Blockchain Technology For Cyber Security: Performance Implications On Emerging Markets Multinational Corporations, Overview Of Nigerian Internationalized Banks.

Chikelue .C. Nwabuike ,Vincent.A. Onodugo , Austine Arachie, Ugonna .C.Nkwunonwo,

Abstract: Blockchain is an overwhelming technology with potentials to change business status quo, especially in emerging markets multinational corporations. This study sought to explore the adoption of Blockchain technology for cyber security of Emerging markets multinational corporations (EMNCs), with an overview of Nigerian internationalized banks. Secondary data from Internet crime complaint centre, Proshare, and Africa cybersecurity report were studied and discussed. Inferences were made from the data obtained and the study concluded that Blockchain technology will make cyber crimes costly to perpetrators and thus discourage cyber criminals from their ventures. This study becomes instrumental for emerging markets multinational corporations (EMNCs) by suggesting solutions to cybercrime challenges. The implication of the study is that performance will improve for Nigerian banks should they adopt Blockchain technology for cyber security, this will drive growth through minimization of cyber crime losses and reposition the banks to be strategically competitive with Developed banks in the industry, this further upholds the New growth theory.

Index Terms: Blockchain Technology, Cybersecurity, Cybercrime, Performance, Emerging Market Multinational Companies, Internationalized Banks, New Growth Theory.

1. INTRODUCTION

Technological advancements are imperatives for sustainable business growth and development. Blockchain technology is fundamentally a decentralized, distributed ledger transactions or events between parties. According to [10], Blockchain can be referred to as blocks in chain, where the corresponding blocks refer to the blocks prior to them. Transaction details once fed to the blockchain network is impossible to be tempered with, and details are shared with members of the network. Blockchain technology can be traced to Bitcoin blockchain, invented by Satoshi Nakamoto and is till date the most popular used cryptocurrency. He developed Bitcoin as a currency, but with few anomalies like applicability for other modes or assets but only as a currency. Secondly, transaction time defect. It takes a very long time sometimes to validate transactions. However developers are working to improve on blockchain with different kind of technologies. Cybersecurity is a part of overall corporate security management. The term cybersecurity is often used to connote "measures taken to guarantee safety and secure usage of the internet". Alternatively stated, cybersecurity are measures taken to check and defend against cybercrimes. Cybercrime can be defined as criminal activities which computers or computer networks are tools, and targets[38].

- *Chikelue.C. Nwabuike is an AI Engineer currently pursuing Doctorate degree program in Management in University of Nigeria. E-mail: nwabuike.chikelue@yahoo.com.*
- *Vincent . A. Onodugo is an Associate Professor of Management and currently the post graduate representative Faculty of Business Administtration in University of Nigeria. E-mail: vincent.onodugo@unn.edu.ng.*
- *Austine Arachie is a lecturer in the Department of Business Administration, Faculty of Management Sciences in Nnamdi Azikiwe University Awka, Nigeria. He is currently pursuing a Doctorate degree program in Management in University of Nigeria. E-mail: arachieaustine@gmail.com.*
- *Rev'd Ugonna .C.Nkwunonwo PhD. Is currently a lecturer in the Department of Geoinformatics and Surveying, Faculty of Environmental studies in University of Nigeria.E-mail: ugonna.nkwunonwo@unn.edu.ng.*

Some of the major impacts of cyber crime are; socio-political impacts, private and public sector businesses impact, consumer behaviour impact, emotional impact, lost of sales impact, cost of security protection and many more. A study by [29] reveals the prevalence of cybercrime; over 65% of internet users worldwide have fallen victims to cybercrimes like; computer viruses, online credit card fraud and identity theft. Norton's study showed that cyber crime has surpassed illegal drug trafficking as criminal money maker. Person's identity is stolen every three seconds as a result of cyber crime, without sophisticated security package, unprotected PCs can become infected within four minutes of connecting to the internet. Hansen and Wernerfelt [16] identified two models of firm's performance as Economic model and organizational model. The Economic model emphasizes on importance of external market factors in determining firm success. Whereas the organizational model anchors on behavioral and sociological paradigm. The organizational model views organizational factors and their relationship with the environment as the major determinants of success.

They further decomposed the Economic model to include:

A. Industry variables (characteristic of the industry in which firm competes)
B. Variable relating the firm to its competitors
C. Firm variables (the quality and quantity of the firm's resources)

The organizational model in broad term advocates that managers can be able to influence the behavior of their employees (and consequently the performance of the organization) by taking into account factors like the formal and informal structure, the planning, reward, control and information systems, their skills and personalities, and the relation of these to the environment. In other words, managers influence organizational outputs by establishing context, and context is the result of complex set of psychological, sociological and physical interaction. Hansen and Wernerfelt [16] later integrated the two models of firm performance and their result confirmed the importance and independence of

