Sustainable Social Development (2023) Volume 1 Issue 3
doi: 10.54517/ssd.v1i3.2309

Asia Pacific Academy of Science Pte. Ltd.

ORIGINAL RESEARCH ARTICLE

Attaining the sustainable development goals using blockchain-based cybersecurity

Emmanuel Okewu*, Pius Onobhayedo, Desmond Moru

Department of Computer Science, Pan-Atlantic University, Lagos 100001, Nigeria

*** Corresponding author:** Emmanuel Okewu, okewue@yahoo.com

ABSTRACT

Sustainable development, or sustainability, refers to meeting the needs of the present generation while not compromising on the needs of the future generation. Cyberspace has increasingly become a tool for actualizing sustainable development, given the increased volume of online transactions. However, cyberspace has equally been used to perpetuate crime and criminality, culminating in high levels of corruption in society. Corruption thrives in secrecy in governance, weakens state institutions, and promotes injustices in society, making the actualization of Sustainable Development Goal 16 (SDG 16) a mirage. Since SDG 16 is the cornerstone for the actualization of the remaining 16 SDGs, this vision paper proposes a blockchain-based cybersecurity system for engendering transparency and accountability in governance, using Nigerian politics as a case study. We used use case diagrams and n-tier component diagrams to explain how the functionalities of blockchain technology can be used to address trust deficits occasioned by crime and criminality. We also harped on how the implementation of the proposed system can impact the attainment of the SDGs by the target year of 2030.

Keywords: blockchain; corruption; cybersecurity; sustainable development goals; transparency

1. Introduction

Transparency in governance has been identified as a key factor in tackling corruption and freeing up public resources for meaningful development[1,2]. Illicit financial outflows and diversion of public resources for personal gains have adversely affected the delivery of justice, peace, and strong institutions advocated in the United Nations Sustainable Development Goal 16[3]. In the absence of these fundamentals, the foundation of sustainable development is threatened, and attainment of the other 16 SDGs by the target year 2030 is a mirage[1].

The social contract between leaders and the led makes it imperative for followers to submit their authority and taxes to a select group of persons who are trusted to, in turn, provide security and amenities for the welfare and wellbeing of the citizens. However, empirical evidence abounds about fiscal indiscipline, culminating in the looting and diversion of scarce public resources for personal gains, particularly in developing economies[4,5]. Statistics from global transparency outfits like Transparency International indicate that developing countries have the poorest transparency records with high corruption cases[1]. Though various

ARTICLE INFO
Received: 22 September 2023 | Accepted: 16 October 2023 | Available online: 20 December 2023

CITATION
Okewu E, Onobhayedo P, Moru D. Attaining the sustainable development goals using blockchain-based cybersecurity. *Sustainable Social Development* 2023; 1(3): 2309. doi: 10.54517/ssd.v1i3.2309

approaches have been adopted to nip graft in the bud, such as the launch of re-orientation agencies and programs, as well as the setting up of anti-corruption agencies, the problem persists[6]. Researchers and other stakeholders concur that participatory and inclusive governance are key to the institutionalization of transparency in public finance. The argument of this school of thought is that what affects all should be tackled by all[7].

The spate of corrupt practices seems to have increased with the increased use of technology for driving political governance activities (the Internet, social media, and corruption). There are reports of cybercrimes in public finance[8]. Online transactions are heavily compromised for personal gains[4,5]. Also, cyberspace is dominated by misrepresentations, misinterpretations, and distortions of facts and figures in political governance[9]. The bottom line is that cyber tools are not only used to steal the commonwealth of the citizenry; they are also used to distort political governance perception[10]. The resultant effect is a trust deficit and an infrastructural deficit in the political body, which negatively affect justice, peace, and the building of strong institutions for the attainment of other SDG targets[11].

In a bid to address cybersecurity in online transaction governance, this study proposes a model that is participatory and inclusive. Our model uses blockchain technology, a digital technology inspired by collective responsibility and motivated by accountability.

Therefore, the aim of this work is to use blockchain-based cybersecurity to enhance transparency and accountability in online transactions for the purpose of attaining the SDGs. The specific objectives are:

- Show that online transactions are liable to manipulation.
- Evaluate the impact of fraudulent online transactions on the delivery of the SDGs.
- Propose a blockchain system that promotes transparency and reduces criminal activities associated with online transactions.

The keywords for this work are blockchain, corruption, cybersecurity, sustainable development goals, and transparency. As used in the context of this research, a blockchain is a dynamic list of records arranged in blocks that are connected in a secured manner using cryptography, while corruption refers to dishonest behavior exhibited by people in positions of power like government officials or managers. Cybersecurity refers to the act of protecting electronic data from misuse, just as sustainable development goals are a set of actions that are meant to meet the needs of the present generation without compromising on the needs of the future generation. Transparency means openness and accountability in transactions[12,13].

The remainder of the article is structured as follows: Section 2 is a literature review, while in Section 3, we discuss the methodology. In Section 4, we discuss the implications of the proposed system for attaining the SDGs. The paper concludes in Section 5.

2. Literature review

2.1. Blockchain

A growing list of records arranged in blocks which are linked together in a secured fashion using cryptography is referred to as a blockchain[14]. The components of every block include transaction data, a timestamp, and a cryptographic hash of the previous block (**Figure 1**). A Merkie tree is used to represent the transaction data, with leaves representing data nodes.

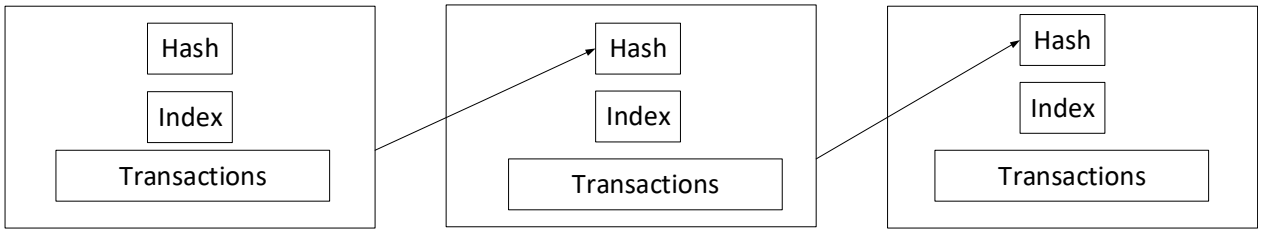

Figure 1. Blockchain diagram.

Figure 1 shows blocks of transactions, with each block containing transaction records. The essence of the timestamp is to prove that at the time the block was published, the transaction data was in existence so as to enable the block of records to get into its hash. Since every block contains information about its previous block, a chain is formed such that each block added reinforces the ones before it. As a result, blockchains resist modification of their data. This is because once recorded, the data in each block cannot be modified retroactively without changing the subsequent blocks.

To manage blockchains, we use a peer-to-peer network so as to guarantee a publicly distributed ledger. In this arrangement, there is collective adherence of nodes to a protocol for communicating and validating new blocks. Despite the fact that blockchain records are not unalterable like forks, they are considered secure by design and exhibit qualities of a distributed computing system with high fault tolerance[15].

The successful implementation of blockchain in the fields of entertainment, social networks, cryptocurrency, and retail has strengthened the advocacy for its implementation in the political and public service domains. The aim is to institutionalize transparent governance using its principles of collectivity and openness[16,17].

The growing quest for transparency and participatory governance for the attainment of sustainable development has forced governments and corporate organizations to embrace the implementation of blockchain technology for secured applications in their respective domains[14]. For successful integration, it is essential to explore the Proof of Work (PoW)-secured algorithms to enhance privacy and integrity in the implementation processes. As an anti-corruption strategy, forensic scientists and research scholars can use blockchain technologies to accurately forecast predictions based on specific identities in law enforcement and financial crime mitigation and eradication. Other blockchain consensus algorithms are Proof of Activity, Proof of Elapsed Time, Proof of Weight, Proof of Capacity, Proof of Importance, Proof of Burn (PoB), Leased Proof of Stake, Practical Byzantine Fault Tolerance, etc. It is important to choose an appropriate algorithm for a given domain as per its business network requirements. This is because blockchain networks will malfunction without the consensus algorithms that verify the individual transactions that are being committed.

2.2. Cybersecurity and political governance

Cybersecurity is also referred to as computer security or information technology security (IT security). It is an initiative aimed at protecting information disclosure from computer systems and networks. It also encompasses the protection of software, hardware, and data from theft or damage. Cybersecurity also ensures that computer systems and networks are shielded from the disruption and misdirection of services that they render[16,17].

Political governance, like any other field of human endeavour, is increasingly experiencing expanded reliance on information and Communication Technology (ICT) with attendant growth in the significance of cybersecurity in the governance space. To guarantee sustainable development for the citizenry, critical stakeholders like governments, non-governmental organizations, and international development partners are increasingly relying on the Internet, computer systems, and wireless networks for policy formulation,

programme implementation, and project evaluation. It is common to find relevant stakeholders in the sustainable development space using wireless network standards like Bluetooth and Wi-Fi to drive adaptable and people-oriented initiatives with a view to promoting creativity, innovation, productivity, and self-reliance. This is complemented by the exponential growth in the use of smart devices such as smartphones, televisions, and component devices of the Internet of Things (IoT).

Stevens[16] and Misa[17] opined that in terms of political usage and technology, cybersecurity has grown in complexity, making it one of the most prominent challenges in our contemporary world. As a result, strategies and policies are being worked out for cybersecurity at the national level[6].

2.3. Crime, corruption and the sustainable development goals

Crime refers to an action or omission which is outlawed and is an offence[10]. It is also viewed as a serious violation of the law and an illegitimate act punishable by the government, just as it is a serious offense that is against morality. On the other hand, corruption is a fraudulent act by those in the corridors of power, which may involve bribery[9]. It also involves changing a word or expression from its original state to a distorted or erroneous state. Both crime and corruption contribute significantly to insecurity in society, hampering economic sustainability, social sustainability, and environmental sustainability. With increased business transactions on the information superhighway (Internet) and social media and their concomitant abuse for promoting crimes and corruption, there is a need to regulate the cyberspace using technologies such as blockchain so that sustainable development policies, programs, and projects at local, national, regional, and international levels can achieve the desired results.

The focus of United Nations Sustainable Development Goal 16 (SDG 16) is to promote inclusive and peaceful societies for sustainable development as well as access to justice for all while building accountable, inclusive, and effective institutions at all levels. Pursuant to achieving this goal, a number of targets have been set: reducing significantly illicit financial flows and recovery/return of stolen assets by 2030 (SDG target 16.4); mitigating corruption and bribery (SDG 16.5); engendering at all levels participatory and representative decision-making (SDG 16.7); widening and consolidating developing countries' participation in global governance institutions (SDG 16.8); and, in tandem with international agreements and national legislation, protecting basic freedoms and guaranteeing public access to information (SDG 16.10). Apart from the United Nations, countries are now adapting policies and strategies for curbing corruption so as to free up resources for national development[6].

The attainment of SDG 16 is critical to the attainment of the other SDGs[18]. Corruption weakens state institutions and paves the way for injustices and the looting of public resources[19]. Tackling corruption will enhance the attainment of SDG 16 and strengthen efforts to achieve SDG policies, programmes and projects being implemented at local, state, national, regional, and international levels.

The United Nations has articulated in SDG 17 the means by which we can successfully implement and resuscitate the instrument of global partnership for the attainment of sustainable development[3]. SDG 17 targets 17.6, 17.7, and 17.8 specifically emphasize the role of technology in this drive, with particular emphasis on the significance of ICT. Our focus in this paper on the use of blockchain technology for tackling cybersecurity challenges like using ICT for aiding and abetting cross-border money laundering and illicit financial flows[20] is therefore to enhance the attainment of the United Nations sustainable development objectives. We acknowledge that a number of digital policies and legal frameworks targeted at curbing crimes and corruption have been formulated in Nigeria, such as the SIM-NIN registration policy[21], TSA policy[22], IPPIS policy[23], GIFMIS policy[24], Whistle-blower policy[25], and Freedom of Information Act[26]. Despite these bold initiatives by the government, criminal and corrupt activities are still being perpetuated in online

transactions for personal gains[4,5]. However, government anti-corruption agencies continue to step up efforts[27,28] even as they concur that technology can be used to solve the problem[29].

2.4. Related work

Ogunjimi et al.[30] investigated the menace of debit card fraud and offered solutions using data mining (DM) technologies. DM is useful for extracting important data and information about debit card users in real-time transactions. The authors observed that despite previous research efforts to stem security issues associated with online transactions, advances in fraud and scam incidences have subdued these efforts. Also, with the large volume of data, traditional fraud detection techniques like discrimination and regression analysis cannot suffice. Hence, the researchers implemented a system for debit card fraud detection using DM techniques to safeguard online transactions. The solution uses the geo-location of customers based on IP address detection and user behaviour to detect debit card fraud. While the graphical user interface of the application was developed using HTML, CSS, Javascript/Fraudulab API, and Swish Mash, the database for the backend was created using PHP and MySQL. Though the work addressed a major cybersecurity concern, the focus was not on using blockchain technology to resolve cybersecurity concerns for enhanced attainment of the SDGs, as done in this current study.

Thach et al.[13] focused on proposing solutions for enhancing the risk management framework of the Vietnam banking system using selected banks. The methodology adopted by the researchers involved using data from the Vietnam Stock Exchange to categorize listed banks into previous private banks (group 1) and previous SOE banks (group 2). Thereafter, the study examined the risk management approaches of Vietnam banks in two separate periods: the pre-low inflation period (2011–2015) and the post-global crisis period (2008–2009). Though faced with varying degrees of risk within these periods, the banks contributed to community activities, as verified by both the quantitative and qualitative methods used in the course of the work. The outcomes of the research indicated that while the capital asset pricing model (CAPM) of group 2 is less than 1, the CAPM of group 2 is greater than 1. Based on the study, the authors recommended ways of improving the risk management processes of Vietnamese banks, just as they outlined the implications for banking policies. Though no mention was made of attaining the SDGs using blockchain cybersecurity as done in our present study, the work bears similarity as it is aimed at tackling risks in the financial sector. Financial deepening impacts on the implementation of sustainable development programmes and projects, as captured in SDG 17. Specifically, finance, technology, trade, capacity-building, and systemic issues were mentioned in SDG 17 as the means of attaining sustainable development.

Shoker[31] opined that blockchain technology (BT) has potential for assisting in the transition to a sustainable society. BT was defined as a novel ecosystem and computing model that engenders trusted digital services as it promotes decentralization and trust. This has resulted in new ways of engaging communities, automating societies, and developing smart digital businesses. The author emphasized that with peculiar properties such as immutability, resilience, trust, decentralization, and automation, blockchain has become a multidisciplinary technology that enables sustainable development. The work shed light on the available variants of blockchain, its rationale, and its core properties. Given its potential for sustainable development, stakeholders like enthusiasts, researchers, and professionals are encouraged to explore the technology for multidisciplinary usage as they intensify awareness of its usage. Our current research aligns with this posture by drawing attention to the use of technology for engendering openness and transparency in public and private sector governance for macroeconomic stability.

Mulligan[7] emphasized that blockchain is a response to dynamics in the present era, just as the technology of the Industrial Revolution responded to societal changes in that period. This is because blockchain promotes

trust, inclusion, and multilateralism from a technical perspective. It ensures that we find new ways to respond through non-governmental organizations, governments, academia, civil society, and international organizations, in line with the fact that we can create fresh solutions to the world's problems by including everyone in the discussion and working together. The author acknowledged that a key issue that needs to be addressed multilaterally is the regulation of digital technologies and suggested the use of blockchain platforms to achieve this objective. This is because blockchain is truly cross-border, as it is not constrained by national boundaries, currency, or technology, and it embraces a multilateral and unified approach to regulation. Hence, civil services globally need to be technically aware as well as understand how regulations are interpreted for proper handling of smart contracts, whose implementation impacts a huge number of people and should therefore be managed across societies. The study argued that with the gradual transition to the global digital economy, citizens' education on data and statistics as part of the open data movement is key, even as blockchain takes it further by requesting citizens to imbibe a new approach to data management. Citizens should also understand key management principles and cryptography in order not to lose their money or be denied government services. In conclusion, it was stressed that we can address emerging technologies by creating appropriate multilateral solutions like blockchain. Since blockchain is a citizen-led and citizen-owned solution to global problems, the international system cannot ignore it. In any case, the focus of the study was not on using blockchain to actualize the SDG targets by 2030 by tackling cybersecurity challenges as done in this current research.

3. Methodology

Though researchers have suggested various ways of ensuring openness and transparency in governance for the purpose of resolving crimes and corruption, our choice of blockchain technique to remedy the situation is based on the following characteristics of the technology, which align with the objectives we intend to achieve:

- Decentralization: BT ensures that information stored is a unit of the whole network without any centralized authority[31]. The information is shared among the nodes.

- Immutability: Blockchain data can only be appended. There is no room for deletion[31]. Consequently, the user can only add fresh annotated data in a bid to fix past transactions. This ensures the traceability of data on the blockchain[7].

- Distributed ledgers: Blockchain belongs to a group rather than an individual and can be public or private. The technology is managed using a peer-to-peer network that collectively adheres to established protocols for validating new blocks and inter-node communication[7].

On the basis of the above findings on BT, we took the following steps to achieve the specific objectives of the present study:

1) We examined the United Nations (UN) requirements for promoting peaceful and inclusive societies for sustainable development, as well as providing access to justice for all and building institutions that are effective, inclusive, and accountable at all levels, as contained in SDG 16[3]. The aim was to ascertain targets to be achieved for sustainable development, such as reducing illicit financial flows (SDG 16.4), mitigating corruption and bribery (SDG 16.5), guaranteeing representative and participatory decision-making, encouraging the participation of developing countries in institutions of global governance (SDG 16.8), and ensuring access to information by the public (SDG 16.10).

2) The study then evaluated the UN technology-based approach to strengthening the implementation and revitalization of sustainable development global partnerships as captured in SDG 17. The specific targets of

this goal include leveraging technology for regional and international cooperation (SDG 17.6), providing environmentally friendly technologies for developing countries (SDG 17.7), and enhancing the use of ICT in developing countries (SDG 17.8).

3) To solve the problem of secrecy and non-transparency in governance that is fueling crime and corruption in governance and online transactions[9,10], we proposed a blockchain-based cybersecurity transparent governance system (BCTGS) as depicted in the use case diagram in **Figure 2**.

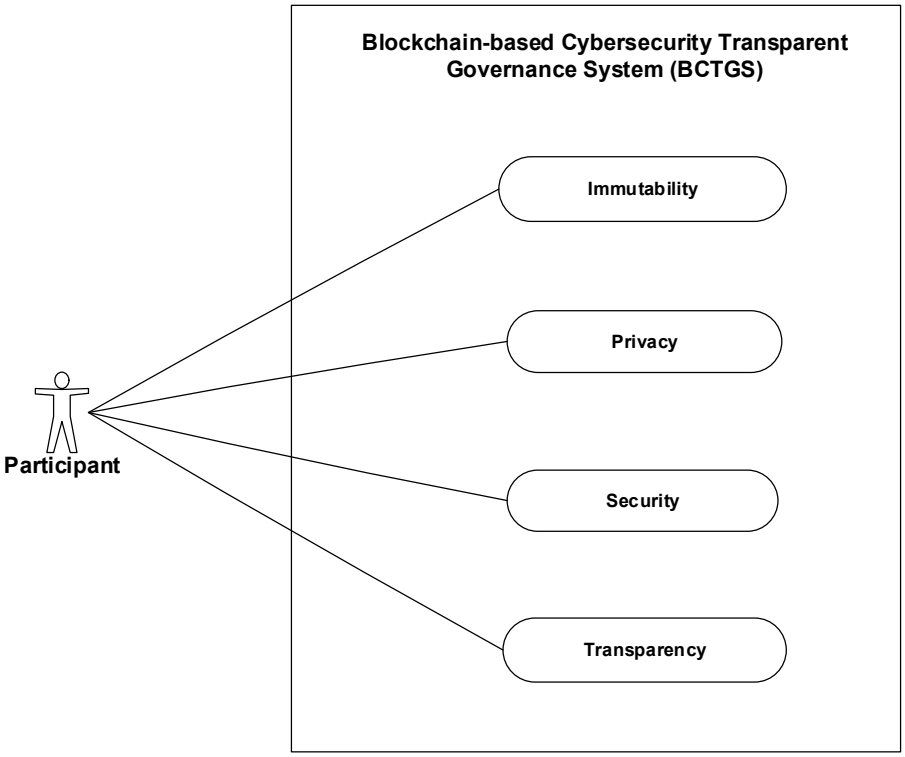

Figure 2. Use Case diagram for the blockchain-based cybersecurity transparent governance system (BCTGS).

Figure 2 contains services which the BCTGS system will offer stakeholders. The strategies for rendering the anticipated services using blockchain platform as shown in **Figure 2** above are explained in **Table 1** below.

Table 1. BCTGS Use Case diagram explained.

System requirement	Blockchain mechanisms	Participant (user) service
Immutability	Consensus protocol Cryptographic hash function	The user (participant) will be able to use the system to add blocks of transactions but will not be able to unilaterally change or delete transaction information.
Privacy	Cryptographic hash function	The user (participant) is assured of confidentiality and privacy of transaction information in the process of using the blockchain-based cybersecurity transparent governance system (BCTGS).
Security	Cryptographic hash function	The user (participant) is assured of the integrity of transaction information.
Transparency	Distributed decentralized database Consensus protocol	Every stakeholder (participant/user) has access to online transaction information readily and is carried along the transaction value chain.

The various components of the BCTGS are shown in the n-tier component-based architecture in **Figure 3** below.

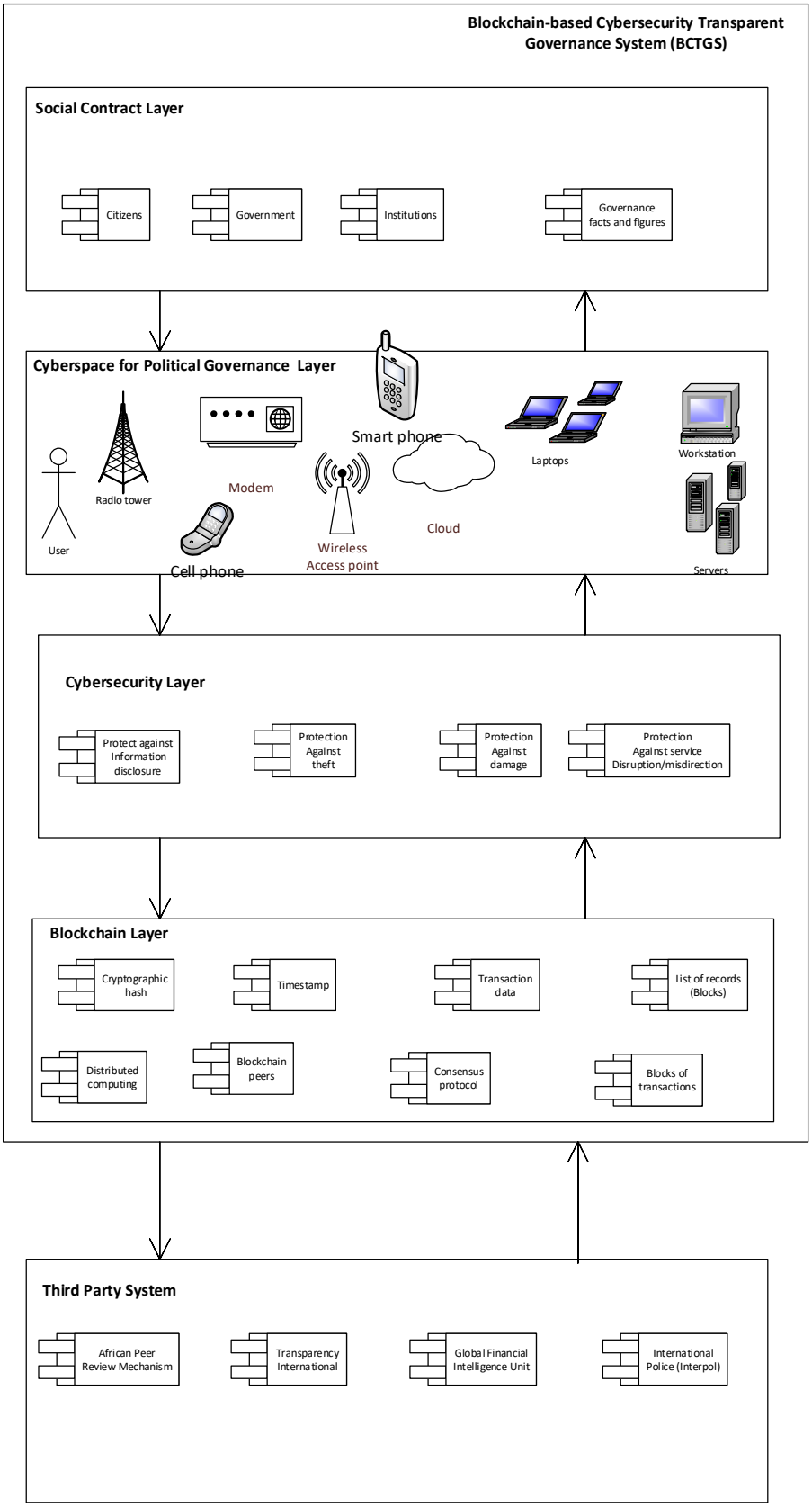

Figure 3. N-tier Component Diagram for blockchain-based cybersecurity transparent governance system.

Figure 3 shows the multiple layers of the proposed system, which are the social layer, cyberspace for political governance layer, cybersecurity layer, blockchain layer, and third-party system layer. The social

contract layer of BCTGS indicates that components like citizens, government, and institutions leverage governance facts and figures to drive sustainable development in society, while the cyberspace layer shows ICT components such as the Internet, smartphones, etc., used to drive interactions among stakeholders. In view of the abuse of cyberspace, the cybersecurity layer hints at protective services that should be rendered against information disclosure, theft, damage, and service disruption/misdirection while the blockchain layer uses functionalities like cryptographic hash, timestamp, etc. to actualize cybersecurity. Because online transactions are a global affair and cyber insecurity is global, the third party system layer specifies that international partnership is needed to tackle problems associated with even local incidences of cyber insecurity. This is because local criminals and corrupt officials collaborate with international networks using ICT components to perpetuate crimes. Blockchain has the capacity to engage both local and international stakeholders in solving global problems[7].

The transparency-related issues addressed in the n-tier component diagram in **Figure 3** are issues that are key to resolving trust deficits in governance and online transactions with a view to restoring trust in the polity, ensuring justice, and building strong institutions for the attainment of the SDGs. These issues include stakeholders' participation, equity, and openness, among others. In **Table 2** below, we explain how the functionalities of blockchain technology address these germane concerns.

Table 2. Transparent governance requirements and blockchain mechanisms matrix.

SN	Governance requirements	Blockchain mechanism	Solution offered	SDG target
1.	Participation of stakeholders	Consensus protocol (algorithm), distributed decentralized network	coming to an agreement, collaboration, co-operation, and mandatory participation. Blockhain ensures mandatory participation of each node in the consensus process. The blockchain is a distributed database of records of all transactions or digital events that have been executed and shared among participating parties. Each transaction is verified by the majority of participants of the system.	Reducing significantly illicit financial flows and recovery/return of stolen assets by 2030 (SDG target 16.4)
2.	Openness in public transactions	Consensus protocol	The Blockchain consensus protocol consists of some specific objectives such as coming to an agreement, collaboration, co-operation, equal rights to every node, and mandatory participation of each node in the consensus process.	Mitigate corruption and bribery (SDG 16.5)
3.	Equity	Consensus protocol	Blockchain ensure stakeholders have equal rights to every node.	Engender at all levels participatory and representative decision-making (SDG 16.7)
4.	Immutability	Cryptographic hash function	Hash function gives security capabilities to the processed transactions, making them immutable.	Widen and consolidate developing countries' participation in global governance institutions (SDG 16.8)
5.	Integrity of transactions	Consensus protocol (algorithms)	Consensus algorithms verify each and every transaction that is being committed.	Mitigate corruption and bribery (SDG 16.5)
6.	Completeness of transaction information	Node/block	Each block or node contains a complete record of all the transactions that were ever recorded in that blockchain. It contains every single record of each transaction.	In tandem with international agreements and national legislation, protect basic freedoms and guarantee public access to information (SDG 16.10)

Table 2. (*Continued*).

SN	Governance requirements	Blockchain mechanism	Solution offered	SDG target
7.	Trust	Hash Consensus algorithm	glues blockchains together and allows them to create mathematical trust. A consensus algorithm is a procedure through which all the peers of the Blockchain network reach a common agreement about the present state of the distributed ledger. In this way, consensus algorithms achieve reliability in the Blockchain network and establish trust between unknown peers in a distributed computing environment.	Enhance international cooperation using technology and innovation and engender knowledge-sharing through global technology facilitation (17.6).
8.	Privacy (Confidentiality)	Hash	Maintains privacy of information.	Enhance international cooperation using technology and innovation and engender knowledge-sharing through global technology facilitation (17.6).
9.	Security	Cryptographic hash function	Ensures security of information in the blockchain network.	Enhance international cooperation using technology and innovation and engender knowledge-sharing through global technology facilitation (17.6).
10.	Scalability	Cryptographic hash function	blockchain hashing using Merkie Tree is useful in enhancing scalability, Scalability is the ability of a system to expand and respond to increasing load.	17.7 Help developing countries by promoting the development, transfer, dissemination and diffusion of environmentally-friendly technologies (17.7)
11.	Authenticity of transaction information	Consensus protocol	Consensus protocol validates and verify transactions. The consensus protocol makes sure that every new block that is added to the blockchain is the one and only version of the truth that is agreed upon by all the nodes in the blockchain.	Engender at all levels participatory and representative decision-making (SDG 16.7)
12.	Collaboration	Consensus algorithm	A consensus algorithm aims at finding a common agreement that is a win for the entire network.	Enhance international cooperation using technology and innovation and engender knowledge-sharing through global technology facilitation (17.6).
13.	Consensus	Consensus algorithm	A consensus algorithm is a procedure through which all the peers of the Blockchain network reach a common agreement about the present state of the distributed ledger.	17.8 Fully operationalize the technology bank and encourage capacity-building for least developed countries using enabling technology such as information and communications technology (17.8)

The ultimate goal is to use blockchain technology to reduce corruption and crimes as well as promote fiscal discipline for the purpose of achieving the SDGs by the target year 2030.

4. Implications of proposed system for attainment of the sustainable development goals

The United Nations has identified means of implementing sustainable development as finance, technology, capacity building, trade, and systemic issues[3]. The specific technology targets are captured in SDGs 17.6, 17.7, and 17.8.

In SDG 17.6, the focus is on enhancing regional and international cooperation in the areas of innovation, science, and technology. This is with a view to fostering knowledge sharing for mutually beneficial global governance and coordination using global technology facilitation, among other mechanisms. SDG 17.7 emphasizes the need for developing economies to have sound technologies by promoting their development and transfer as well as disseminating and diffusing them in an environmentally friendly manner. The full operationalization of the technology bank for least-developed countries is contained in SDG 17.8. Other aspects include science and innovation capacity-building, with particular attention given to the use of enabling technologies like information and communications technology.

However, the massive deployment of ICT by both the citizenry and government to enhance the welfare and wellbeing of people has opened up opportunities for distortion of public information and looting of public resources. Cybersecurity threats have to be tackled for the envisaged benefits of deploying ICT as a means for implementing and actualizing the SDGs by 2030 to materialize.

The n-tier layered component-based system proposed in this study aims at promoting participation and accountability in public and private sector governance and online transactions for optimal utilization of public resources for the greater good of the people. The proposed blockchain system uses a consensus algorithm to ensure that all critical stakeholders in online transactions in the public and private sectors are carried along in the transaction value chain. The blockchain consensus protocol empowers stakeholders to agree, collaborate, cooperate, share equal rights, and ensure the participation of every stakeholder in the consensus process. This implies that the blockchain platform aligns with the principles of transparency and accountability in online transaction governance as an anti-graft measure. This is evident in the fact that its consensus algorithm is aimed at ensuring a common agreement among stakeholders. This offers a win-win for the entire network of stakeholders committed to measuring, monitoring, and evaluating the use of public resources.

By engendering fiscal discipline in public finance through transparency, participation, and accountability, blockchain mitigates corruption, strengthens institutions, promotes justice, and frees up resources for sustainable development. This way, the implementation of blockchain technology in the public and private sectors will strengthen the attainment of the SDGs by the target year 2030.

We have achieved the three (3) specific objectives of the study: the research provided evidence that online transactions can be manipulated; we also showed that misuse of technology in abetting crimes and corruption hinders the attainment of the SDGs; and finally, we explained how mechanisms of blockchain could be used to promote transparency and accountability in online transactions.

5. Further work

In this present study, we have used software engineering models like use case diagrams and component diagrams to design blockchain-based cybersecurity systems that address trust deficits in online transactions. The proposed model is intended to promote transparency and openness in transactions using the functionalities of blockchain. In future work, we will implement blockchain using Python programming. Python is known for its tools and libraries that support blockchain implementation[14,15].

6. Conclusion

Attaining the UN SDGs by the target year of 2030 has necessitated people-oriented projects and programmes across the globe. Researchers have also intensified efforts towards tackling perceived and real challenges militating against the attainment of the SDGS. This study addresses corruption in cyberspace as a contribution. The exponential growth in the use of ICT in governance has led to serious cybersecurity concerns. Besides the distortion of public information on social media, ICT-based procurement processes have been known to be manipulated for personal gains. Another concern is the role of ICT in cross-border illicit financial flows and money laundering. Thriving crimes, corruption, and bribery mean weak public institutions, pervasive injustices, and a lack of peace, which SDG 16 focuses on. The inability to achieve SDG 16, which is the bedrock for actualizing other SDGs, entails the attainment of the entire SDG by the target year 2030. To address this problem, this present study proposes an n-tier component-based blockchain technology solution. We have explained how the mechanisms of blockchain networks can be used to address the requirements of transparent governance and linked such efforts to the actualization of SDG targets. In future work, tools and libraries of a programming language like Python will be used to implement blockchain. This is an area that future researchers can explore.

Author contributions

Conceptualization, EO and PO; methodology, DM; software, PO; validation, EO, PO and DM; formal analysis, EO; investigation, DM; resources, EO; data curation, PO; writing—original draft preparation, EO; writing—review and editing, DM; visualization, EO; supervision, PO; project administration, EO; funding acquisition, PO. All authors have read and agreed to the published version of the manuscript.

Conflict of interest

The authors declare no conflict of interest.

References

1. Transparency International. *Corruption and the Sustainable Development Goals: Shadow Report on SDG 16.4, 16.5, 16.6 and 16.10 for the Netherlands*. Transparency International; 2020.
2. Transparency International. *Monitoring Corruption and Anti-Corruption in the Sustainable Development Goals: A Resource Guide*. Transparency International; 2017.
3. United Nations Economic and Social Council. *Report of the Inter-Agency and Expert Group on Sustainable Development Goal Indicators*. United Nations Economic and Social Council; 2016.
4. Are J. EFCC: How suspended accountant-general diverted TSA, IPPIS funds for personal gain. *The Cable*, 29 July 2022.
5. Omolaoye S. N109bn fraud: How suspended accountant-general compromised TSA, IPPIS, for personal gains-EFCC. *The Guardian*, 29 July 2022.
6. Federal Republic of Nigeria. *National Cybersecurity Policy and Strategy 2021*. Federal Republic of Nigeria; 2021.
7. Mulligan C. Blockchain and sustainable growth. Available online: https://www.un.org/en/un-chronicle/blockchain-and-sustainable-growth (accessed on 1 September 2021).
8. Ademola AE. Impact of agricultural financing on Nigeria economy. *Asian Journal of Agricultural Extension, Economics & Sociology* 2019; 31(2): 1–3. doi: 10.9734/AJAEES/2019/v31i230130
9. Jha CK, Sarangi S. Social media, internet and corruption. Available online: https://www.researchgate.net/publication/262181503_Social_Media_Internet_and_Corruption (accessed on 1 September 2023).
10. Asongu S, Nwachukwu J, Orim SM, Pyke C. Crime and social media. *Information Technology & People* 2019; 32(5): 1215–1233. doi: 10.1108/itp-06-2018-0280
11. Misra A, Okewu E, Misra S, Fernández-Sanz L. Deep neural network model for evaluating and achieving the Sustainable Development Goal 16. *Applied Sciences* 2022; 12(18): 9256. doi: 10.3390/app12189256
12. Hang BT, Huy DT, An PT, et al. Current situation of Bitcoin management and use: Perspectives from the world and recommendations for Vietnam. *Management* 2020; 24(2): 209–235. doi: 10.2478/manment-2019-0054

13. Thach NN, Huy DTN, Nuong LN. Solutions for enhancing risk management mechanism of Vietnam bank system—Case of listed banks. *Revistageintec* 2021; 11(2): 315-326. doi: 10.47059/revistageintec.v11i2.1669
14. Gaurav K. Using Python tools and libraries for blockchain programming. Available online: https://www.opensourceforu.com/2019/08/using-python-tools-and-libraries-for-blockchain-programming/ (accessed on 1 September 2023).
15. Dutta S, Saini K. Blockchain implementation using Python. *Advances in Systems Analysis, Software Engineering, and High Performance Computing* 2022; 123–136. doi: 10.4018/978-1-7998-8367-8.ch006
16. Stevens T. Global cybersecurity: New directions in theory and methods. *Politics and Governance* 2018; 6(2): 1–4. doi: 10.17645/pag.v6i2.1569
17. Misa TJ. Computer security discourse at RAND, SDC, and NSA (1958–1970). *IEEE Annals of the History of Computing* 2016; 38(4): 12–25. doi: 10.1109/mahc.2016.48
18. Okewu E, Ananya M, