

# **GODFREY OKOYE UNIVERSITY ENUGU**

**Challenges Confronting Future Banking Globally and Locally**

**5<sup>th</sup> Inaugural Lecture of the Godfrey Okoye University**

**Delivered on 01 July 2021**

By

**PROFESSOR DR. TITUS FREEMAN IFEANYI NWANNE**

**PROFESSOR OF BANKING AND FINANCE**

**GODFREY OKOYE UNIVERSITY**

The background features abstract, overlapping green geometric shapes, primarily triangles and polygons, in various shades of green, creating a modern and dynamic visual effect.

# **“CHALLENGES CONFRONTING FUTURE BANKING GLOBALLY AND LOCALLY”**

# **1. INTRODUCTION**

## 1. Origin of Banking

History regarding the origin of “Banking” is still not clear. It has been based on guesses. According to some writers such as W. Frankace, a German writer and the British writer, Chamber, the word “bank” is called “bancus” by the early bankers, the Jews in Lombardy, the Spanish call it “banc”, the Italians call it “banca” while the French call it “banque” all of which mean a bench upon which the early European Money-lenders and Money-changers used to display their coins (Frankace, 2018 & Chamber, 1992).

Maclead, in his own opinion, maintained that these words were used for the purpose of economic activities of different countries of Europe (Nwanne, 2016). Today, globally and locally, banking still has to do with money-exchange and other transactions concerning money and the public.

In modern times, banks have also continued with transactions concerning money. It is also during this modern times that cryptocurrency emerged. Considering the fast rate at which technological changes are affecting the spheres of life globally and locally, it is expected that future banking will be confronted with some challenges. The question then is what are these challenges that will confront future banking globally and locally?

This lecture therefore intends to identify the challenges that will confront future banking globally and locally. In dealing with this, the lecture will first of all look at banking today, that is, modern banking as well as the emergence of Cryptocurrency. It will then discuss future banking by looking at factors that may bring about the changes that will take place in future banking, including the effects of COVID-19 and Financial Technology (Fintech) and then, the problems that these factors will cause. These will be followed by summary, conclusion and recommendations.


- A. Modern Banking
- B. Cryptocurrency
- C. Future Banking: Factors that are changing the future banking landscape.
- D. The Effects of COVID-19 on Future Banking.
- E. The Effects of Financial Technology (FinTech) on Future Banking.
- F. Summary
- G. Conclusion and Recommendations

## **1. (A). MODERN BANKING**

Modern banking as we know it today had its roots in the laissez-faire philosophy of British economist Adam Smith, who advocated for a much more free market (a free market is a type of economic system that is controlled by the market forces of supply and demand, that is the “*invisible hand*” as opposed to one regulated by government control). The “invisible hand” is the unobservable market force that helps the demand and supply of goods in a free market to reach equilibrium automatically.

Banking has moved away from the days of using agricultural goods as deposits in ancient times and is now very highly regulated and organized, inspiring a lot of confidence which is something that is absolutely necessary in banking (Hasman & Mattei, 1988, Nwanne & Nwanbeke, 2012).

In the modern world, banks offer a variety of services to attract customers. According to Nwanne (2015), some basic modern services offered by the banks are listed below:

- 
- i. Advancing of Loans.
  - ii. Overdraft.
  - iii. Discounting of Bills of Exchange.
  - iv. Cheque Payment.
  - v. Collection of Payment of Credit Instrument.
  - vi. Foreign Currency Exchange.
  - vii. Consultancy.
  - viii. Bank Guarantee.
  - ix. Remittance of Funds.
  - x. Credit cards
  - xi. ATMs Services.
  - xii. Debit cards.
  - xiii. Home Banking.
  - xiv. Online Banking.
  - xv. Mobile Banking.
  - xvi. Acceptance of Deposit.
  - xvii. Priority Banking.
  - xviii. Private Banking.
  - xix. Point of Sale



## **2.1 (B) Emergence of Cryptocurrency.**

Recently, we have seen the emergence of cryptocurency. Precisely in 2009, the first decentralized **cryptocurrency**, bitcoin, was created by a presumably pseudonymous developer Satoshi Nakamoto. In April 2011, Namecoin was created as an attempt at forming a decentralized DNS (The DNS, the **Domain Name System**, is a service at the heart of how the Internet operates), which would make internet censorship very difficult. Soon after, in October 2011, Litecoin was released (Lee, 2011).

A cryptocurrency is a digital or virtual currency that is secured by cryptography which makes it nearly impossible to counterfeit or double-spend. It is a form of digital asset based on a network that is distributed across a large number of computers. This decentralised structure allows them to exist outside the control of governments and central authorities,

## Features of Cryptocurrency

- It is digital, that is, it only exists on computers.
- Transaction data and ledger are encrypted using Cryptograph – the art of writing or solving codes or the art of encrypting and decrypting messages to keep them secret from outsiders (which is why it is called “Crypto” “Currency”). The word “Crypto” refers to the various encryption, algorithms, and cryptographic techniques that safeguard these entries such as elliptical curve encryption, public-private key pairs and hashing functions.
- It is decentralized - meaning it is controlled by users and computer algorithms and not a central government.
- It is distributed – meaning that the block chain is hosted on many computers across the globe. A block chain is a digital public ledger. Block chains are organizational methods for ensuring the integrity of transactional data.
- It is transferred between peers (there is no middle man or a bank)
- It is traded on online cryptocurrency exchanges like stock exchanges.
- The most defining feature of cryptocurrencies is that they are generally not issued by any central authority, thereby rendering them theoretically immune to government interference and manipulation.

## Types of Cryptocurrency

The first blockchain-based cryptocurrency was [Bitcoin](#), which still remains the most popular and most valuable. Today, there are thousands of alternate cryptocurrencies with various functions and specifications. Some of these are clones or [forks](#) of Bitcoin, while others are new currencies that were built from the scratch (Frankenfield, 2017).

Some of the competing cryptocurrencies that sprang up as a result of Bitcoin's success, known as "altcoins," include [Litecoin](#), Peercoin, and [Namecoin](#), as well as [Ethereum](#), Cardano, and [EOS](#) (Reynor, 2021). . Today, the aggregate value of all the cryptocurrencies in existence is around \$1.5 trillion—Bitcoin currently represents more than 60% of the total value (CoinMarketCap, 2021).

## **How does cryptocurrency work?**

Cryptocurrency works a lot like bank credit or a debit card. In both cases, a complex system that issues currency and records transactions and balances works behind the scenes to allow people to send and receive currency electronically. Likewise, just like with banking, online platforms can be used to manage accounts and move balances. The main difference between cryptocurrency and bank credit is that instead of banks and governments issuing the currency and keeping ledgers, an algorithm (a process or set of rule to be followed in calculations or other problem-solving operations, especially by a computer) does it.

Transactions are sent between peers using software called “[cryptocurrency wallets](#).” The person creating the transaction uses the wallet software to transfer balances from one account (a public address) to another. To transfer funds, knowledge of a password (a private key) associated with the account is needed. Transactions made between peers are encrypted [convert (information or data) into a code, especially to prevent unauthorised access] and then broadcast to the cryptocurrency’s network and queued up to be added to the public ledger. Transactions are then recorded on the public ledger through a process called “mining”. All users of a given cryptocurrency have access to the ledger if they choose to access it, for example by downloading and running a copy of the software called [a “full node” wallet](#) (as opposed to holding their coins in a third party wallet like [Coinbase](#)). The transaction amounts are public, but who sent the transaction is encrypted (transactions are pseudo-anonymous). Each transaction leads back to a unique set of keys. Whoever owns a set of keys, owns the amount of cryptocurrency associated with those keys (just like whoever owns a bank account owns the money in it). Many transactions are added to a ledger at once. These “blocks” of transactions are added sequentially by miners. That is why the ledger and the technology behind it are called “block” “chain.” It is a “chain” of “blocks” of transactions.

Apart from discussing how Bitcoin and many other coins which use blockchains work, there are still some other altcoins which use unique mechanics. Some of these altcoins offer fully private transactions without the use of blockchains at all.

# Advantages and Disadvantages of Cryptocurrency

## Advantages

1. It makes it easier to transfer funds directly between two parties, without the need for a trusted third party like a bank or credit card company. These transfers are instead secured by the use of public keys and private keys and different forms of incentive systems, like Proof of Work or Proof of Stake.
2. In modern cryptocurrency systems, a user's "wallet," or account address, has a public key, while the private key is known only to the owner and is used to sign transactions.
3. Transfers of funds are completed with minimal processing fees, allowing users to avoid the steep fees charged by banks and financial institutions for wire transfers.
4. They have been praised for their portability, divisibility, inflation resistance, and transparency.



## Disadvantages

1. The semi-anonymous nature of cryptocurrency transactions makes them well-suited for a host of illegal activities, such as “[money laundering](#)” and “[tax evasion](#)”. On the other hand, cryptocurrency advocates often highly value their anonymity because it protects them from being detected under repressive governments.
2. Some cryptocurrencies are more private than others. Bitcoin, for instance, is a relatively poor choice for conducting illegal business online, since the forensic analysis of the Bitcoin blockchain has helped authorities arrest and prosecute criminals. More privacy-oriented coins do exist such as [Dash](#), Monero, or [ZCash](#), which are far more difficult to trace.

# Criticisms of Cryptocurrency

Since market prices for cryptocurrencies are based on supply and demand, the rate at which a cryptocurrency can be exchanged for another currency can fluctuate widely, since the design of many cryptocurrencies ensures a high degree of security.

Bitcoin has experienced some rapid surges and collapses in value, climbing as high as \$19,000 per Bitcoin in Dec. of 2017 before dropping to around \$7,000 in the following months (Brown & Kharpal, 2021). Cryptocurrencies are thus considered by some economists to be a short-lived interest or speculative bubble (a ball of air).

Cryptocurrency blockchains are highly secure, but other aspects of a cryptocurrency ecosystem, including exchanges and wallets, are not immune to the threat of hacking. In Bitcoin's 10-year history, several online exchanges have been the subject of hacking and theft, sometimes with millions of dollars' worth of "coins" stolen (Wikipedia, 2013).

# Difference between a Digital Currency and a Cryptocurrency

The difference between a digital currency and a cryptocurrency is that the latter is decentralised, meaning it is not issued or backed by a central authority such as a central bank or government. Instead, cryptocurrencies run across a network of computers. Digital currencies have all the characteristics of traditional currencies but exist only in the digital world. They are issued by a central authority.

# Nigerian Senate and the Central Bank on Cryptocurrency

In February, this year 2021, Nigerian Senate summoned the Governor of CBN, Emefule and the Chief Securities Regulator, Lamido Yuguda, for a briefing after the Cental Bank ordered the local financial institutions to stop providing services to crypto companies and users. The briefing focused on explaining to the Senate Banking Committee the “opportunities and threats of cryptocurency.”

CBN’s directive – which ordered local financial institutions to stop providing services to cryptocurrency companies and users – led local crypto advocates to write to the bank (CBN) asking for clarification on the order. In response, the CBN published a five-page statement that included a pledge to protect Nigerian citizens from the risks of cryptocurrencies.

The CBN maintained that it will continue to do all within its regulatory powers to educate Nigerians to desist from its use and protect our financial system from activities of fraudsters and speculators.

But a number of Senators opposed the CBN move and an outright ban on crypto, though they spoke in favour of regulating the industry. According to Sen. Bassey, “the next level is cryptocurrency and we can’t run away from it. It is the CBN’s responsibility to bring Nigerians to the next level, not discouraging it.”

## Cryptocurrency and the Central Bank of Nigeria

Meanwhile, on 14 June 2021, information reaching us stated that according to Rakiya Mohammed, a Central Bank officer and information technology specialist at CBN, Nigeria may launch a CBN digital currency by the end of 2021 to serve as pilot scheme. This will be the result of the exploration the CBN has been making for over two years. She was quoted as saying, “Before the end of the year, the CBN will be making some special announcement and possible launching of the pilot scheme in order to provide this kind of currency to the populace.”

According to Mohammed, one reason for a CBDC (Central Bank Digital Currency) would be to make it easier to transfer remittances into the country. Earlier this year, Nigeria set up a temporary rewards program to encourage international transfers to Nigeria.

### **3. (C) FUTURE BANKING**

As earlier mentioned in the statement of the problem, the technological advancement of the next decade will challenge banks globally and locally. Some are already playing out now; others will be far more prominent by 2025 and more pronounced by 2030.

In order to compete in a world with increasingly blurred boundaries — where smart devices and platforms such as Google can deliver the banking experience, and ride-sharing applications can supply loans, banks will be confronted with many challenges both from the perspectives of the banking system itself and from the perspective of the customers. Four clear themes are expected to emerge in the future of banking: Future banking would be invisible, connected, insight-driven and purposeful. Consequently, banks must be determined to face up to these challenges.

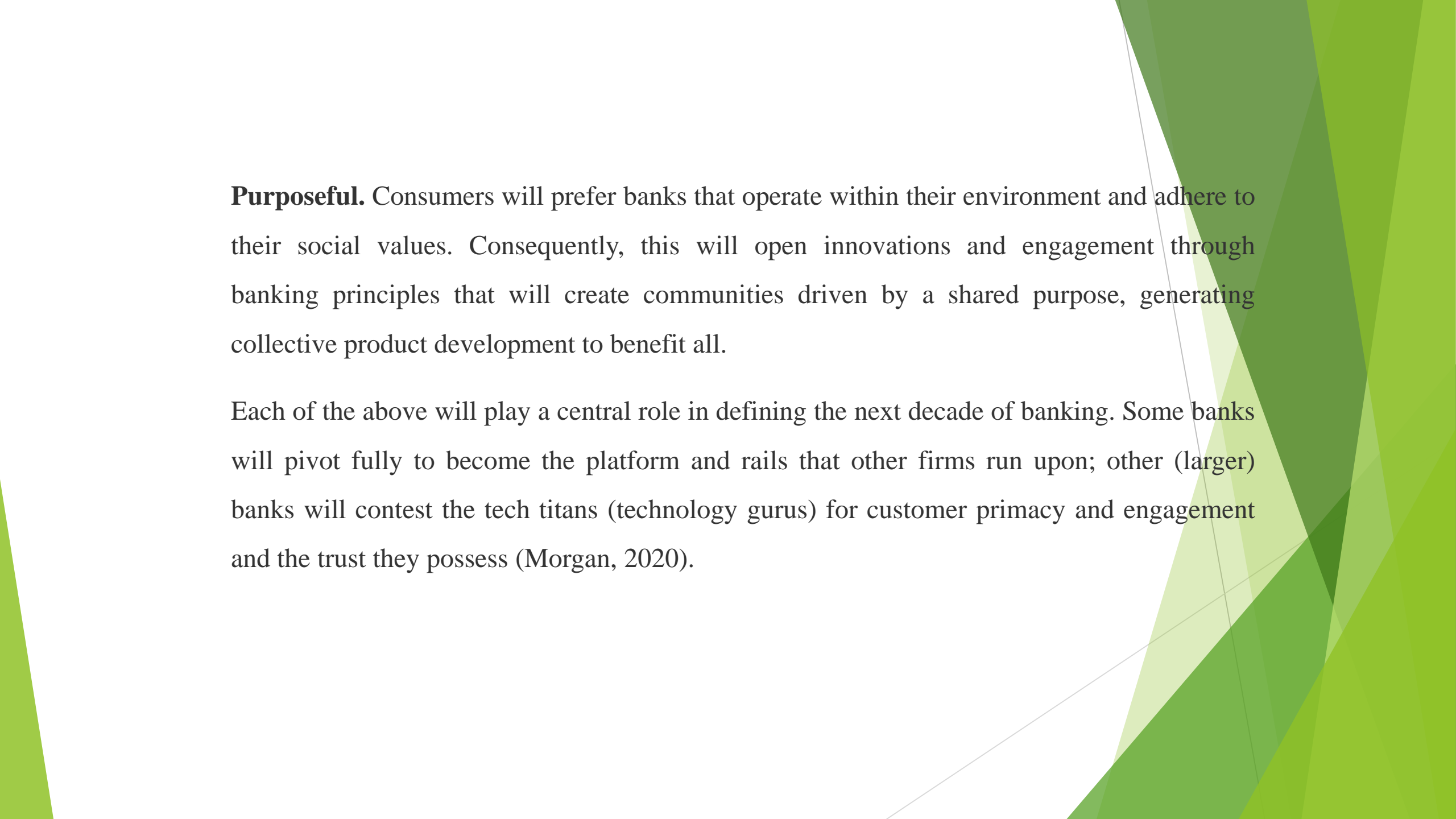
**Invisible.** This means that leading banks will use technology and far deeper customer information to render financial services at the customer's moment of need, often at the expense of specific type of technology.

Distribution models are evolving to make use of marketplaces and technologies such as open APIs (Application Programming Interfaces) and 5G to connect finance with homes, machinery, and other devices. This will pose challenges for many banks as their retail brands will become increasingly invisible to the end consumer.



**Connected.** To remain relevant, banks must be present in the ecosystems (physical environment) and products that customers use. To do this, they must cease to see partnerships — and intermediation of their brand — as a threat. Banks will assemble constellations (group of similar people) of value: interoperable, trusted environments that enable collaborators beyond banking to weave value into frictionless, rich customer journeys. “Trusted advisor” status is what will differentiate banks from all other touch-points that offer embedded financial services.

**Insights-driven.** Banks will obtain information from data which will make their customers trust them more. Consumer trust is the critical asset here. Banks must firmly step up an advisory service which will generate financial intimacy with their customers — customers that expect “RoC” (return on consent) for that trust.

The background of the slide features abstract, overlapping green geometric shapes, primarily triangles and polygons, in various shades of green, creating a modern and dynamic visual effect.

**Purposeful.** Consumers will prefer banks that operate within their environment and adhere to their social values. Consequently, this will open innovations and engagement through banking principles that will create communities driven by a shared purpose, generating collective product development to benefit all.

Each of the above will play a central role in defining the next decade of banking. Some banks will pivot fully to become the platform and rails that other firms run upon; other (larger) banks will contest the tech titans (technology gurus) for customer primacy and engagement and the trust they possess (Morgan, 2020).

Five key factors that are changing the future banking landscape are:

- i. CyFi (cyber and financial crime).
- ii. Data Integrity
- iii. Embracing and becoming Digital.
- iv. COVID-19 Pandemic
- v. Fintech (Financial Technology) and Future Banking in Nigeria.

## **3.1 Cybercrime and Financial Crime**

The **financial** sector is closely associated with **cybercrime** in many ways. Fraud, bank account theft, money-laundering, personal data breaches and terrorist funding are some of the attack types affecting **financial** institutions (Hasham, Joshi & Mikkelsen, 2019).

## **Cybercrime in Finance**

Cybercrime in finance is the act of obtaining financial gain through profit-driven criminal activity, including identity fraud, ransomware attacks, email and internet fraud, and attempts to steal financial account, credit card, or other payment card information.

In other words: Financial cybercrime includes activities such as stealing payment card information, gaining access to financial accounts in order to initiate unauthorised transactions, extortion, identity fraud in order to apply for financial products, and so on.

The financial services industry is a very lucrative target and is, therefore, heavily impacted by the rise of cyber criminality. Cyber Financial crime also affects all sorts of companies and unsuspecting individuals. Anyone can fall victim to credit card skimming by having their virtual wallets targeted, or malware designed to steal your password.

## Types of attacks motivated by financial gains

Various social engineering techniques are most often used in order to manipulate victims into providing confidential information. This can be anything from fake emails supposedly sent by Netflix asking you to pay your subscription invoice, to illegitimate replica emails pretending to be from Paypal or iTunes informing you of your monthly invoice—trying to get you to click on a fraudulent link.

Other well-known scams are Bitcoin scams or love scams, where people are targeted through fake profiles on dating sites or popular social media sites to strike up relationships, leading to the scammer asking for money transactions exploiting the victim's feelings.

## Consequences of Financial Crimes

The consequences of a successful attack can be traumatic and have devastating effects on a company. Loss of large sums can impact the whole economy of the company and even lead to bankruptcy in the most severe cases, especially if the company is small.

Reputational damage in the eyes of stakeholders, clients, and the general public is also an unfortunate consequence. When it comes to private individuals, they may experience having their accounts emptied, savings stolen and debts taken up in their name after having their identity stolen.

## **3.2 Data Integrity**



Data integrity refers to the trustworthiness of data (Yau, 2021). Some data security tactics include permissions' management, data classification, identity and access management, threat detection,

In this era of big data, when more pieces of information are processed and stored, implementing measures that preserve the integrity of the data that is collected is increasingly important. Understanding the fundamentals of data integrity and how it works is the first step in keeping data safe.

Data integrity also refers to the safety of data in regards to regulatory compliance — such as General Data Privacy Regulation (GDPR compliance) — and security. It is maintained by a collection of processes, rules, and standards implemented during the design phase. When the integrity of data is secure, the information stored in a database will remain complete, accurate, and reliable no matter how long it is stored or how often it is accessed. Data integrity also ensures that your data is safe from any outside forces.

## **Data integrity and GDPR (General Data Privacy Regulation) compliance**

Data integrity is key to complying with data protection regulations like GDPR. Non-compliance with these regulations can make companies liable to large penalties. In some instances, they may be sued in addition. Repeated compliance violations can put companies out of business.

## Data integrity risks

There are several factors that can affect the integrity of the data stored in a database. A few examples include:

- **Human error:** When individuals enter information incorrectly, duplicate or delete data, do not follow the appropriate protocol, or make mistakes during the implementation of procedures meant to safeguard information, data integrity is put in jeopardy.
- **Transfer errors:** When data cannot successfully transfer from one location in a database to another, a transfer error has occurred. Transfer errors happen when a piece of data is present in the destination table, but not in the source table in a relational database.
- **Bugs and viruses:** Spyware, malware, and viruses are pieces of software that can invade a computer and alter, delete, or steal data.
- **Compromised hardware:** Sudden computer or server crashes, and problems with how a computer or other device functions, are examples of significant failures and may be indications that your hardware is compromised. Compromised hardware may render data incorrectly or incompletely, limit or eliminate access to data, or make information hard to use.

Protecting the integrity of your company's data using traditional methods can be an overwhelming task. Secure, [cloud-based data integration platforms](#) offer a modern alternative that provide a real-time view of all of your data. With industry-leading cloud integration tools, you can connect multiple source data applications and get access to all of your company's data in one location.

(Please see **Appendix 2** for Types of data Integrity and more)

## **3.3 Embracing and becoming Digital**

Financial services are undergoing a huge period of digital transformation, as advanced technologies radically transform the way the industry operates. AI (Artificial Intelligence), machine learning (ML) and robotics are fundamentally changing the sector and banks need to embrace the amazing opportunities that have surfaced. In addition to the impact of digital transformation, financial services are also undergoing a crisis of trust with [PwC](#) (PricewaterhouseCoopers) reporting that British consumers have lost trust in the industry (Strange, 2019 & Tipping, 2019). With rising competition from fin-tech disrupters, the question is how can financial services succeed in this increasingly digital world? How can they embrace and deliver the digital innovation that customers demand without compromising security and ultimately consumer trust because the customer is still king?

The financial sector has historically been a digital slowcoach due to strict regulations, legacy systems and senior decision makers being slow to recognise potential ROI (Return on Investment). Whilst banks are now increasing I.T (Internet Technology) spend and are automating business processes through artificial intelligence (AI), there is still a lag in meeting consumer expectations for seamless mobile apps, alternative technologies like person-to-person (P2P) payments, mobile wallets and more. The problem is that many banks still believe that digital transformation is about systems and workflows rather than customers.

Many banks are also hindered by fears that new technologies will lead to new security threats. This is a misconception because consumer behaviour in banking is changing. Studies show that instead of speaking in-person to an advisor at a local bank branch, most customers will prefer to interact remotely via digital channels. In fact, the average consumer will initiate up to 10 digital interactions with their bank per month. These changes in consumer behaviour are opening doors for a new breed of fintech disrupters (obstructions) who are ready and waiting to take market share and customers. Digital-first providers like Monzo and Revolut are giving dissatisfied consumers the opportunity to literally take their money elsewhere, and with multiple challenger banks shaking up the industry, consumers are faced with multiple choice. Consumers are enjoying digital transformation in other sectors and now expect the same from financial services; disrupter banks are simply giving them the innovation they crave for.

Digital transformation and digital banking have become the core focus for banks. While digital banking was a substantial part of many strategies prior to the pandemic, the necessity to deliver these offerings happened at an accelerated rate. So, now digital banking and services are not only nice to have, they are necessities (Barnes, 2021).

As many companies have adapted their work policies to not only work from home, but work from anywhere, many customers now want to do business from anywhere. That means many bank customers want to bank from anywhere and this can only be possible through technology.

The basic need for banking services has not changed. People still need to deposit a cheque, open a new account, get a new debit card, refinance their homes, and more. What has changed is the way technology enables customers and members to do these services on their terms, and the empowered customer wants *convenience, simplicity, and options*.

Also despite the threat from disrupters, traditional financial services organisations, such as banks and credit unions can win back favour with today's entitled consumers by establishing themselves as stewards of consumer financial assets, namely money and data, and by ensuring that their service is relevant.

## Meeting consumers' demands with new technology

Consumers are aware of the value their data has for banks, especially in this post-GDPR (General Data Privacy Regulation) world. They are willing to share, but with this comes higher expectations of the service they will be getting as a result. Research by Accenture found that almost half of UK bank customers expect relevant advice and product information available at their fingertips that they can access easily. They expect banks to inform them of the best rates to suit their individual financial situation. Big Data provides significant opportunities for banks to outshine their competitors. Migrating data onto a cloud platform provides a 360-degree view of every customer and this deep insight shows banks where they can provide a higher level of service and create more value (Tipping, 2019). For **example**, if a customer is in the process of buying their first house, their bank can contact them with relevant and useful information to ease the process. With all the data available to financial services, customers expect their bank to know what they want and need, before they do, offering them next level personalisation that caters to their every possible financial need.



## Creating seamless experiences

Another aspect of the customer experience that needs to be improved is flexibility that is giving customers the freedom to access and manage their finances without delay is vital. Consumers expect to perform transactions anywhere, at any time (Johnson, 2020).

Despite the ongoing fundamental changes in the industry, three things remain certain: customers want to bank with companies they can trust, customers demand individual financial advice, and customers insist on full control over their finances. Prioritising customer experience in these ways is nothing new, but financial services must wake up to the new technologies at their disposal in order to match changing consumer behaviour.

## Benefits of Appointment Schedule Software:

With virtual queuing, customers and members have the choice to go online, check in, and be notified regardless of their location when it is time for their appointment or to meet with a staff member. Capacity management can be used to set a limit, manage walk-ins at peak times, and ensure there is enough space and distance in bank entrances and waiting areas.

While appointment booking may seem simple, it is complex, especially for the financial services industry. There are many technologies considerations from accessibility to security compliance (Marr, 2019).

## (1) Information security

Data breach costs are among the highest in the financial services industry. Finding a technology partner that goes above and beyond to ensure security is a must. Strict information security policies should protect both the bank and customers.

## **3.4 (D) The Effect of COVID-19 on Future Banking**

The global Covid-19 pandemic has changed consumer behaviour and their expectations indefinitely. Consumers expect the same experience from their bank as they do in their other daily interactions (Peplow, 2021). The pandemic also made digital capabilities critical, enabling banks to continue to serve their customers remotely. When bank branches across the world closed, customers had no choice but to embrace digital channels where appropriate; bank employees became equipped to serve customers from the confines of their homes in a matter of days because there was no other choice. This prompted an accelerated culture shift within banks who had previously been reluctant to view digitalisation as the primary channel for serving customers (Mukherjee, 2021).

With this shift, came a whole new expectation of what customer experience should look like. This race for banks to adjust the way they serve their customers both in the short and long-term, laid the foundations for a new banking model that is reflective of the shift the pandemic created in both consumer behaviours as well as the underlying economic environment (Ukpeh, 2018). Customers want access to the financial services and the tools they need, when and where they need them. Covid-19 essentially created a new opportunity for banks to fundamentally re-imagine their operating model to meet customer needs in a digital world, introducing new innovative services through new technologies while reducing their cost to serve. The availability of new technology and tools to enable this transition is also facilitating change (Anderson, 2018 & Barrows, 2021).

However, for all the positives on how banks have adapted to serving their customers over the course of last year, it has also only served to reinforce the gaps in the legacy banks' customer experience and operational transformation. According to a [recent study](#) by Publicis Sapient, 70% of banks surveyed say that the pandemic has highlighted weaknesses in their customer experience, and nearly all (81%) say the pandemic has improved their digital skills and (Fernando, 2021 & Warren, 2020).

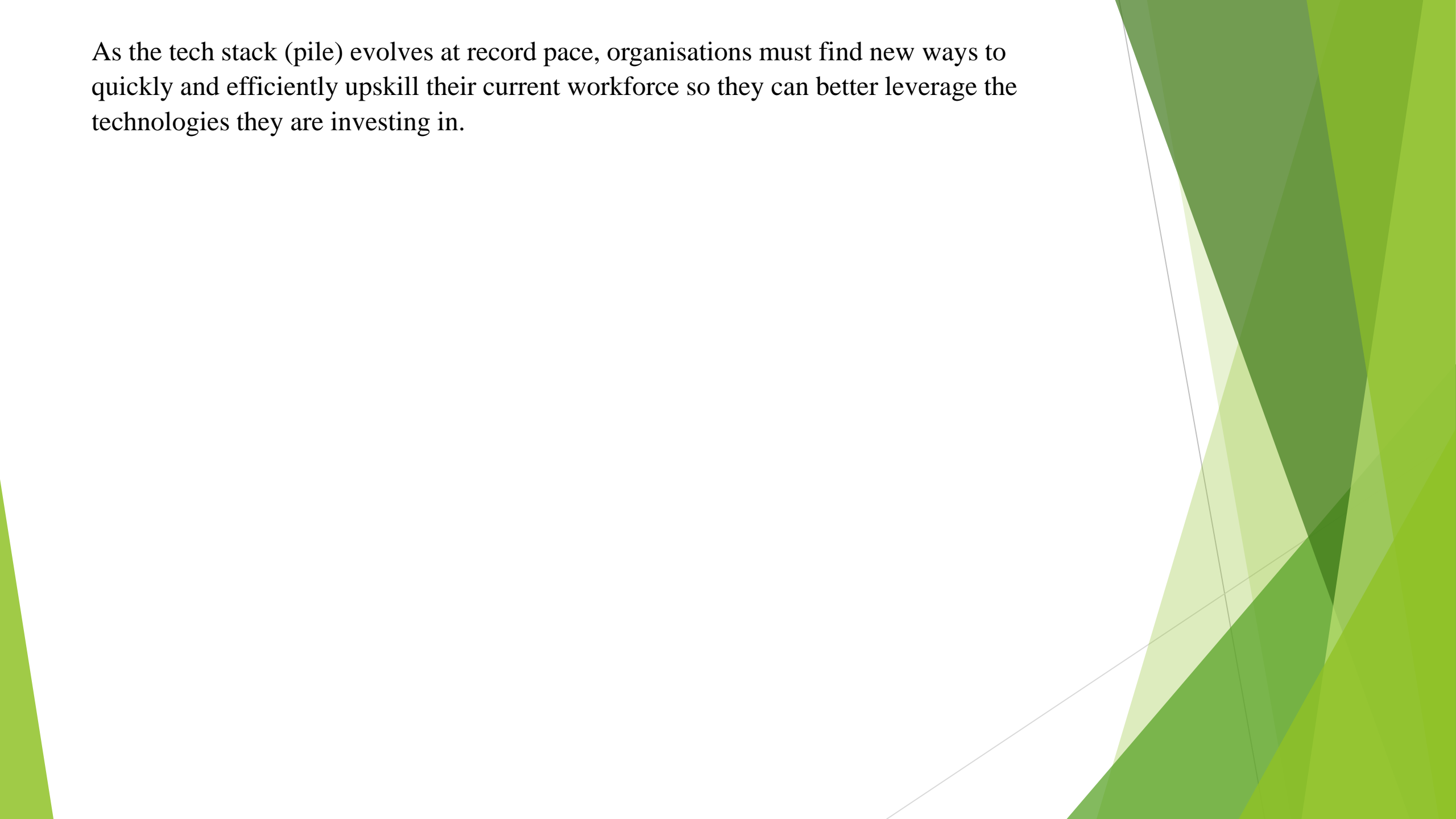
## Training is key to the digital evolution of banks

There is no doubt that banks have undergone a rapid digital transformation in the last year. The pandemic has seen financial institutions achieve seven years' worth of digitalisation in mere months. However, what good is all this shiny, new technology if employees have not been trained to use it effectively?

Banks, and indeed other industries and organisations, are struggling with this very confusing problem. Training courses may have been provided to help people use new and updated technology, but in many instances they may not be proving effective. This is limiting the return on investment for these new technologies and truncating the digital capabilities of banks (Laney, 2020)


In line with new ways of working, banks need to modernise their employee training programmes, both for new joiners coming to terms with different technologies and existing employees who want to use the technology more effectively. This means doing away with rigid, compulsory training in favour of something more flexible and intuitive. The question for banks is: how? To reap the benefits of their newfound digital capabilities, they will need an answer to this question (Pedersen, 2021).

As the tech stack (pile) evolves at record pace, organisations must find new ways to quickly and efficiently upskill their current workforce so they can better leverage the technologies they are investing in.





### **3.5 (E) The Effects of Financial Technology on Future Banking in Nigeria**

The background of the slide features abstract, overlapping green geometric shapes, primarily triangles and polygons, in various shades of green, creating a modern and dynamic visual effect.

The emergence of FinTech has been a welcome change to global commercial transactions. Whilst FinTech makes it easy for customers to pay bills, invest, save money, access loans/other financial products at little or no additional cost, e-commerce makes it easy for goods to be purchased online and delivered to customers.

E-Commerce companies typically integrate their platforms with FinTech to accept online payments. While this relationship has proved beneficial to both parties, they have also had to suffer the hurdles of running digital businesses in Nigeria (Udom, 2019).

# Key Challenges

FinTech has redefined financial services through technology, speed, and simplifying transactions. It has led to the emergence of new business models, products and solutions that are reshaping financial services in Nigeria. It has influenced the approach of banks to financial services. Nigerian banks now have internet/mobile banking platforms while some are also leveraging the social media to provide financial services to their customers.

Since the introduction of the [cashless policy](#) in 2012, the CBN has issued numerous guidelines that have improved the Nigerian FinTech ecosystem. The Federal Government also enacted the [Cyber Crimes Act 2015](#) to combat cybercrime, while the Electronic Transaction Bill and the Data Protection Bill have been enacted by the National Assembly (Scott & Eke, 2020). Notwithstanding the above, these regulations and laws do not adequately address the numerous challenges the ecosystem faces. Details of some of the challenges are:

# 1. Chargebacks

A chargeback is a payment returned to a credit/debit card after a customer debates the validity of an online purchase. Although it may occur as a result of an error from an e-commerce merchant or the unauthorized use of debit/credit card information, there are instances where the customer that received the purchased product denies receiving it or claims to have returned the product without being refunded (friendly fraud).

In the scenario described in the paragraph above, the CBN mandates the merchant to refund the payment to the customer even where the transaction was a friendly fraud. As such, no regulation currently exists that protects e-commerce merchants and or FinTech companies from friendly fraud. Depending on the amount involved, the merchant and the FinTech companies have to reach a commercial decision on loss sharing.

## 2. Fraud

The CBN mandates financial institutions to put security mechanisms in place towards protecting their system against fraud. FinTech companies are prone to cyber fraud, and their systems are consistently under attack. It has been estimated that Nigerian financial institutions lost approximately N159, 000, 000, 000.00 (One Hundred and Fifty-Nine Billion Naira) to cyber fraud between 2000 and 2013. Nigeria is ranked third globally in cybercrimes (Jonathan, 2017).

### 3. Barrier to Entry

Under the Guidelines for Mobile Money Services in Nigeria, anyone applying for a mobile money license from the CBN must provide evidence of having a minimum of N2, 000, 000, 000.00 (Two Billion Naira) as its shareholders' funds, or roughly \$7, 000, 000 (Seven Million Dollars) and serves as a huge discouragement to FinTech startups from applying for a mobile money licence (Strange, 2019).

## 4. Law Enforcement Agencies' Ignorance of e-Commerce and FinTech

Law enforcement agencies rarely have the knowledge of how e-Commerce and or FinTech platforms work. Consequently, this tends to affect the course of their investigating cyber fraud committed on a payment platform. As you would have seen from the FinePay scenario, their first step typically is to instruct the merchant and or FinTech company's bankers to place a lien on the company's account, regardless of the amount involved in the alleged crime or in the respective merchant/Fintech company's account with the bank.

## 5. Unclear Regulation

The CBN Guidelines for Mobile Money Services in Nigeria stipulate that mobile money services can either be Bank-Led or Non-Bank Led. The Bank-Led model refers to a Bank and or its consortium acting as lead initiator, while Non-Bank Led refers to a company licensed by the CBN acting as lead initiator. The Non-Bank Led model allows a CBN licensed company to deliver mobile money services to its customers. The licensed mobile money operators under the Non-Bank Led model often integrate their platforms with other financial solutions provider (as customers) to onboard merchants or use their respective platforms to process payments. Although, the guideline permits the integration, the CBN requires all financial solution providers to be licensed. The CBN often fines the licensed mobile money operators for integrating its platform with an unlicensed financial solutions provider.



## 6. Lack of Trust

Despite the innovative products offered by FinTech companies, customers prefer to conduct financial transactions with Nigerian banks. The brick and mortar banks are considered safer than FinTech platforms, despite being faster. In the same vein, some customers do not trust e-commerce companies. They are skeptical about the quality of goods, return policies and data security. Some e-Commerce companies have introduced Pay-On-Delivery (POD) to encourage customers to order online and pay when the goods are delivered. However, the POD has drawbacks: customers may refuse to pay/collect the goods, which could affect profit since time, human resources, and other expenses would have been incurred in the delivery of the goods.

## 7. Slow adaptation of Customers to New Technologies

Currently, many customers are still analogue. Consequently, they have difficulty with operating even the ATM services and doing Home and Online banking. This has resulted in many customers being defrauded as well as losing money by wrong operation of the services. Apart from customers who can attempt the use of E-banking system are the complete illiterates who thumbprint. By the next decade many of these analogue customers will still be around in Nigeria. This will pose problems for banks and such customers which banks must find ways to educate as quickly as possible in order to retain these numerous customers since we do not have only millennial customers.

The challenges described above as well as the FinePay scenario are typical of what future banking and FinTech companies alike would look like in the future in Nigeria.

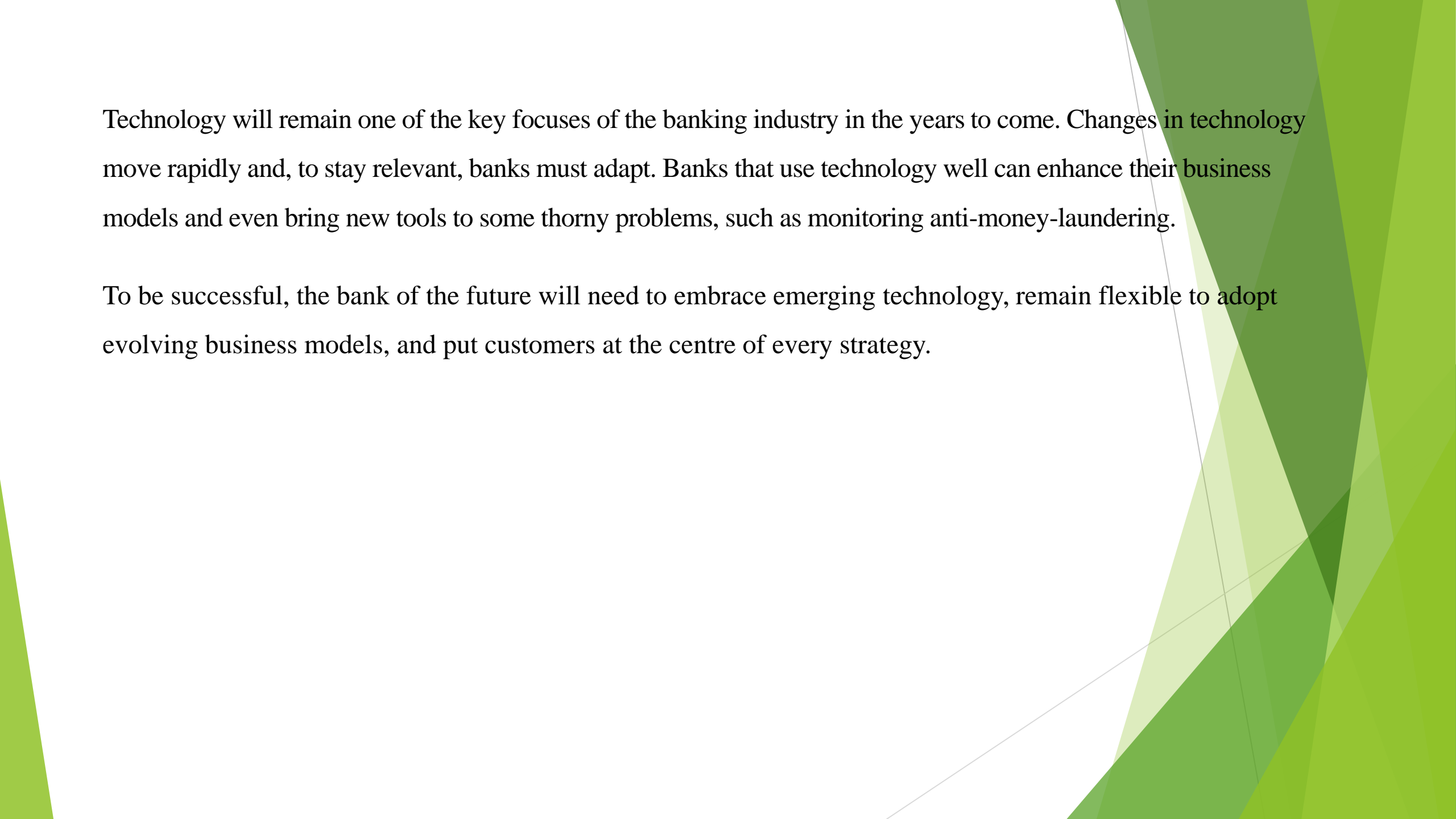
## **(F) SUMMARY**

The banking challenges discussed in this lecture have become more relevant in future banking where technology is advancing by leaps and bounds. Today's disruptive technology allows banks to reach a wide audience with great ease. However, they need to deal with these issues and problems not only to reach but also engage and build relationships with their customers in future.

Indeed, the 'unbundling' of banking services has accelerated, thanks to the growing wave of financial technologies, with a focus on digital-based solutions, enabling banking to be delivered in a similar manner with software services – that is, without having to set up an actual bank.

The barrier to entry to launch new banking services has lowered, while at the same time the willingness of consumers to 'try out' new services from non-traditional providers has dramatically increased.

The future of banking will look very different from today. Faced with changing consumer expectations, emerging technologies, and new business models, banks will need to start putting strategies in place now to help them prepare for banking in 2030.

The background of the slide features abstract, overlapping green geometric shapes, primarily triangles and polygons, in various shades of green, creating a modern and dynamic visual effect.

Technology will remain one of the key focuses of the banking industry in the years to come. Changes in technology move rapidly and, to stay relevant, banks must adapt. Banks that use technology well can enhance their business models and even bring new tools to some thorny problems, such as monitoring anti-money-laundering.

To be successful, the bank of the future will need to embrace emerging technology, remain flexible to adopt evolving business models, and put customers at the centre of every strategy.

The background features abstract, overlapping green geometric shapes, primarily triangles and polygons, in various shades of green, creating a modern, layered effect on the right side of the page.

## **(G) CONCLUSION AND RECOMMENDATIONS**

Since this lecture is on “Challenges confronting Future Banking globally and locally”, it can be seen that future banking is hinged on technology which changes very fast with many giant competitors. The onus lies on the banks to fall in line with the speed of technological changes. It also demands from customers a readiness to adapt to new changes which may take some time. It is therefore recommended that in order to remain relevant, banks should do the following:

### **1. Organise Seminars for Customers**

Since many analogue customers are still around, the ways to solve this problem are:

- (i) To organise seminars for such customers by grouping them according to age brackets and level of literacy/education.
- (ii) To create a section of the bank that will handle such customers because they should not forfeit their life-saving to the banks or risk leaving their money at home.
- (iii) It is also important for the CBN to realize that in its role regulating the space, it must continuously review its policies towards enabling the ecosystem to blossom. Our law enforcement agencies, particularly the Police also need a thorough understanding of how FinTech and e-banking work in order to enable them conduct investigations properly and not stifle business.

## **2. Training is key to the digital evolution of banks**

In line with new ways of working, banks need to modernise their employee training programmes, both for new joiners coming to terms with different technologies and existing employees who want to use the technology more effectively. This means doing away with rigid, compulsory training in favour of something more flexible and intuitive.

The best training programmes recognise that learning is an ongoing exercise. The objective is to enable employees to learn on the job and apply that learning directly to their work. Give them access to the new tools and technologies and then let them get their hands dirty. Allow staff to learn and grow in their daily routines by applying today's technologies to grow and perform in their everyday roles. Strive to create learning environments, rather than learning requirements.

The best answer is learning something new everyday



### 3. The effect of COVID-19 on Future Banking

To stay ahead, banks must not only deliver a reimagined experience but also focus on increasing their operational agility in enabling cross-functional collaboration, real-time data access and a more adaptive culture that will allow them to continue to innovate at speed as customer needs and expectations evolve. Banks need to deliver superior customer experiences while being operationally agile to drive growth and compete with digital-first challengers and new tech entrants.

4. **Digital:** To fully take advantage of the opportunities that digital-first offers, banks need to optimize all pillars of their customer experience and operations – from their business models and technology, to their products and services, and even their people. To stay ahead, banks must not only deliver a reimagined experience but also focus on increasing their operational agility in enabling cross-functional collaboration, real-time data access and a more adaptive culture that will allow them to continue to innovate at a speed as customer's needs and expectations evolve.

**5. Data Integrity:** Risks to data integrity can easily be minimized or eliminated by doing the following:

- Limiting access to data and changing permissions to restrict changes to information by unauthorized parties.
- Validating data to make sure it is correct both when it is gathered and used.
- Backing up data.
- Using logs to keep track of when data is added, modified, or deleted.
- Conducting regular internal audits.
- Using error detection software.

## **6. Future Banking and Disrupter Banks**

Banks can overcome this problem posed by these disrupter banks by entering the financial market, and making every point of contact for their customers digital as the disrupter banks are doing to succeed and regain their consumers' confidence; put simply, banks must evolve or die.

## 7. Lack of Personalization

Banks today need to take a leaf from other industries that value customer experience. The time when the focus of the bank was on transaction execution is gone.

Banks should give customers the option to do business on their terms and with expert guidance as this will lead the way to improving customer satisfaction and loyalty.

The question is how banks can provide personalisation at scale-across multiple branches, staff members and time zones. Banks can achieve this through appointment scheduling technology. It gives customers an unmatched level of service and the personalisation that keeps them coming back for more. In addition, [virtual queuing](#) and capacity management can help branch staff manage waiting areas while simultaneously improving the customer experience.

Furthermore, with virtual appointments, there is the benefit of providing services during non-traditional hours. The after-hours availability could be the difference between a loyal customer and having them choose a competitor. Also, having more convenient hours and ways to connect with customers opens up doors to more socio-economic groups (Barnes, 2021).

## **8. Creating seamless experiences**

Banks should create a seamless omni-channel experience that will meet this demand. This will be possible with flexible appointment modes from virtual technologies that will enable customers to access the services they need anytime, anywhere, through any device, and this is exactly what the empowered, hybrid customer expects.

## 9. Prevention of Financial Cybercrimes:

Human error is usually why exploits happen, so it goes without saying that training and awareness are important.

As a company, it is also important to focus on awareness campaigns so that the employees will be equipped with the knowledge of how they can be tricked in order to change these behaviours. It is also essential to have well-functioning threat intelligence in place, regular vulnerability tests run by the IT security team, and overall good cyber hygiene.

When it comes to you as an individual, try thinking about these things:

- Always be on alert and careful when shopping online, making transactions, or signing into your online bank and government portals
- Always make payments and transfers through official sites and be critical of who you are sending money to and why
- Be careful not to click on suspicious links, always verify the sender's identity and if in doubt, ask for a second opinion.

Raising awareness and running training in cybercrime techniques and consequences are necessary in order to reduce the number of victims.

Through sharing knowledge, expertise, and experience in our digital channels as well as participating in conferences and running awareness campaigns internally, we help to contribute to the fight against cyber criminality.