both sets of factors in explaining performances. Emerging markets Multinational companies (EMNCs) basically are companies that originate from Emerging markets (developing economies). Malik and Aggarwal [25] opines that it is difficult to develop theoretical arguments about EMNCs without clarifying and explicitly stating what constitutes an emerging market and distinguish them from developed markets (DM). Luo and Tung [24] deducted that Emerging markets multinational companies (EMNCs) are firms engaged in outward FDI, where they exercise effective control and undertake value adding activities in one or more countries. Prior to liberalization, the political economies of developing countries were limited to local markets by adopting import-substitution industrialization strategy. However with trade liberalization, developing countries became more participatory with cross border trades and investments. One major industry that has benefited and still taking advantage of trade liberalization in Emerging market like Nigeria is the banking industry. Oluduro [31], described banking as a business activity of accepting and safeguarding money owned by individuals and entities known as depositors, and lending this money out with objective to earn profit and create financial multiplication in an economy through multiplier effect. He asserts that banking has come a long way in Nigeria, giving three basic phases of banking historical development/evolution in Nigeria as; The era of free and monoculture banking (1892-1954), the era of classical liberalism (1952-1985), and then 1986 to present as characterised by series of structural adjustment, reforms and consolidations in the banking industry for viability and customers/investors confidence in the system. The high prevalent internet fraud activities locally known as yahoo-yahoo in Nigeria has continually discourage online business activities not just in Nigeria but the world in entirety as concluded by [30] in his study; A social technological analysis of cybercrime and cyber security in Nigeria. The basic mode of operation of internet fraudsters is anchored on [23] three asset attributes of Confidentiality, Integrity, and Accessibility. Confidentiality has to do with the privacy of data so that only authorized users (human and machine) can access the data. In the Banking industry where lots of data (corporate and individual) are used, unsecured data transmitted to or from IoT devices and services can be intercepted by cyber criminals and leveraged upon. Cybercrimes centred on confidentiality can be termed Credit card fraud in the banking industry. Integrity is about the verification that data has not been tampered with and that data have been sent by the claimed source. Banks with vulnerable IoT devices and services can unintentionally transmit dubious or malicious data, thus endangering not only the Bank's brand reputation but also customers assets. Such cybercrimes are termed Identity theft. Thirdly, accessibility refers to the allowance of only authorized users to access data and ensuring that those authorized users are not prevented from such access. A breach of this, results to Denial of service for Banks and bank customers that use IoT devices and services of the bank.

2 REVIEW OF RELATED LITERATURE

2.1 Blockchain Technology

Today, Blockchain is viewed as one of the most influential technological advancments in the business sector. Blockchain technology offers commonly agreed record of truth to multiple for mutually distrusting participants in an economic system. Benefits may be derived from removing the requirement for participants to trust a particular person or entity to maintain that record on their behalf, opening the door to more direct, peer-to-peer (or machine-to-machine) transactions or to the independent execution of smart contracts. Thus, the technology could reduce overall friction in the system, cut processing time, lower barriers to entry, and reduce back-office costs involved in reconciling data across organisations. The concept of blockchain was first published by a cryptographer Satoshi Nakamoto in 2008, in a paper that was part of an international response to the 2008 financial crisis. Satoshi strived to create a peer-to-peer payment system without the need of a middleman (third party like financial institutions). It is a technology association with the forth industrial revolution. This was the opinion of [18] when they opine that blockchain is a foundational emerging technology of the fourth industrial revolution, with its defining features as the distributed and immutable ledger with advanced cryptography. These enable the transfer of a range of assets among parties' securely and inexpensively without third party intermediaries. Zhang, Yuan, Hu, NandaKumer, Chopra, Sim and Caro [42] assert that blockchain is a peer-to-peer distributed/shared ledger that immutably records sequence of transactions without need of centralization or trusted entities. Blockchain has potentials to transform transactions with its unique features. It is a decentralized electronic ledger system that produces a cryptographically secured and immutable record of any valuable transaction. The architecture can be harnessed to facilitate per-to-peer payments, manage records, and track physical objects and transactions while transferring value through smart contracts. It has given fillip to new solutions to problems that existed decades ago. Blockchain and smart contracts has given rise to new solutions for ancient problems in emerging markets [17]. To explain the technicalities and operationality of blockchain, transactions are grouped into blocks and the blocks appended to the distributed ledger sequentially. Every block has a cryptographic hash of the previous block. It is practically impossible to tamper with blocks/transactions that are recorded on the blockchain without detection. Chatterjee and Chatterjee [10] conceptualized blockchain as a consensus oriented secured distributed public/private ledger which stores data over a peer to peer network. They further explain the operation of blockchain to include "endorsement" and "validation" of transactions that must be done by parties involved using private and public keys as the case maybe. There are different types of blockchains. It can be private, public or hybrid blockchain. In private blockchains (permissioned),participants or validators must be authorized by the owners of the blockchain. But in public blockchains, transactions can be validated by anyone and there is no access control. The hybrid blockchain on the other hand, combines both private and public blockchain characteristics. Blockchain has many benefits that it brings to the table in the present day economy. However, just as it has many benefits, it also comes with a lot of challenges. Buttressing this point, (Herweijer et al [18]) highlight the following benefits and challenges of blockchain:

Benefits

- Enables decentralization in peer-to-peer transactions.
- Increased transparency, tracking and traceability.
- Immutable, reliable and shareable ledger of

transactions.
- Reduced transaction costs via disintermediation and automation.
- Promotes dynamic pricing.
- Access to markets for investors and issuers especially non-traditional assets.
- Enables effective monitoring, auditing and compliance.

Challenges
- Adoption challenges.
- Technological barriers.
- Security risks.
- Legal and regulatory challenges.
- Interoperability risks.
- Energy consumption challenges.

