal Government of Nigeria, (2000) The Corrupt Practices and Other Related Offences Act 2000.

Federal Reserve Bank of Philadelphia, (2020) Central Bank Digital Currency: Central Banking for All? Page 3. Accessed August. 21, 2020.

Fred Huibers, (2021), Distributed Ledger Technology and the Future of Money and Banking, pg. 12, 14, 16, 28 -68

Frutos, N. D. (2006), Financial Times Online, U.K., 14th August, 2006.
Government of Nigeria, (1995), Advance Fee Fraud and Other Related Offences Act, 1995.

Government of Nigeria, (1995, Money Laundering (Prohibition) 2001 and 2004), Act, 1995, 2001 and 2004.

Government of Nigeria, (2002), Economic and Financial Crimes Act, 2002

Government of Nigeria, (2004), Economic and Financial Crimes Commission (Establishment) Act 2004

Gray, Cheryl W. and Daniel Kaufmann, (1998) "Corruption and Development", Finance and Development, March 1998

H. Sukhwani, J. M. Martínez, X. Chang, K. S. Trivedi, and A. Rindos, (2017) "Performance modelling of PBFT consensus process for permissioned blockchain network (hyperledger fabric)," in *Proceedings of the 36th IEEE International Symposium on Reliable Distributed Systems (SRDS '17)*, pp. 253–255, September 2017.View at: Google Scholar

I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, (2015) "Bitcoin-NG: A Scalable Blockchain Protocol," 2015.View at: Google Scholar

I. Kocsis and A. Klenik, (2016) "Towards Performance Modelling of Hyperledger Fabric". View at: Google Scholar

ICPC, (2006) About ICPC; A publication of the Education Department of the ICPC, Abuja, 2006.

International Monetary Fund, (2004) "Fighting Dirty Money", A Survey by IMF, August 9, 2004, pg. 242-244

Imran Khan Azeemi, Mike Lewis, Theo Tryfonas, (2013) Migrating to The Cloud: Lessons and Limitations of 'Traditional' IS Success Models. https://www.sciencedirect.com/science/article/pii/S1877050913000781. Accessed August 27, 2020

International Monetary Fund, (2000) Economic Issues: Improving Governance and Fighting Corruption in the Baltic and CIS Countries, July 2000, p.3.

J. Behl, T. Distler, and R. Kapitza, (2014) "Scalable BFT for multi-cores: actor-based decomposition and consensus-oriented parallelization," in *Proceedings of the 10th USENIX Conference Hot Topics in System Dependability*, 2014.View at: Google Scholar

J. Rubin, (2015) "BTCSpark : Scalable Analysis of the Bitcoin Blockchain using Spark," pp. 1–14, 2015.View at: Google Scholar

Jake Frankenfield, (2019), Silk Road (Website), https://www.investopedia.com/terms/s/silk-road.asp. Assessed on 10th September, 2020.

James Manyika, Jacques Bughin, and **Jonathan Woetzel, (2016)** Digital Globalization: The New Era of Global Flows. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows**.** Accessed on November, 13th 2020.

Joseph Bonneau, (2017), "Hostile Blockchain Takeovers." Cornell Tech Blockchains Workshop, http://jbonneau.com/presentations.html. Assessed on 19th September, 2020.

Justice Emmanuel O. Ayoola, (2005) "Corruption in Nigeria: the way forward", Paper delivered at the 50th anniversary of Ilesha Grammar School, Dec. 17th, 2005.

K. Croman, C. Decker, I. Eyal et al., (2016) "On Scaling Decentralized Blockchains," *International Financial Cryptography Association*, vol. 1, pp. 1–31, 2016.View at: Publisher Site | Google Scholar

K. Suankaewmanee, D. T. Hoang, D. Niyato, S. Sawadsitang, P. Wang, and Z. Han, (2017) "Performance Analysis and Application of Mobile Blockchain," pp. 1–6, 2017.View at: Google Scholar

Katharina Buchholz (2021) How Common is Crypto? https://www.statista.com/chart/18345/crypto-currency-adoption/. Accessed on April 14th 2021

L. Aniello, R. Baldoni, E. Gaetani, F. Lombardi, A. Margheri, and V. Sassone, (2017) "A prototype evaluation of a tamper-resistant high performance blockchain-based transaction log for a distributed database," in *Proceedings of the 13th European Dependable Computing Conference (EDCC '17)*, pp. 151–154, September 2017.View at: Google Scholar

M. Bartoletti, S. Lande, L. Pompianu, and A. Bracciali, (2007) "A general framework for blockchain analytics," in *Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers (SERIAL '17)*, December 2017.View at: Google Scholar

M. Castro and B. Liskov, (1999) "Practical Byzantine fault tolerance," in *Proceedings of the 3rd Symposium on Operating Systems Design and Implementation (OSDI '99)*, pp. 173–186, February 1999.

M. H. Miraz and M. Ali, (2018) "Applications of blockchain technology beyond cryptocurrency," *Annals of Emerging Technologies in Computing*, vol. 2, no. 1, pp. 1–6, 2018.

M. Vukolić, (2016) "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface*, vol. 9591, pp. 112–125, 2016.View at: Google Scholar

Mallam Nuhu Ribadu, (2006) Executive Chairman, Economic and Financial Crimes Commission, "Corruption: The Trouble with Nigeria", paper presented at the 3rd Annual National Trust Dialogue, January 19, 2006.

