Journal of Innovative Technology, Vol. 6, No. 2, pp. 31-39, September 2024
http://doi.org/10.29424/JIT.202409_6(2).0003

The effects of blockchain technology penetration testing: Evidence from the emerging economy - Nigeria

Eghe-Ikhurhe Grace Osariemen [1*], Roni Naheed Nawazesh [2], Osei-Assibey Bonsu Mandella [2]

ABSTRACT

Blockchain penetration testing is critical in ensuring that blockchain networks are secured and resilient to cyber threats. Therefore, firms must adopt blockchain penetration testing as a holistic approach focusing on risk management and compliance. Adopting questionnaires based on a sample of 122 firms in Nigeria and analysed with a multiple regression model, the results reveal that blockchain penetration testing has a positive impact on reducing risk and breach of data security in firms that carry out this test, which invariably implies that there will be fewer cyber-attack and no threat to loss of any data and smooth transactions process in the firm. The paper highlights implications for firms supporting the policy-making process in terms of data protection and regulation in financial institutions, the supply and logistics company sector in Nigeria, and other sectors that might want to adopt blockchain technology.

Keywords: Penetration test, Blockchain adoption, system networks, emerging economy.

1. INTRODUCTION

Contemporary technological advances have caused considerable disruptions in sectors, prompting the development of new tactics and business models (Koh et al., 2019). Among the technological breakthroughs, blockchain has emerged as a highly promising technology. Blockchain technology adoption has gained significant attention as an emerging technology in Industry 4.0. Blockchain technology is characterized as a decentralized database of interrelated records that can be exchanged publicly or privately by network participants. Blockchains are ledgers that record transactions in a trustless environment while being safeguarded by cryptographic mechanisms (Gurtu & Johny, 2019). Blockchain technology requires distributed shared ledgers, smart contracts, consensus mechanisms, and cryptographic technology (Pournader et al., 2020; Dolgui et al., 2020). Blockchain's unique attributes distinguish it from centrally managed databases, offering goal achievement, cost reduction, and environmental friendliness, reducing opportunistic and opaque behavior (Mangla et al., 2021; Dong et al., 2023; Cao & Shen, 2022).

Blockchain technology is gaining popularity due to its potential to offer secure, transparent data management solutions and enhance operational efficiency (Rico-Peña, 2023). However, the massive blockchain technology adoption has led to new security threats and vulnerabilities (Rico-Peñan, 2023). The study indicates that blockchain penetration testing can effectively mitigate security threats and vulnerabilities. Blockchain penetration testing is a type of security testing performed on blockchain-based systems to identify and exploit vulnerabilities that could be exploited by attackers (Arsat et al., 2022; Bhardwaj et al., 2021; Dalalana Bertoglio & Zorzo, 2017). It aims to simulate an attack on a blockchain network to find and address weaknesses in its security infrastructure.

Blockchain adoption in supply logistics and financial sectors is in its early stages, with academic research being scarce and fragmented (Alazab et al., 2021). There is a growing urgency to conduct extensive research considering its fast-growing adoption in sectors with the propensity of being hacked if a test is not conducted before its full adoption (Eghe-Ikhurhe & Bonsu-Assibey, 2022; Rakshit et al., 2022; Rico-Peña et al., 2023). Therefore, this research enhances scanty literature on blockchain penetration testing by investigating the benefits and anticipated risks of the system network during penetration testing prior to the full adoption of blockchain technology by firms in emerging economies, especially Nigeria. Blockchain penetration testing is critical for confirming the security and sustainability of blockchain networks in emerging economies. By addressing the unique challenges and adopting a collaborative approach, firms can guarantee that their blockchain networks will remain secure and reliable, supporting the growth and progress of the blockchain ecosystem.

Economic growth in developing nations frequently leads to the adoption of blockchain in practical applications. Blockchain technology has been remarkably adopted in emerging markets. Specifically, $474 million in finance was obtained by African blockchain firms in 2022, a remarkable 429% increase in funding from the $90 million collected in 2021. Furthermore, Africa has the fastest financing growth rate of any region in the world, in contrast to the relatively stable funding levels observed in the United States. This demonstrates the continent's growing importance as a key player in the global blockchain environment. For instance, South Africa, Kenya, and Nigeria embrace cryptocurrencies as a

Manuscript received April 6, 2024; revised May 21, 2024; accepted June 4, 2024.

[1*] Lecturer (corresponding author), Teesside University International Business School, Middlesbrough, UK (email: G.Eghe-Ikhurhe@tees.ac.uk).

[2] Lecturer, Teesside University International Business School, Middlesbrough, UK.

substitute for traditional financial systems amid economic uncertainty, highlighting the continent's potential for promoting blockchain technology and innovation.

The widespread adoption of blockchain in Africa presents potential threats and vulnerabilities to firms' sustainability, necessitating successful penetration testing to mitigate these issues. Indeed, successful blockchain penetration testing is crucial for ensuring security and trust and unlocking its full potential for economic, social, and technological advancements. First, penetration testing helps firms identify blockchain vulnerabilities, increasing trust and adoption. In addition, it addresses privacy and security threats, encourages innovation in new blockchain applications, and finally, can revolutionize industries like finance and logistics by ensuring secure decentralized systems.