2.2 Cyber Security

Yokohama [41] defined cyber security as a measure guaranteeing safe and secure usage of the internet. Dissecting the two words into cyber and security, cyber derived from cybernetics means "skill" or "taking the helm". It was originally described as commingling of life-forms and information systems in a networking condition. However, contemporarily cyber suggest "internet", meaning international network. Whereas security management according to [41] is defining the conditions necessary to maintain a system, including sequence of activities maintaining the conditions factors with potentials to cause deviation from the conditions to maintain a specified system are deemed "threats". Conditions to be maintained ordinarily would be those ensuring normal continuation of business activities, with all threats causing deviation from these business activities viewed as business risk. Some risk factors are reduced, avoided or accepted. Concretely, cyber security is simply part of overall corporate security management. Businesses must take cyber security measures as they address other security management issues. Cybersecurity measures would also be termed activities against cybercrimes. According to [15], hacking is the originating term of cybercrime. They described hacking as an activity of modifying products or procedures to alter their normal function or to fix a problem. The term was first used in the 1960s to describe the activities of a certain Massachustts Institute of technology (MIT) model train enthusiasts who modified the operation of their model trains. These individuals later worked on early computer systems by learning and changing the computer code that was used in early programs. Some of their hacks became so successful and outlived the original products such as the UNIX operating system developed as a hack by Dennis Ritchie and Keith Thompson of Bell labs. Malicious association with hacking became pronounced in the 1970s as reported by [15] when early telephone systems became a target. Hackers impersonated system operators, searched through bell telephone company garbage and found secret information, later performed experiments on telephone hardware in order to exploit the system. In 1986, the systems administrator at the Lawrence Berkeley National Laboratory, Clifford Stoll observed irregularities in accounting data. Thus invention of the first digital forensic techniques, he determined that an unauthorized user was hacking into his computer network. The Berkeley lab intrusion was followed by the discovery of the Morris worm virus created by Robert Morris a Cornel University student. This virus damaged more than 6000 computers and resulted in estimated damages of USD 98 million. This innovative crime type was a difficult issue for law enforcement, due to lack of legislation to aid criminal prosecution and a shortage of skilled investigators in the technology that was being hacked. United States congress passed its first hacking related legislation; the federal computer fraud and Abuse act of 1986. This act made computer tampering a felony crime punishable by jail term and monetary fines. Then in 1990, during the project; operation sundevil, Federal Bureau of Investigation (FBI) agents confiscated about 42 computers and over 20,000 floppy disks that were used by cyber criminals for illegal credit card transactions and telephone services. Pariyani [33] opines that cybercrime means a crime committed by an act or omission in the violation of law forbidding or commanding it and for which punishment is imposed on conviction. (Anah et al [6]) asserts that cybercrimes are offences committed against individuals or groups of individuals with a criminal motive, with intentions to destroy the reputation of the victim or cause physical/mental harm to the victim directly or indirectly with the help of modern telecommunication networks like internet and mobile phones. It has some impacts which include; socio-political impacts, emotional impact, loss of sales for private and public sector businesses, cost of security protection and many more. (Anah et al [6]) itemized some of the effects of cybercrime to include:

a. Reduction of competitive edge of organizations
b. Time wastage and slow financial growth
c. Slow production time and more overhead cost
d. Defamation of organizational image

Similarly, [33] gave some impacts of cybercrime as:

a. Potential Economic Impact: Involvement of losses in millions of dollars per year.
b. Impact on market value
c. Impact on Consumer Trust.
d. Effect on National security.

Cybercrimes come in different forms. Some of the types of cybercrimes as enunciated by [33] are as follows:

a. Crackers: Criminals with intention of causing loss to the victim to satisfy some anti-social motives or for fun.
b. Hackers: Criminals that gain access into the computer system or data base of victims to get personal information hidden in those computer systems.
c. Pranksters: These criminals perpetrate tricks on others with no intention of any particular or long lasting harm.
d. Career criminals: These criminals adopt cybercrime as their career and make part or all of their income from crime. In different cases, they form alliance with others or work within organized gangs like the mafia.
e. Cyber terrorists: They attack websites, phone books, mail accounts, and others by sending malware, like Trojans, viruses, worms and the like to victims in order to disturb their database. Their purpose is to weaken the information technology infrastructure of countries, making them unreliable for prospective investors and individuals who wish to become part of such victim country's IT system.
f. Cyber bulls: This set harasses victims through the

internet. They send defamatory mails, vicious posts and make such statements through the internet which causes harassment in any form to the victim.

g. Salami attackers: They attack through internet for the commissions. Their main aim is to make a little alteration in single cases which become unnoticed generally. For example a bank employee acquires and inserts a program into bank's servers which deducts small amount from the account of every customer automatically, such act is generally unnoticed, but the overall gain by the criminal results into huge loss for the victims.

2.3 Emerging Markets Multinational Corporations (EMNCS)

According to [7],the term emerging markets (EMs) was first introduced in 1981 by the International Finance Corporation (IFC) to be new developing stock markets. There are three major variables used to identify emerging markets. They are standard of living of a population measured by the average Gross domestic product (GDP) per capita, the pace of economic growth (measured as the GDP growth rate) and finally the economic policies adopted by governments to maintain economic growth and improve living conditions of citizens [11,36]. Buckley and Casson [9] defined multinational corporations (MNCs) as firms that acquire a substantial controlling power in establishments located in at least two countries, through outward Foreign Direct Investment (FDI). Likewise the international monetary fund IMF [19] and the Organization for Economic Co-operation and development OECD [32] define an MNC as "an incorporated or unincorporated enterprise in which a direct investor, who is a resident in another country, owns about 10 percent or more of the ordinary shares or the voting power". Multinational corporations emanating from emerging markets are called Emerging markets multinational corporations. Mortensen [26] notes that EMNC based in Africa have received noticeably less attention, relative to those domiciled in other continents. Most EMNCs relevant studies are done on firms based mainly in Asia. Furthermore, (Estrin et al [14]) conclude that EMNCs from countries that are highly urbanized are most likely to internationalize, highlighting the importance of urbanization forces in the study of emerging market firm's behaviour.