Marcus Swanepoel, CEO Luno (2021) An Update for Nigeria Crypto Users. https://www.luno.com/blog/en/post/an-update-for-nigerian-crypto-users-from-luno-ceo-marcus-swanepoel. Accessed August 4th 2021

Mauro Paolo, (1998) Finance and Development, "Corruption: Causes, Consequences and Agenda for Further Research", March 1998, https://www.internationalbudget.org/wp-content/uploads/Corruption-Causes-Consequences-and-Agenda-for-Further-Research. pdf pp. 11-14.

Merkle, R.C. (1982) Method of Providing Digital Signatures. U.S. Patent 4,309,569, 5 January 1982. Available line: https://patents.google.com/patent/US4309569A/en (accessed on 15 January 2020).

NATHAN REIFF, (2020), Blockchain Explained. https://www.investopedia.com/terms/b/blockchain.asp., Assessed on 10th August, 2020.

National Institute of Standards and Technology, (2013) FIPS-186-4-Elliptic-Curve-Digital-Signature-Al. https://csrc.nist.gov/publications/detail/fips/186/4/final (accessed on 15 January 2020).

NIST, (2014) Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS). Federal Information Processing Standards. FIPS 186-4. 2014. Available online: https://csrc.nist.gov/Presentations/2014/

Obasanjo, O. (2000) Statement presented at the Inauguration of the Independent Corrupt Practices and Other Related Offences Commission, 29th September, 2000.

Obasanjo, O. (2003), "Nigeria: From Pond of Corruption to Islands of Integrity". Lecture delivered at the 10th Anniversary Celebration of Transparency International, Berlin, 7th November, 2003.

Obasanjo, O. (2004), Welcome Address delivered at the Public Procurement Workshop, Abuja, July 12, 2004.

Odekunle, Femi (2015). Tackling Corruption in Nigeria: Strategic and Operational Options for the Buhari Administration. The 5th Convocation Lecture at The Al-Hikmah University Ilorin, Nigeria.

Odozi, Victor, (2002) "Nigeria and the global fight against financial crime", The Comet, Thursday, November 7, 2002, p.9

Okonjo-Iweala, Ngozi (Dr), 2006 "Economy: The need for sovereign credit rating", A speech delivered at the inauguration of the Bond Market Steering Committee (BMSC), Lagos, The Comet, March 1st, 2006

Okonjo-Iweala, Ngozi Dr., (2006) "Economy: The need for sovereign credit rating", A speech delivered at the inauguration of the Bond Market Steering Committee (BMSC), Lagos, The Comet, March 1st, 2006

Otite, Onigu (2000) "Corruption against the Norms of African Life" in O. Femi (ed.) Effective and Efficient Implementation of Nigeria's Recent Anti-Corruption Legislation.

R. Yasaweerasinghelage, M. Staples, and I. Weber, (2017) "Predicting latency of blockchain-based systems using architectural modelling and simulation," in *Proceedings of the IEEE International Conference on Software Architecture (ICSA '17)*, pp. 253–256, April 2017.View at: Google Scholar

Raj Kamal, (2004), "Blowing the Whistle on Corruption in Construction: One Man's Fatal Struggle" Jha, Indian Express (India) 7th May, 2004.
Raj Kamal, (2005) Global Corruption Report 2005: Corruption in construction and post-conflict reconstruction. https://issuu.com/transparencyinternational/docs/2005_gcr_construction_en/4. Accessed August 9th 2020.

S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, (2017) "Performance analysis of private blockchain platforms in varying workloads," in *Proceedings of the 26th International Conference on Computer Communications and Networks (ICCCN '17)*, August 2017.View at: Google Scholar

Sadiq Isah Radda, (2013) Globalization and the prospects for sustained economic growth: issues of economic and financial crimes in nigeria. Https://www.academia.edu/21621664/globalization_and_the_prospects_for_sustained_economic_growth_issues_of_economic_and_financial_crimes_in_nigeria. Accessed on 16th august, 2020.

Schneider, S. (2019, October 11). *Advance fee fraud*. *Encyclopedia Britannica*. https://www.britannica.com/topic/advance-fee-fraud

SECG, (2010), Recommended Elliptic Curve Domain Parameters. SEC 2 Version 2.0. 2010. Available online: **Standards for Efficient Cryptography Group** (2009) https://www.secg.org/sec2-v2.pdf (accessed on 15 January 2020).

T. T. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K. Tan, (2017) "Blockbench: A framework for analyzing private blockchains," in *Proceedings of the the ACM International Conference*, pp. 1085–1100, Chicago, IL, USA, May 2017.

Techshielder, (2021) https://techshielder.com/catfish-analysis-the-countries-with-the-highest-rates. Accessed on 9th September 2021.

The New Partnership for Africa's Development (NEPAD), (2006) A summary of NEPAD Action Plans, Section I, under Economic and Corporate Governance Initiative, the chapter on Money Laundering.

Timothy B. Lee, (2017), Bitcoin's Insane Energy Consumption Explained. https://arstechnica.com/tech-policy/2017/12/bitcoins-insane-energy-consumption-explained/, Assessed on 9th September, 2020. ttp://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.590.2899&rep=rep1&type=pdf

V**ictor Gayoso Martinez, Luis Hernandez-Alvarez and Luis Hernandez Encinas** (2020), Analysis of the Cryptographic Tools for Blockchain and Bitcoin; pdf pg. 12 - 112

X. Xu, I. Weber, M. Staples et al., (2017) "A taxonomy of blockchain-based systems for architecture design," in *Proceedings of the IEEE International Conference on Software Architecture (ICSA '17)*, pp. 243–252, April 2017.View at: Google Scholar