Recognizing the potential economic, social, and technological impacts of blockchain technology penetration testing, we examine the impacts, benefits, and risks of blockchain penetration testing in Nigeria. Nigeria is regarded as the largest economy, and the IMF predicted that it would grow to $574 billion by the end of 2023. The Nigerian government adopted the National Blockchain Policy in May 2023, decoupling blockchain technology from cryptocurrency, allowing Nigerians to continue using and benefiting from blockchain technology. For blockchain to provide wider socioeconomic, economic, and technological benefits, a study is necessary on blockchain penetration testing to address threats and security vulnerabilities that arise from blockchain usage. However, we found no empirical studies on the impact of penetration testing on blockchain technology adoption. Therefore, this research fills this important observed gap and contributes to the extant blockchain literature by utilizing a questionnaire based on a sample of 122 financial institutions and supply chain and logistics and analyzed with multiple regression analysis. The findings provide implications to the management of firms considering blockchain technology adoption and those that have adopted it but did not conduct penetration testing.

The article contributes to the ongoing discourse regarding the security of blockchain technology by highlighting the need for and benefits of blockchain penetration testing. In addition, the study shares insights on best practices, considering its potential to improve the overall security and reliability of blockchain systems networks in line with the security through obscurity model.

The paper is divided into various sections: the theoretical review is the first section, followed by the literature review. The third section describes the research methodology used in the study. The fourth section reports findings and discussions. The final section presents conclusions with theoretical and policy implications.

2. LITERATURE REVIEW

2.1 Blockchain Penetration Testing

Blockchain is a distributed ledger technology that can process data and large volumes of transactions at a reduced time, accurately, transparently, and securely (Eghe-Ikhurhe & Bonsu-Assibey, 2022; Kumar et al., 2022). Its application has been used widely in the last decade, especially in supply chain management, the health sector, financial institutions, and SMEs, and findings from these studies have indicated that the benefit has come to disrupt and revolutionize the traditional way of transactions in large volumes in terms of accuracy, transparency and securely (Kumar et al., 2022; Rakshit et al., 2022; Sangeetha et al., 2019; Spanò et al., 2021; Ullah et al., 2022).

According to Arsat et al. (2022), blockchain-based systems are substantially distinct from traditional applications and have distinct testing standards that must be achieved during the testing process. For example, the smart contracts of a blockchain-based technology require testing techniques because their implementation cannot be altered due to the immutable nature of blockchain technology (Bhardwaj et al., 2021; Chiem, 2014; Kushwaha et al., 2022).

Penetration testing prior to blockchain technology adoption helps to protect the firm from the possible hack and/or loss/theft of data. Therefore, in-depth performance testing is essential to ensure the smart contract works as planned (Lal & Marijan, 2021). Arsat et al. (2022) and Koteska et al.(2017) emphasized the various implementation concerns that must be considered while testing blockchain system, and thus incorporate the blockchain platform, be it public or private, the environment structure and assimilation with other systems networks within the firm. Performance is the most critical aspect to consider when implementing blockchain technology. It is, therefore, advised that an exceptionally high volume of transactions should be tested to make certain that the effect of the performance testing is trustworthy (Arsat et al., 2022). Effective and efficient blockchain testing supports a firm in building up and using the technology tightly with the connected structures (Bhardwaj et al., 2021).

During a blockchain penetration test, security professionals use various techniques to identify potential attack vectors, including scanning for open ports, analysing network traffic, and testing the system's response to common attack methods. Once vulnerabilities have been identified, the tester will attempt to exploit them to gain unauthorized access to the blockchain network and the firm's data (Arsat et al., 2022).

According to (Arsat et al., 2022; Denis et al., 2016; Lal & Marijan, 2021) the main purpose of blockchain penetration testing is to provide organizations with a better understanding of their blockchain security posture and to identify and remediate security issues before they can be exploited by attackers. By performing regular blockchain penetration testing, organizations can ensure that their blockchain networks are secure and that they can quickly detect and respond to any security threats that may arise. Even though blockchain could counter attacks from conventional cybersecurity on the applications from smart contracts, Bhardwaj et al. (2021) explained in their study on the framework of penetration testing that there is an evolving cyberattack that usually appears in the form of new threats and attack trajectories that affect blockchain and this is similar to other web and application based systems.

Smart contracts driven by blockchain technology will make sure that transaction processes are always effectively secure and efficient when compared to conventional contacts. It facilitates a trustless procedure, with time efficiency, transparency, and cost-effectiveness in default of any intervention from a third party or an intermediary such as lawyers (Bhardwaj et al., 2021). Blockchain, as a disruptive ledger technology, comes with security concerns such as irreversible transactions, scarce access, and non-competent strategies, which make the innovation prone to possible attack vectors that are different and could not be easily detected or found on web portals and other applications.

Penetration testing is the oldest technique in evaluating computer system security. The notion behind penetration testing is that the penetration tester is expected to follow a procedure or format as indicated during the test (Alisherov & Sattarova, 2009). There are instruments that are used in penetration testing with blockchain technology, and these tools simply analyze a system, as well as other tools that will actually attack the system to discover any vulnerabilities (Denis et al., 2016). There are numerous utilities that could be used in testing the blockchain security in smart contracts, the framework of Ethereum, and cyber security in a firm, according to (Emery et al., 2021) These utilities are listed below:

1.MAIAN: The MAIAN is a greedy, prodigal, and suicidal test case. The prodigal and greedy test cases deal with cryptocurrency alone and, therefore, would not be significant to smart contracts election, its accounts, and the blockchain system of reward. The suicidal test case checks for the Ethereum Virtual Machine (EVM) kill op-code that can be called by anyone who will disable the related contract.

2. Mythril: Mythril is a security instrument for analyzing Ethereum smart contracts. It was first introduced at the Hack in the Box Security Conference 2018 (HITBSecConf, 2018) in Amsterdam. Mythril can detect a range of security breaches; Mythril encloses a dozen cases of several that can check for insecure calls from a delegate; it can also detect deprecated opcodes, integer overflow and underflow, and insecure low-level calls.

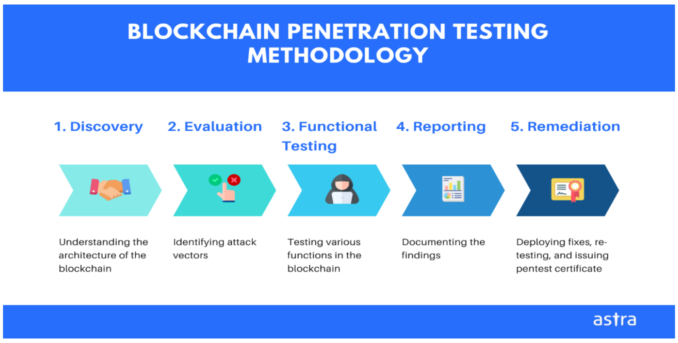
3.Echidna: It uses fuzz testing of smart contract interfaces. Echidna obliges that the targeted smart contracts be improved to assist in invariant testing. This entails producing a counterfoil function that will allow Echidna to affirm the logic in smart contracts to always be true, although sometimes false and could reverse suspected breaches.

Following possible breaches and errors that could occur in integrating blockchain technology, researchers such as (Denis et al., 2016) suggested that it is pertinent to test blockchain technology before fully integrating it into a firm's information technology systems, which is referred to as penetration testing. The potential benefits of penetration testing are that it assists in protecting the firm's network systems and reveals potential security challenges (Denis et al., 2016). Penetration testing, as explained by Denis et al. (2016), is a replication of a potential system attack to authenticate the security of a firm's network system or its environment and to evaluate the extent of the attack if it occurs.

The test could be executed physically by utilizing hardware or social engineering. The main objective of the test is to observe, under extreme situations, the behavior of the firm's network systems or its personnel devices so that the testing team can identify the weaknesses and exposures to system breaches. Therefore, a penetration test can be done manually or automated with a software application. Whichever means the procedure will include gathering information on the targeted network system (before the full adoption of blockchain) before the test (exploration), identifying any potential access points, trying to break in (either through virtual or real), and reporting feedback of the findings. The key purpose of blockchain penetration testing is to ascertain the security weaknesses of the blockchain technology that needs to be improved on before full adoption (Denis et al., 2016; Arsat et al., 2022; Bhardwaj et al., 2021; Emery et al., 2021; Kushwaha et al., 2022; Lal & Marijan, 2021).

In every firm their operations involve a large volume of data and transactions, there is a high attraction for hackers to want to infiltrate their data (Bhardwaj et al., 2021; Denis et al., 2016), especially when the firm wants to adopt a new technology to improve its security network, these firms are habitually affected by security breaches, risks to cyber-attacks and firms from emerging countries adopting the blockchain technology is growing in manifold (Mahamood et al., 2023). In summary, a blockchain penetration test is a decentralized application system security audit (Rahman, 2020) of a network of systems that use blockchain technology owing to the numerous benefits of blockchain technology such as transparency, immutability, security, and be used in different spheres of operations such as e-voting, land ownership, (Eghe-Ikhurhe et al., 2023; Rahman, 2020; Yermack, 2017). It was specifically carried out to uncover and solve any vulnerabilities in the installation after adoption before a malevolent user, or hackers exploit the loophole(s).

Blockchain penetration testing entails a step-by-step process of integration by the testing team of innovation into the firm's technological systems. According to Astra, there are five basic steps in blockchain penetration testing that a firm that is adopting the innovation is expected to take. These steps are Discovery, Evaluation, Functional Testing, Reporting and Remediation. Below is a diagram of the methodology of the steps proposed by Astra (2021) on blockchain penetration testing.


BLOCKCHAIN PENETRATION TESTING METHODOLOGY
1. Discovery
2. Evaluation
3. Functional Testing
4. Reporting
5. Remediation
Understanding the architecture of the blockchain
Identifying attack vectors
Testing various functions in the blockchain
Documenting the findings
Deploying fixes, re-testing, and issuing pentest certificate
astra

Source: (Astra 2021)

2.2 Discovery

Discovery is the first step in a penetration testing method. it is simply the discovery of probable vulnerabilities in the network system before full installation and adoption of the blockchain technology. It is imperative to understand how the blockchain works with the firm's application to know how secure it will be the adoption of blockchain technology. During the discovery stage, the following are taken into cognizance by the tester team: (1) Blockchain architecture to be implemented: The tester team is expected to evaluate the blockchain application to make sure the blockchain's competence to retain confidentiality, availability, and integrity, throughout the running of the system network, to fulfilment the purpose of adoption, as well as the storage of the firms' data. (2) Compliance preparedness: The tester team should be mindful that they must safeguard the blockchain installation and ensure that the implementation process complies with the legal requirements of the governance structure in the firm. (3) Assessment Readiness: The tester team should be properly trained and understand the expert and thorough knowledge of blockchain technological features and Blockchain applications so that they can ensure the most profitable security and practices of the technology.

2.3 Evaluation

The next step after the discovery process in blockchain penetration testing is evaluation. This stage entails evaluation and the analysis of the knowledge gained in the discovery stage. This evaluation will support the testing team to determine what exposure or gap could place the blockchain technology application in a position of risk. This step entails the following tests: testing on the network penetration, testing on the blockchain integrity, and static and dynamic blockchain application testing, which includes logic application, testing wallets, and databases. These attack vectors pointed out above will be properly analyzed to make sure that the security mechanisms are in a position to identify, improve, and sufficiently review the access.

2.4 Functional Testing

A functional test is implemented to ensure that the services used in the blockchain technology application are running as expected. The elements brought into consideration by a blockchain penetration testing team are as follows: (1) Size of a block and the chain: A block comprises the data in a transaction. Presently, the size of a typical block is about 1MB. This estimate needs to be consistently checked. Additionally, there is no restriction on the chain size as it continues to increase with time. It is, therefore, crucial to test the operational performance of the chain to maintain it under continuous check. (2) Addition of blocks in the chain: Additional blocks could be added during the penetration testing process; these blocks can be added to the chain by the testing team and validated after the transaction has been verified and authenticated. (3) Transmission of data: As a result of peer-to-peer architectural features of Blockchain, it will make it simpler for the testing team to make the encoding and decoding of data faultless (4) Application Programming Interfaces (API) Test: API test is carried out to maintain a safety check on the interface of the Blockchain technology application system. It is made to ensure that the requirements and reactions sent through the APIs are valid. (5) Integration Testing: Integration testing is carried out in the penetration functional step to make sure that the various sections of the blockchain interact with each other flawlessly. The necessity for integration testing occurs because of the distribution of blockchain around similar platforms. (6) Testing Performance: The intent of performance testing is to establish the probable bottlenecks that may occur in the functional testing phase and to verify if the blockchain technology application is prepared to be thrust into production or not. (7) Security Testing: The intention of executing the security testing is to make sure that the blockchain technology application is secure against all malware and viruses that could possibly attack the network systems if not checked (8) Reporting stage: Blockchain Penetration testing is not complete without a comprehensive penetration testing report. The testing team ensures that the report prepared comprises a meticulous outline of every vulnerability and exposure encountered in the blockchain technology application. A perfectly explained penetration testing report will make it easily for the cyber security specialists to utilize the required security practices when holding in mind the loopholes found during the testing stage (9) Remediation & Certification: The final step in the blockchain penetration testing is to remediate the susceptibilities stated by the system security professional and possibly request for a re-scan if there is a need for it.

Considering the specific type of blockchain, this study suggests permissionless or public blockchain that can influence penetration testing. A permissionless blockchain allows anybody to join the network, make transactions, validate blocks, and contribute to the consensus mechanism. This openness creates significant issues for penetration testing because the network is decentralised and potentially anonymous. This paper briefly explains how a permissionless blockchain can affect the penetration testing process. (1) Decentralized nature: Because the network is dispersed among several nodes in a permissionless blockchain, it is challenging to pinpoint a single point of entry for penetration testing. Penetration testers must evaluate the security of different nodes and participants while considering the scattered nature of the network. (2) Anonymity and pseudonymity: In a permissionless blockchain, users can maintain total anonymity. Because of this, it may be difficult to link activities taken during penetration testing to particular people or organisations. To find any vulnerabilities, testers might have to concentrate on examining transaction patterns, network traffic, and user behaviour. (3) Smart contract security: Smart contracts, which are self-executing contracts with the terms of the agreement explicitly put into code, are frequently supported by permissionless blockchains. Penetration testers must assess the security of smart contracts and find weaknesses that malevolent parties can exploit. (4) Network openness: Anyone can join the network and take part in transaction validation on permissionless blockchains. This openness may increase the likelihood of attacks and attract malevolent actors. Penetration testers must consider the possibility of network-level vulnerabilities such as Sybil attacks and eclipse attacks.

However, because of its distinct features, blockchain technology has created a new class of attack vectors, such as the 51% Attack, Sybil Attack, Eclipse Attack, and Privacy Attacks. A 51% attack is one in which more than 50% of the network's processing power is possessed by one or a small group of organizations. They can alter, reverse, and possibly even double-spend coins because of this control. An attacker uses a Sybil attack to take over a network by fabricating several fictitious identities or nodes. An attacker can modify transactions and interfere with the consensus mechanism if they control a substantial percentage of the network. Isolating a specific node or set of nodes from the rest of the network is known as an Eclipse attack. By manipulating information flow to and from these nodes, the attacker can cause disruptions to the consensus mechanism and manipulate transactions. Self-executing contracts with pre-established rules inscribed on the blockchain are known as smart contracts. They may, nevertheless, have weaknesses that an attacker could take advantage of. Reentrancy attacks, integer overflows and underflows, and unchecked external calls are a few examples.

2.5 Theoretical review

One theory that can support the use of penetration testing for blockchain is the "obscurity" principle. This principle suggests that security should not rely on the secrecy or obscurity of the system design but rather on the strength of the security mechanisms in place (Stuttard, 2005). In the context of blockchain, this means that the system's security should not be dependent on the secrecy of the blockchain protocol but on the effectiveness of the security measures implemented by the firm to protect it. Penetration testing is an essential tool in evaluating the effectiveness of these security measures by simulating real-world attacks (Mahamood et al., 2023) and attempting to exploit vulnerabilities in the system (Chiem, 2014; Dalalana Bertoglio & Zorzo, 2017; Rico-Peña et al., 2023). By identifying and remediating these vulnerabilities, the blockchain can be made more secure, and the risk of cyber-attacks can be reduced.

Moreover, the blockchain's decentralized and distributed nature presents unique security challenges (Eghe-Ikhurhe & Bonsu-Assibey, 2022; Dorri et al., 2017), making it even more important to conduct thorough and regular penetration testing to ensure that all aspects of the system are protected. Overall, penetration testing is a vital part of ensuring the security of blockchain systems, and it can help firms identify and remediate vulnerabilities before they can be exploited by malicious actors.

2.6 Methodology

This study uses a quantitative methodology in its data collection and analysis. The purpose of using the quantitative method was to get many eligible participants who could respond to the designed questionnaire at their convenience time as the selected participants are usually very busy, and scheduling an interview will be very difficult if the study were to be a qualitative one. Data were measured from the variables collected from financial institutions and supply and logistics firms in Nigeria that were chosen for the study. The quantitative method yielded an excellent result with standard structured questions that were interpreted the same way for all eligible participants (Burns & Burns, 2008).

The research randomly sampled IT personnel, delivery personnel, and managers of financial institutions and Supply and logistics firms adopting blockchain technology in Nigeria. Notably, we selected supply and logistics and financial institutions, believing that these firms would benefit from penetration testing prior to full blockchain technology adoption in their firm as these are at the forefront amongst the various sectors in Nigeria that have more firms using blockchain technology.

The questionnaires were issued to respondents for 6 months, from October 2022 to March 2023. IT personnel, delivery personnel, and managers of supply and logistics and financial institutions were selected based on their experience, training, and knowledge of penetration testing prior to blockchain technology adoption in their firm, and some of the respondents were part of the penetration testing team as well as the outcome of its expectation were approached through their firms and their experience based on the outcome and impact of the testing phases.

The designed questionnaire consisted of four parts. The first section asked six questions on demographic questions, with the remaining sections asking questions related to blockchain penetration testing (Six items), benefits of penetration testing (six items), and penetration test risks that might be encountered (six items). It is worth noting that these questions were self-developed and measured on the 5-point Likert scale ranging from strongly disagree, which is option 1, to disagree, which is option 5 strongly. The question contained a cover letter explaining the constructs and the purpose of the research to the participants. First, the questionnaires were designed, and they were confirmed to be adequate according to experts' opinions in the field of information and communication technology, fintech, and specifically, the blockchain technology penetration tester team. The questionnaire was sent to the eligible participants through the HR, PR, and publicity departments of the chosen firm used for the study. Participants were ensured of confidentiality and anonymity.

Out of 340 questionnaires distributed to eligible respondents, we received 129 responses. However, we included 122 responses after excluding the incomplete response, representing 35.8%. Of 122 responses, 67.2% were males, leaving the remaining 32.8% as females. 48.4% of respondents were employees in the department of ICT, 33.6% in the supply and logistics department, and 18% were managers. In addition, over 50% of respondents work in financial institutions, 44.3% have working experience of 6 –10 years, 53.3% have a first degree, and 46.7% have a postgraduate degree. Table 1 below reports the summary of the respondent's profile.

Table 1 Respondents' Profiles

Description	Profile	Frequency	Percentage (%)
Gender	Male	82	67.2
	Female	40	32.8
Age	18 – 25 Years	25	20.5
	26 –35 Years	59	48.4
	36 – 45 Years	38	31.1
	Above 45 Yrs.	0	0
Educational Qualification	Graduate	65	53.3
	Postgraduate	57	46.7
Job Role	ICT	59	48.4
	Supply and logistic	41	33.6
	Managers	22	18.0
Sector Working	Financial Sector	71	58.2
	Supply and logistic	51	41.8
Experience	1 – 5 years	23	18.9
	6 – 10 years	54	44.3
	11 – 15 years	39	32.0
	Above 15 years	6	4.9

3. DATA ANALYSIS

3.1 Common method bias

The common method bias is often associated with the cross-sectional survey design used for data collection (Bonsu et al., 2023). Therefore, the study calculated CMB by adopting the Harman single factor analysis, considering our study collected data from a single source. The results show 24% below the threshold of 50% (Bonsu et al., 2023), indicating that there is no concern about common method bias from the data collected (Kock, 2020). Before conducting the reliability and validity of the study variables, the study assessed the sample fitness of the data collected using the Kaiser Meyer Olkin (KMO). The result shows a significant value of 0.68, greater than the 0.6 minimum threshold for any sample adequacy (Hidayah et al., 2020).

3.2 Reliability and Validity

After testing the sampling adequacy and common method bias, we ran validity and reliability constructs of the variable used for the study using factor loading, Cronbach alpha, composite reliability, and average variance estimates. Factor loading shows the variance that is explained by the variable on that factor with a threshold of 0.5 and over. Results reveal that all factor loadings for all the constructs outstrip the threshold of 0.5. For example, the factor loadings for the penetration test range from 0.665 to 0.745, which shows the validity of the constructs (Thorndike, 1987). Cronbach Alpha for all constructs exceeded the acceptable threshold of 0.7, indicating the acceptance of the internal reliability of the study (Daud et al., 2018; Pallant, 2020).

Further, the composite reliability exceeded 0.8 thresholds, confirming the convergent reliability of the constructs. In addition, the average variance estimates (AVE) values show 0.541 for the blockchain penetration test and 0.512 for benefits, and the Risk is

0.510, which is higher than the acceptability limit of 0.5. This also further specifies that the disparity recorded by the items in the questionnaire was significantly greater than the variations caused by measurement error (Raykov, 2012; Mandella et al.., 2023). Table 2 reports the findings.