2.4 Performance

Performance can be categorized into two models [16]. They identified two models of firm's performance as economic model and organizational model. The economic model emphasizes on the importance of external market factors in determining firm success, whereas the organizational model consolidates on the behavioral and sociological paradigm, and views organizational factors including their fit with the environment as the major determinants of success.

They further streamlined the economic model to include:

A. Industry variables (characteristic of the industry in which the firm competes)

B. Variable relating the firm to its competitors

C. Firm variables (the quality and quantity of the firm's resources)

The organizational model in broad term advocates that managers could influence the behavior of their employees (and thus the organizational performance) by considering salient factors such as the formal and informal structure, control and information systems, the planning, reward, their personalities and skills, and the relation of these to the environment. In other words, managers can influence organizational outcomes by establishing context, and the context is the result of a complex set of psychological, sociological and physical interaction.

Hansen and Wernerfelt [16] later integrated the two models of firm performance and their result confirmed the importance and independence of both sets of factors in explaining performances. (Vasanth et al [40]) attempted to develop a model for firm performance based on stakeholder theory by Freeman in 1984. Stakeholder is seen as "any individual or group who can affect or is affected by the achievement of the organization's objectives".Hence, satisfaction of diverse stakeholders is being considered to be a variable for the firm performance.

Many authors and researchers have also identified other forms and determinants of performance. For instance, [40] identified nine determinants for firm performance as;

a) Profitability performance: This includes return on investment, revenue, net income, return on equity, return on assets, economic value added.

b) Growth performance: This has to do with market share growth, asset growth, net revenue growth, net income growth, number of employees growth.

c) Market value performance: this deals with dividend yield, earnings per share, changes in stock price, stock price volatility, market value added (Market value/equity), Tobin's Q(market value/replacement value of assets)

d) Employee Satisfaction: Turn-over, investments in employees' development and training, wages, rewards, policies, career plans, organizational climate, general employee's satisfaction.

e) Customer Satisfaction: mix of products and services, number of complaints, repurchase rate, new customer retention, and general customer's satisfaction, number of new products/services launched.

f) Environmental performance: Number of projects to improve/recover the environment, use of recyclable materials, level of energy intensity, energy management systems.

g) Environmental audit performance; environmental policy, environmental audit report, environmental review.

h) Corporate governance performance; Board size, board independence, outside directors, inside ownership.

i) Social performance; Employment of minorities, number of social and cultural projects, number of lawsuits filed by employees, customers and regulatory agencies.

It is important to note that [40] aver that determinants are multidimensional in that the indicators of different dimensions should not be used interchangeably, since they represent different dimensions of firm performance. Strategies may also have different impacts on the individual dimensions.

2.5 History and Internationalization of Nigerian Banks

The free and monoculture banking era between (1892-1954) was the origin of banking in Nigeria. It dates back to 1892 when the African Banking Corporation(ABC) commenced the activities of banking in Lagos [31]. Also, the British Bank of West Africa (BBWA) by Sir Alfred Jones started operating in Nigeria as a trust fund in 1893. The BBWA absorbed ABC operations in 1894 and in 1957, BBWA was changed to the

Bank of West Africa and then to the Standard Bank of Nigeria in 1965, before finally becoming the renowned First Bank of Nigeria (FBN) in 1979. The Post Office Savings Bank was established under the savings bank ordinance in 1936, and between 1949 and 1952 over ten banks sprang up but did not survive for long with reasons like; inadequate capital base, unskilled or poor management, lack of banking regulation and acceptable prudential guidelines, illiquidity, inexperienced staffing, fraudulent operators, reckless and rapid expansion of branches, and inability to meet the demands of new government regulations. The era of classical liberalism (1952-1985) saw the establishment of many banks with laid down regulations like the 1952 Banking ordinance, and the banking Amendment Act. It marked the beginning of banking regulation in Nigeria. Specialized banks like; Development banks and Merchant banks which include the Nigerian Industrial Development Bank(NIDB), the Nigerian Bank of Commerce and Industry(NBCI), and the Nigerian Agricultural and Credit Bank(NACB) were established. In 1970, there were a total of 14 commercial banks in Nigeria which increased to 29 in 1980. Then the period of (1986 to date), there has been massive expansion and structural changes in the banking sector. By 1991, there were over 120 commercial banks and merchant banks in Nigeria, arising from the deregulation of the economy by the federal government which brought enhanced free-market enterprise and the liberalization of the banking licensing scheme. The deregulation and proliferation of banks since 1986 also came with consequences among which are distresses in the sector owing to mismanagement in the form of grants, bad loans and advances, and then ownership structure. Also, inappropriate corporate governance, inadequate regulatory and supervisory capacity and more played a role in distressing the banks. Between 1994 and 2003, twenty seven banks were extinct because of distress. From 2004 to present, there have been mixed feelings in the sector in line with CBN's directive of twenty five billion naira capital base (paid-up) for commercial banks. The result is that by 2006, only 25 banks remained in existence resulting from reorganizations, mergers, and acquisitions. Banks in Nigeria have tried to improve their capital base, profitability and reach through expanding to various regions in the country. Some of them have also moved internationally; thereby bring the concept of internalization of banks in Nigeria to the fore. Nigerian banks extended into other African countries after the 2004 consolidation that increased minimum capital requirements over tenfold. Most banks extended their operations domestically and internationally by increasing branch networks in the domestic market and opening subsidiaries abroad [3].In recent times Nigerian banks have expanded abroad and set up subsidiaries in several countries in sub-Saharan Africa and beyond [4].At present (September, 2019), according to the data from CBN circulars on commercial banks, Nigeria has 8 commercial banks with international presence. These banks are Access Bank PLC, First City Monument Bank PLC , First Bank Nigeria Limited and Fidelity Bank PLC. Others are Guaranty Trust Bank PLC, United Bank of Africa PLC, Union Bank OF Nigeria PLC and Zenith Bank PLC. Many reasons have been adduced as to why banks move abroad. For instance, [4] identified some things that trigger banks in Nigeria to move abroad to include success of the banking reforms in Nigeria, a business shift in strategic scope of the banks and their desires to exploit tangible and intangible assets in less developed and profitable markets in Sub-Saharan Africa. Similarly, environmental uncertainty in the host markets influenced entry through high equity commitment modes was also found to be a trigger. Other reasons have also be ascribed to moving internationally Some of the common motives for the internationalization of banks as identified by these researchers are:

1. Diversification of risks: internationalisation in order to diversify banks risks.
2. Seeking strategic asset: entering a financial centre in order to access a currency or knowledge.
3. Market seeking: this is done to get to new clients/customers
4. Defensive expansion; this is undertaken to protect existing bank client relations by following clients to their home or new operational country.

3 EMPIRICAL REVIEW

Duah and Kwabena [12] carried out a study to investigate the extent of fraudulent cyber activities on electronic business in Ghana and to obtain the impact of cybercrime on the development of electronic business in Ghana. The study used secondary data collected from the internet, books and papers published by other authors and researchers in related areas over a six month period. A generic inductive approach for data analysis was used to analyse the data obtained. The results revealed that cybercrime is fast gaining ground in Ghana and also, that cybercrime causes direct financial losses to consumers and businesses. The study found the following reasons as why Ghananian youths engage on cybercrime: attempts to meet society's expectations, ambitious lifestyle, and breakdown of social institutions like the family and lack of legislation for culprits. Kyalo and Kanyaru [22] conducted a research on the factors affecting online transactions in the developing countries; A case of E-commerce businesses in Nairobi county, Kenya. This study used secondary data. After analyzing the data, the study concluded that; lack of customer awareness on security risks found in online transactions, increased use of mobile devices with high vulnerabilities also the sophistication and advancement of fraudsters attacks are specifically the challenges in the online transaction. The study further identified robust security systems for detection and prevention of fraud related attacks, continuous detection and conventional protection measures, incident management plans, and regular security assessments as the best practices that can be used to prevent online transaction fraud. Balogun and Obe [8] examine the trends, peculiarities and reasons for the upsurge in e-crime in Nigeria. The study used the conventional content analysis to dissect the various forms of electronic crime (E-crime) and the perpetrators of e-crime. The study concluded from the deductions made that there is a very solid possibility that computer-based crimes will become more common because of increasing sophistication in the use of computers and technologies at large. And that Nigeria is rated as a top member of countries with the highest levels of e–crime activities in Africa.

4 THEORETICAL FRAMEWORK

This study is founded on New Growth Theory. The stimulation of the New Growth theory (Endogenous growth theory) is credited to work of [43]. The theory states that Economic growth results from the increasing returns associated with new knowledge or technology. New growth theory makes a shift from resources-based to a knowledge-based economy. It

emphasizes the point that economic processes which create and diffuse new knowledge are critical to shaping the growth of business firms. The essential point of new growth theory is that knowledge drives growth. The major assumptions of new growth theory are:-

a. It views technological progress as a product of economic activity whereas previous theories treated technology as a product of non-market forces.
b. It maintains that unlike physical objects, technology and knowledge are characterized by increasing returns, and these increasing returns consequently drive the process of growth.

Linking this theory to the study therefore, technological advancements like Blockchain and cybersecurity systems which have been introduced to the business world globally will boost performance of business firms such as internationalized banks in Nigeria if well adopted and adapted into their operations.

5 METHODOLOGY

This study took an exploratory research design format as it seeks to explore the benefits, merits and demerits of Blockchain secured cyber systems on business performance of emerging markets multinational companies. The study was carried out in Nigeria with a population of eight (8) Nigeria banks that have internationalized at the time of survey. Secondary data from these banks, internet crime complaint centre and Africa cyber security Report were sourced and used for inferences and postulations.

6 DATA PRESENTATIONS

Table 1 complainant *statistics by country in 2014*
(Source internet crime complaint centre 2014.)

Rank	State	Complaints	Percent
1	United States	246,620	91.54%
2	Canada	4,074	1.51%
3	United Kingdom	2,103	0.78%
4	India	2,094	0.78%
5	Australia	1,423	0.53%
6	France	896	0.33%
7	Puerto Rico	528	0.20%
8	Brazil	515	0.19%
9	Mexico	475	0.18%
10	China	458	0.17%
11	South Africa	434	0.16%
12	Germany	395	0.15%
13	Philippines	393	0.15%
14	Netherlands	297	0.11%
15	Spin	290	0.11%
16	New Zealand	289	0.11%
17	Pakistan	250	0.09%
18	United Arab Emirates	249	0.09%
19	Israel	243	0.09%
20	Malaysia	240	0.09%
21	Sweden	239	0.09%
22	Italy	232	0.09%
23	Singapore	231	0.09%
24	Nigeria	215	0.08%
25	Saudi Arabia	215	0.08%

Table 1 above shows statistics of complaints for top 25 countries across the globe gathered by the internet crime complaint centre in 2014 from the table above, Nigeria is ranked 24th in complaint entries with total complaints of 215 which is about 0.08% of total complaints recorded in 2014.

Table 2: *Complainant loss by victim country in 2014*
(Source internet crime complaint centre 2014.)

Rank	State	Complaints	Percent
1	United States	$672,080,323	83.96%
2	Canada	$11,838,789	1.48%
3	Australia	$11,149,8800	1.39%
4	Hong Kong	$8,683,462	1.08%
5	United Kingdom	$8,641,506	1.08%
6	Chile	$6,585,354	0.82%
7	South Africa	$6,581,690	0.82%
8	India	$5,888,264	0.74%
9	Spain	$4,651,181	0.58%
10	China	$3,673,131	0.46%
11	Germany	$3,147,174	0.39%
12	Nigeria	$2,999,357	0.37%
13	United Arab Emirates	$2,865,701	0.36
14	Saudi Arabia	$2,157,234	0.27%
15	Mexico	$2,034,155	0.25%
16	Mongolia	$2,005,774	0.25%
17	Republic of Korea	$1,965,255	0.25%
18	Japan	$1,941,273	0.24%
19	Norway	$1,695,877	0.21%
20	Netherlands	$1,659,926	0.21%
21	Sweden	$1,598,282	0.20%
22	Brazil	$1,499,456	0.19%
23	Belgium	$1,487,552	0.19%
24	Singapore	$1,447,133	0.18%
25	Indonesia	$1,307,382	0.016%

Table 2 above shows statistics of losses in US dollars of top 25 countries all over the world in 2014. Nigerian is ranked 12th with a total loss of two million, nine hundred and ninety nine thousand, three hundred and fifty seven dollars ($2,999,357) representing 0.37% of total loss recorded by internet crime complaint centre in 2014.

Table 3 *Breakdown of key statistics for some African countries in 2017(Source- Africa cybersecurity report 2018)*

Country	Population (2017 Est.)	GDP (2017) in USD	Est.Cost of Cyber-crime (2017)
South Africa	1,300,000,000	$3.3T	$3.5B
Nigeria	195,875,237	$405B	$649M
Tanzania	59,091,392	$47B	$99M
Kenya	50,950,879	$70.5B	$210M
Uganda	44,270,563	$24B	$67M
Namibia	2,597,,801	$11B	-
Botswana	2,333.201	$15.6B	-
Lesotho	2,263,010	$2.3B	-
Mauritius	1,269,315	$12.2B	-

From table 3 above, Nigeria with a GDP of four hundred and five billion dollars in 2017 has an estimated cyber crime loss of six hundred and forty nine million dollars in 2017 as recorded by cyber security report 2017.

Table 4 *Africa cyber crime cost for industry analysis in 2017* (Source-Africa cybersecurity report 2018)

Industry	Cyber crime cost (USD)
Banking and Financial Services	$248M
Government	$204M
E-Commerce	$173M
Mobile transaction	$140
Telecommunication	$119M
Other sectors/industries	$194M
Total	$1B

Table 4 above shows that the banking and financial sectors tops the list of industrial loses to cyber crime with a total loss of two hundred and forty eight million dollars ($248m) in 2017 representing 23% of total loss.

Table 5: *Total operating income for Nigeria banks in 2018 (Source –Proshare 2019.)*

S/N	Bank	Amount (Naira Billion)	Percentage (%)
1	Access	114.73	10
2	FBN	113.01	10
3	Union Bank	48.06	4
4	Keystone	19.63	1.7
5	GTB	150.80	13
6	Stanbic IBTC	70.98	6.3
7	Eco Bank	55.90	5.02
8	Diamond	52.57	4.72
9	FCMB	45.51	4.08
10	Keystone	19.63	1.70
11	Standard Charted	53.25	4.78
12	Sterling	38.53	3.40
13	UBA	100.13	8.90
14	Unity	11.38	1
15	Wema	15.75	1.40
16	Zenith	202.92	18
	Total	1,112.78	100

Table 5 above shows the total operating income of Nigerian commercial banks in 2018, with the eight internationalized banks contributing over 65%.
Namely Access bank, fidelity bank, first city monument bank, Guaranty Trust bank, Union bank, United bank of Africa, first bank of Nigeria and Zenith bank.

Table 6 profit *After Tax's among Deposit money banks in 2018 (Source- Proshare 2019)*

S/N	Total Operating income	Amount (Naira Billion)
1	Access	32.27
2	FBN	26.35
3	Union Bank	11.78
4	Keystone	5.90
5	GTB	83.62
6	Stanbic IBTC	26.85
7	Eco Bank	13.97
8	Diamond	5.95
9	FCMB	3.34
10	Keystone	5.80
11	Standard Charted	26.84
12	Sterling	5.69
13	UBA	19.67
14	Unity	0.53
15	Wema	1.82
16	Zenith	86.30

Table 6 above shows the profit after tax of some selected Nigerian banks with the internationalized banks net over 68% of the total profit in the industry.

Table 7: *Gross earning, and Profit After Tax (PAT) for selected Nigerian Banks in 2018. (Source- Proshare 2019)*

.	Banks	Gross Earning	PAT
1	Guaranty	226,632,061,000	95,581,580,000
2	Eti	384,588,000,000	16,900,000,000
3	Zenith Bank	322,201,000,000	81737,000,000
4	Stanbic	114,207,000,000	7,646,000,000
5	Access	253,024,000,000	17,509,000,000
6	FBNH	293,300,000,000	33,500,000,000
7	Diamond Bank	98,200,000,000	2,200,000,000
8	FCMB	64,310,000,000	5,726,000,000
9	UBA	257,918,000,000	43,792,000,000
10	Sky Bank	13,561,734,622	22,491,078,008
11	UBN	83,300,000,000	11,500,000,000
12	Fidelity Bank	88,917,000,000	11,843,000,000
13	Sterling Bank	77,637,000,000	6,214,000,000
14	Unity Bank**	15,742,119,632	443,519,000.00
15	Wema Bank	32,030,000,000	1,570,000,000

Table 7 above shows a comprehensive presentation of the Gross earning, profit before tax and profit after tax of the commercial banks in Nigeria.

7 DISCUSSION

The data tables above show various statistical representations of cyber crime and performance indicators of some selected banks in Nigeria. Some salient take away from the presentations include but not limited to the following:

a) Table 1 and table 2 shows a contradictory representation of Nigeria in the volume of recorded complaints and corresponding volume of losses recorded by victims in Nigerian respectively. Deduction is that more victims have not complained in Nigeria which will further increase the total loss to cyber crime in Nigeria.

b) Table 3 shows that Nigeria is among the top African countries with the bulk of estimated cyber crime losses, this further supports the deduction on (a) above, that more complaints are expected to be recorded in Nigeria.

c) Table 4 identified the banking and financial sectors in Africa as the number one victim industry to cyber crime and this consequently indicate an urgent need for a robust cyber security system.

d) Table 5, table 6 and table 7 show some basic key performance indicators in the banking industry like total operating income, profit after tax (PAT), profit before tax (PBT), and Gross earnings. Expectations are that these values should continuously grow for competitiveness of emerging markets multinational companies like the Nigerian banks. However with the volume of losses estimated on table 2 and table 4 for Nigeria and the

industry respectively, there are indications of likely contraction in operating income and profit if the cyber crime loss growth rate is not urgently checked.

8 RECOMMENDATIONS

Blockchain technology according to [37] has proven to be a-go-to tech for better security. Basically because of the enormous challenge it poses for cyber criminals, when individuals have control over their data. Organizations can leverage on this unique technology quality especially the cryptographical aspect to build robust cyber security systems.

For a start, the internationalized Nigerian banks could go for private blockchains, or a hybrid. This could serve as a beta platform and a test of the technology. Also a feedback system should be designed to evaluate the performance costs minimized with Blockchain cybersecurity systems. This could be achieved by creating a compliant cyber security department to gather and analyze data before and during the implementation of Blockchain secured systems. Emerging markets multinational companies should also improve on data collection for cyber crime incidents, as recorded on tables 1 and 2 respectively; there are discrepancies between reported complaints and losses for Nigeria. Furthermore, strong passwords, encryption and probably factor authentication mechanisms are recommended for company's blockchains to protect users and clients by blocking identity theft crimes which could easily mar the entire blockchain advantage. Also, the decentralization attribute of blockchain technology requires network of computers to constantly exchange information, and run complex algorithms at high speeds. This demands capacity increase both in hardware and energy consumption. Effort should be made to conserve resources in Blockchain implementation especially in energy consumption. Investment in renewable independent energy supply alongside blockchain development will be a major lead in this regard.

9 CONCLUSION

Blockchain for cyber security remains a top cybersecurity measure owing to cryptography. This is majorly because cyber crimes are made costly to perpetrators and thus discourage cyber criminals from their ventures. Emerging market multinational companies in the 4th industrial revolution (industry 4.0) market place have a handful of technological advancements to stay a breast with while maintaining competitiveness with their developed markets multinationals counterparts. Such advancements are cloud computing with internet of things, and a major challenge to those is cyber crime. This is supported by the concluding remarks of [8] in their study E-crime in Nigeria: Trends, Tricks, and Treatment conducted in Nigeria. Unchecked cyber crime could erode profit of an established profitable EMNC as the case of Nigerian banks, especially in a Global cyber space as it is obtainable with the internet today. Identifying and implementing a state of the art cyber security measure as asserted by [22] research on the factors affecting online transactions in the developing countries; A case of E-commerce businesses in Nairobi county, Kenya. Blockchain adoption becomes an imperative. This further supports and adapts the New growth theory as in [43], which states that Economic growth results from the increasing returns associated with new knowledge or technology.

REFERENCES

[1] Abomhara, M and Koien, M. (2015). Cybersecurity and Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal of cyber security. 4, 65-88.

[2] Africa cyber Security Report (2017) by the Africa cyber immersion Centre.

[3] Alade, S. O (2016). Cross-border expansion of Nigerian banks: has it improved the continent's regulatory and supervisory frameworks? BIS Papers No 76, 83-96.

[4] Amungo & Buck, (2017).International Expansion of Nigerian Banks, which Theories of Internationalization Prevailed? Nile Journal of Business and Economics6, 79-96

[5] Amungo, E. and Buck, T. (2017). International Expansion of Nigerian Banks which theories of internationalization prevailed? Nile Journal of Business and Economics 17(6): 79-96.

[6] Anah, B.H., Funmi, D.L. & Makinde, J. (2012). Cyber crime in Nigerian: causes, Effects and the way out. ARPN Journal of science and Technology. 2(7): 626-631

[7] Aybar, B. and Thirunavukkarasu, A. (2005). Emerging market multinational: An analysis of performance and risk characteristics. Journal of Asia-Pacific Business, 6(2), 5-39.

[8] Balogun, V.F & Obe, O.O. (2010). E-crime in Nigeria: Trends, Tricks, and Treatment. The pacific journal of science and Technology. 11(1): 343-355.

[9] Buckley, J.P. and Casson, M. (2009). The Internatisation Theory of the Multinational Enterprise: A Review of the Progress of a Research Agenda after 30 years. Journal of International Business studies. 40(9): 1563-1580.

[10] Chatterjee, R. and Chatterjee, R. (2017). An Overview of the Emerging Technology: Blockchain, 2017 International Conference on Computational Intelligence and Networks Doi: 10,1109/CINE. 2017 33:1-3.

[11] Cortesi, D. and Plantoni, M. (2011). The Internationalization of emerging market firms: Motivations and approaches. University of Bergamo, Italy.

[12] Duah, F. A. & Kwabena, A.M. (2015). The impact of Cyber crime on the development of Electronic Business in Ghana. European Journal of Business and social sciences 4(1):22-34

[13] Dunning, J.H. (1980). Towards an eclectic theory of international production: some empirical tests. Journal of International Business Studies, 11 (2): 9-13.

[14] Estrin, S., Nielsen, B.B., and Nielsen, S. (2016). Emerging market Multinational Companies and internationalization: The role of industry internationalization and home country urbanization. Journal of international management. ISSN 1075-4253.

[15] Florida tech magazine-winter(2019)

[16] Hansen, G.S. & Wernefelt, B. (2007) Determinants of firm performance: The Relative Importance of Economic and Organizational factors. Strategic Management Journal 1.10(5): 399-411.

[17] Haveson, S., Lau, A. and Wong, V. (2017). Protecting farmers in emerging markets with Blockchain. Cornell SC John College of Business, 1(1): 1-19.

[18] Herweijier, C., Waughray, D. and Warren, S. (2018) Building Blockchains for a better planet. World Economic forum, fourth Industrial Revolution for the Earth Series (1): 6-37.

[19] International Monetary Fund (2008). Balance of payments and international investment position manual, Washington.
[20] Internet Crime Report (2014). Internet Crime Complaint Centre.
[21] Internet Crime Report (2018). Internet Crime Complaint Center.
[22] Kyalo, J.K. & Kanyaru, P.M. (2015) Factors affecting the online transaction in the Developing countries. A case of E-commerce Business in Nairobi county, Kenya. Journal of Educational policy and Entrepreneurial Research 2 (3): 1 – 7.
[23] Lin, H and Berbmann, N.W. (2016). IoT Privacy and Security Challenges for Smart Home Environments. Information 7(3):44
[24] Luo, Y. and Tung, R.L. (2007). International Expansion of Emerging Market Enterprises: A Spring board perspective. Journal of International Business Studies, 38(4): 48 1-98.
[25] Malik, O.R. and Aggarwal, R. (2012). The Rise of Emerging Market Multinational Companies (EMNC): A capabilities-based perspective, the third Copenhagen Conference on "Emerging Multinational: Outward Investment from Emerging Economies", Copenhagen Denmark 25-26 october 2012 1-35.
[26] Mortensen, J. (2009). Emerging Multinational: The South African Hospital industry overseas. Danish Institute for international studies. University of Copenhagen.
[27] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer electronic cash system. May 2009.
[28] Nigeria Banks Performace H, 2018. Proshare Economy 1 (187): 1599-8842.
[29] Norton cybersecurity insights report (2014)
[30] Olayemi, J.O.(2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. International Journal of Sociology and Anthropology.6(3):116-125
[31] Oluduro,F.O.(2015). History and Evolution of Banking in Nigeria.Academia Arena.7(1):1-6
[32] Organization for Economic Cooperation and Development (2008) OECD Benchmark definition of foreign direct investment. Fourth Edition 2008 www.oecd.org/day/inv/investentstatiticsandanalysis/
[33] Pariyani, R. (2013). Online crimes and their impacts: A review. Manupatra journal. 2(1): 3 – 19.
[34] Sakr, M. and Jordan, A. (2016). Emerging Multinational Corporations: Theoretical and Conceptual Framework. University of Pretoria working paper: 2016-04.
[35] Sakr, M. and Jordan, A. (2016). Emerging Multinational Corporations: A prominent player in the Global economy. Economic Research Southern Africa (ERSA) (1): 1-38.
[36] Sandberg, S. (2012). Internationalization Processes of small and Medium enterprises: entering and taking off from emerging markets. Linnaeus University Dissertation No. 78 2012. Linnaeus University press.
[37] Sari, A.(2018). Use of Blockchain in strengthening cybersecurity and protecting privacy. International journal of Engineering and Information systems. 2(12): 59-66.
[38] Sumanjit, D. & Nayak, T. (2013). Impact of cyber crime: Issues and challenges. International Journal of Engineering sciences & Emerging Technologies 6(2), 142-153.
[39] United Nations Conference for Trade and Development (2014). World Investment report.
[40] Vasanth, V., Selvam, M., Gayathri, J., Lingaraja, K. and Marxia, S. (2016). Determinants of Firm Performance: A Subjective Model. International Journal of Social Science Studies 4(7): 90-100
[41] Yokohama, S. (2017). Business Management and Cyber Security. NTT Corporation Journal (1): 1-123.
[42] Zhang, W., Yuan, Y., Hu, Y., Nandakumar, K., Chopra, A., Sim, S. and Caro, A.D. (2018). Blockchain-based distributed compliance in Multinational Corporations, cross-border intercompany transactions future of information and communication conference (FICC) 2018 5-6 April 2018/Singapore.
[43] Romer, P.M. (1994). Beyond Classical and Keynesian Macroeconomic Policy. Policy journals 15:15-21.