Table 2 Validity and reliability test

Construct	Items	Factor loading	Cronbach Alpha

Blockchain penetration test
AVE= 0.541
CR=0.814
	PT1	0.775	0.710

	PT2	0,543	
	PT3	0.745	
	PT4	0.651	
	PT5	0.512	
	PT6	0.604	
Benefits of Penetration test AVE= 0.512 CR=0.801	BPT 1	0.593	0.737
	BPT2	0.625	
	BPT3	0.629	
	BPT4	0.583	
	BPT5	0.715	
	BPT6	0.649	

Risk management.
AVE= 0.510
CR=0.862
	RISM1	0.740	0.742

	RISM2	0.703	
	RISM3	0.739	
	RISM4	0.633	
	RISM5	0.747	
	RISM6	0.740	

The table presents validity and reliability results where CR represents Composite Reliability; PT represents Penetration Test, BPT represents Benefits of Penetration Testing, and RISM is Risk management.

4. DISCRIMINANT VALIDITY

We tested discriminant validity. Table 4 shows that correlations between the constructs are significantly less than 0.6. The study assumed that the correlations between variables bigger than 0.90 might suggest a common method bias. Importantly, the authors assess discriminant validity using the Fornell and Larker AVE metric. For the Fornell and Larker AVE metric model to achieve its criteria for discriminant validity, the average variance estimates square root of the latent variable must be larger than the correlations across all model dimensions to be used (Bonsu et al, 2023). The AVE square root for all constructs (diagonal of Table 3) is higher than their correlations. Therefore, discriminant validity was found between the two constructs. Moreover, all AVE square roots are larger than correlations among all variables (evidence in Table 3). Henceforth, the study will accept the discriminant validity.

Table 3 Descriptive and discriminant results

	CA	AVE	PT	BPT	RISM
PT	0.710	0.541	**0.712**		
BPT	0.737	0.512	0.406	**0.613**	
RISM	0. 742	0.510	0.477	0.508	**0.622**
Mean			5.13	6.10	4.76
Std Dev			0.410	0.471	0.401

Table CA represents Cronbach Alpha, AVE represents Average variance estimates, PT represents penetration test, BPT represents Benefits of penetration testing, RISM is Risk management and Std Dev represents Standard deviation.

4.1 Empirical Results

This study examines the blockchain adoption penetration test on its benefits and risks considering financial institutions and supply and logistics companies in Nigeria. Multiple regression was used to test the data collected and the hypothesis because the data set was limited. Table 4 reports the estimation spotlight and the empirical evidence from the regression model used. The results reveal that there is a significant relationship, and it benefits a firm in carrying out a penetration test prior to full adoption of blockchain technology. The penetration test also helps to erase or minimize the cyber threat or loss of data as well as data breaches.

Table 4 Empirical results

Hypothesis	Estimates	Std err	T statistics	Supported
PT to BPT	0.261***	0.0037	5.913	Yes
PT to RISM	0.287***	0.0041	6.215	Yes
Adjusted R-Square	0.58			

The positive impact shown in the table above suggests that blockchain penetration tests will significantly enhance data security in a firm by 0.58%. This result is in line with the security through obscurity" principle that states that security should not rely on secrecy or obscurity of the system design but rather on the strength of the security mechanisms in place (Stuttard, 2005). Additionally, it indicates that the threat of data breaches or theft in a firm will be less than half the other could account for compliance and monitoring systems network. Furthermore, this will validate (Arsat et al., 2022) that highlighted the benefit of carrying out a penetration test as it eliminates clogs in the network of the system, eradicates the threat of data loss/breach in a firm, and erases the possibilities of hackers into the system network. The findings are new and will contribute to research in blockchain penetration tests prior to full adoption in an emerging economy, as many studies reviewed were mainly theoretical (Arsat et al., 2022; Bhardwaj et al., 2021; Mahamood et al., 2023), and none from Africa.

5. CONCLUSIONS AND IMPLICATIONS

Blockchain penetration testing is a critical process that helps organizations identify vulnerabilities in their blockchain systems and applications. This testing involves a thorough examination of the blockchain infrastructure, including nodes, smart contracts, and APIs, to identify potential security weaknesses that could be exploited by attackers. The main objective of blockchain penetration testing is to find vulnerabilities that can be used to compromise the integrity, confidentiality, or availability of the blockchain system. By performing penetration testing, organizations can proactively identify and remediate vulnerabilities, thereby improving the overall security of their blockchain infrastructure system. Generally, blockchain penetration testing is an important part of any comprehensive security program for blockchain-based systems and applications, and it should be conducted to ensure ongoing security and compliance are not compromised in the firm. Using financial institutions and the supply logistics sector, the research examined the effects of blockchain penetration testing on the benefits of a blockchain penetration test and risk management. The results find that blockchain penetration testing has a positive and significant effect on the benefits of penetration testing and risk management. This study's unique contribution is to provide fascinating insights into the empirical impact of penetration testing on risk management and its benefits. Therefore, the study concluded that regular penetration testing is important because the blockchain system constantly evolves, and new vulnerabilities can be introduced as new features are added or changes are made. Apart from a few theoretical works in Fintech research, we offer the first scholarly investigation of blockchain technology based on the "obscurity" principle on blockchain penetration testing. In addition, we conclude that by conducting regular penetration testing, firms can stay on top of potential security challenges and ensure their blockchain system remains secure. Penetration testing should be conducted by trained and experienced professionals who can simulate real-world attacks and attempt to exploit vulnerabilities in the system. The penetration team should also have a deep understanding of blockchain technology and its unique security challenges, such as the decentralized and distributed nature of the system.

Importantly, the paper supplies policy implications. First, blockchain and cryptocurrency laws and regulations are still in the formulation stage in Nigeria, this study therefore recommended that blockchain penetration testing be a mandatory requirement for organizations that are implementing blockchain technology or utilizing blockchain-based solutions, and the results of these tests should be reported to relevant authorities, stakeholders, and customers and feedback made on continuous improvement basis. This policy recommendation is based on the need to ensure the security and integrity of blockchain systems, especially in sensitive and critical applications such as financial services, healthcare, and supply chain management.

In addition, the policy should encourage collaboration between organizations, regulatory bodies, and industry associations to share knowledge and best practices related to blockchain security and penetration testing. Furthermore, Penetration testing also promotes transparency and accountability in the blockchain ecosystem, facilitating the establishment of standards and best practices. It encourages the adoption of secure blockchain technologies, fostering innovation and driving the growth of trusted decentralized applications.

In line with the theoretical framework of the study, the study recommends that security measures should be implemented to protect the blockchain system, and penetration testing should be used to assess the effectiveness of these measures. By identifying and remediating vulnerabilities, the blockchain can be made more secure, and the risk of cyber-attacks can be reduced by relying on the secrecy or obscurity of the blockchain protocol to ensure security is not a reliable approach.

Furthermore, penetration testing helps detect potential faults in smart contracts and consensus mechanisms, allowing developers to refine and optimize blockchain protocols, resulting in safer and more efficient decentralized apps.

6. LIMITATION AND FURTHER STUDIES

The study is novel and uses a survey; thus, future studies can use interviews or a mixed methodology and compare results. Additionally, the study is carried out in an emerging economy using a survey; often, surveys might suffer from low response rates, especially in specialized fields like blockchain penetration testing in Nigeria; further studies could be done in a developed economy that has a high rate of blockchain adoption.

7. ACKNOWLEDGMENT

We wish to acknowledge the Journal of Innovative Technology for giving us the platform to submit our carefully researched paper on the effects of blockchain penetration testing in an emerging economy. We also wish to thank the reviewers and editor for taking the time to review our manuscript and provide feedback that has supported us in getting the paper accepted for publication.

REFERENCES

Alazab, M., Alhyari, S., Awajan, A., & Abdallah, A. B. (2021). "Blockchain technology in supply chain management: an empirical study of the factors affecting user adoption/acceptance. " *Cluster Computing,* **24**(1), 83-101. https://doi.org/10.1007/s10586-020-03200-4.

Alisherov, F., & Sattarova, F. (2009). "Methodology for penetration testing." *International Journal of Grid and Distributed Computing,* **2**(2), 43-50.

Arsat, N., Bakar, N. S. A. A., & Yahya, N. (2022, September). "Testing in Blockchain-based Systems: A Systematic Review." *In 2022 10th International Conference on Cyber and IT Service Management* (CITSM) (pp. 1-6). IEEE.

ASTRA. (2021), https://www.getastra.com/security-audit/blockchain-penetration-testing/ accesses 17 February 2023.

Bhardwaj, A., Shah, S. B. H., Shankar, A., Alazab, M., Kumar, M., & Gadekallu, T. R. (2021). "Penetration testing framework for smart contract blockchain." *Peer-to-Peer Networking and Applications,* **14**, 2635-2650.

Bonsu, M. O. A., Wang, Y., & Guo, Y. (2023). "Does fintech lead to better accounting practices? Empirical evidence." *Accounting Research Journal,* **36**(2/3), 129-147.

Bonsu, M. O. A., Guo, Y., & Zhu, X. (2024). "Does green innovation mediate corporate social responsibility and environmental performance? Empirical evidence from emerging markets." *Journal of Applied Accounting Research,* **25**(2), 221-239.

Burns, R. P., & Burns, R. (2008). *Business Research Methods and Statistics Using SPSS. SAGE.*

Cao, Y., & Shen, B. (2022). "Adopting blockchain technology to block less sustainable products' entry in global trade." *Transportation Research Part E: Logistics and Transportation Review,* **161**, 102695.

Chiem, T. P. (2014). *A study of penetration testing tools and approaches* (Doctoral dissertation, Auckland University of Technology).

Dalalana Bertoglio, D., & Zorzo, A. F. (2017). "Overview and open issues on penetration test." *Journal of the Brazilian Computer Society,* **23**, 1-16.

Daud, K. A. M., Khidzir, N. Z., Ismail, A. R., & Abdullah, F. A. (2018). "Validity and reliability of instrument to measure social media skills among small and medium entrepreneurs at Pengkalan Datu River." *International Journal of Development and sustainability,* **7**(3), 1026-1037.

Denis, M., Zena, C., & Hayajneh, T. (2016, April). "Penetration testing: Concepts, attack methods, and defense strategies." In 2016 *IEEE Long Island Systems, Applications and Technology Conference (LISAT)* (pp. 1-6). IEEE.

Dolgui, A., Ivanov, D., Potryasaev, S., Sokolov, B., Ivanova, M., & Werner, F. (2020). "Blockchain-oriented dynamic modelling of smart contract design and execution in the supply chain." *International Journal of Production Research,* **58**(7), 2184-2199.

Dong, C., Huang, Q., Pan, Y., Ng, C. T., & Liu, R. (2023). "Logistics outsourcing: Effects of greenwashing and blockchain technology." *Transportation Research Part E: Logistics and Transportation Review,* **170**, 103015.

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). "Blockchain for IoT security and privacy: The case study of a smart home." In 2017 *IEEE international conference on pervasive computing and communications workshops (PerCom workshops)* (pp. 618-623). IEEE.

Eghe-Ikhurhe, G. O., & Bonsu-Assibey, M. O. (2022). "The effects of blockchain technology on corporate governance: Evidence from emerging economy." *Management Dynamics in the Knowledge Economy,* **10**(3), 239-250.

Eghe-Ikhurhe, G. O., Roni, N., Bonsu, M. O. A., & Chen, X. (2023). "The relevance of blockchain based voting adoption in governance structure: evidence from Nigeria." *International Journal of Economics, Commerce and Management,* **11**(1), 1-21.

Emery, S., Chow, C. E., & White, R. (2021). "Penetration testing a us election blockchain prototype." *Electronic Voting (E-Vote-ID),* 82-97.

Gurtu, A., & Johny, J. (2019). "Potential of blockchain technology in supply chain management: a literature review." *International Journal of Physical Distribution & Logistics Management,* **49**(9), 881-900.

Hidayah, N. A., Utami, M. C., & Fajrisani, N. (2020, February). "Measurement of Public Service Applications Quality Using the Electronic Government Quality (E-GovQual) Framework. " *In 2nd International Conference on Islam, Science and Technology (ICONIST 2019)* (pp. 106-109). Atlantis Press.

Kock, N. (2020). "Harman's single factor test in PLS-SEM: Checking for common method bias." *Data Analysis Perspectives Journal,* **2**(2), 1-6.

Koh, L., Orzes, G., & Jia, F. J. (2019). "The fourth industrial revolution (Industry 4.0): technologies disruption on operations and supply chain management." *International Journal of Operations & Production Management,* **39**(6/7/8), 817-828.

Koteska, B., Karafiloski, E., & Mishev, A. (2017, September). "Blockchain implementation quality challenges: a literature." *In SQAMIA 2017: 6th workshop of software quality, analysis, monitoring, improvement, and applications* (Vol. 11, p. 2017).

Kumar, A., Mangla, S. K., Kumar, P., & Song, M. (2021). "Mitigate risks in perishable food supply chains: Learning from COVID-19." *Technological Forecasting and Social Change,* **166**, 120643.

Kumar, S., Raut, R. D., Agrawal, N., Cheikhrouhou, N., Sharma, M., & Daim, T. (2022). "Integrated blockchain and internet of things in the food supply chain: Adoption barriers." *Technovation,* **118**, 102589.

Kushwaha, S. S., Joshi, S., Singh, D., Kaur, M., & Lee, H. N. (2022). "Systematic review of security vulnerabilities in ethereum blockchain smart contract." *IEEE Access,* **10**, 6605-6621.

Lal, C., & Marijan, D. (2021). "Blockchain testing: Challenges, techniques, and research directions." *arXiv preprint arXiv:2103.10074.*

Mahamood, A. K., Malik, M., Ruhani, A. B., & Zolkipli, M. F. (2023). "Cybersecurity Strengthening through Penetration Testing: Emerging Trends and Challenges." *Borneo International Journal eISSN* 2636-9826, **6**(1), 44-52.

Pallant, J. (2020). "SPSS survival manual: A step by step guide to data analysis using IBM SPSS." Routledge.

Pournader, M., Shi, Y., Seuring, S., & Koh, S. L. (2020). "Blockchain applications in supply chains, transport and logistics: a systematic review of the literature." *International Journal of Production Research,* **58**(7), 2063-2081.

Rahman, M. (2020). "General overview of the blockchain technology. Investigation of its security issues and its practical uses." *In Proceedings of the XII International scientific-practical conference «INTERNET-EDUCATION-SCIENCE»(IES-2020), Ukraine, Vinnytsia,* 26-29 May 2020: 188-189.. ВНТУ.

Rakshit, S., Islam, N., Mondal, S., & Paul, T. (2022). "Influence of blockchain technology in SME internationalization: Evidence from high-tech SMEs in India." *Technovation,* **115**, 102518.

Raykov, T. (2012). "Evaluation of latent construct correlations in the presence of missing data: a note on a latent variable modelling approach." *British Journal of Mathematical and Statistical Psychology,* **65**(1), 19-31.

Rico-Pena, J. J., Arguedas-Sanz, R., & Lopez-Martin, C. (2023). "Models used to characterise blockchain features. A systematic literature review and bibliometric analysis." *Technovation,* **123**, 102711.

Sangeetha, R., Harshini, B., Shanmugapriya, A., & Rajagopal, T. K. P. (2019). "Electronic health record system using blockchain." *Int Res J Multidiscip Technovation,* **1**(2), 57-61.

Spanò, R., Massaro, M., & Iacuzzi, S. (2023). "Blockchain for value creation in the healthcare sector." *Technovation,* **120**, 102440.

Stuttard, D. (2005). "Security & obscurity." *Network Security,* **2005**(7), 10-12.

Thorndike, R. L. (1987). "Stability of factor loadings." *Personality and Individual Differences,* **8**(4), 585-586.

Ullah, N., Al-Rahmi, W. M., Alfarraj, O., Alalwan, N., Alzahrani, A. I., Ramayah, T., & Kumar, V. (2022). "Hybridizing cost saving with trust for blockchain technology adoption by financial institutions." *Telematics and Informatics Reports,* **6**, 100008.

Yermack, D. (2017). "Corporate governance and blockchains." *Review of finance,* **21**(1), 7-31.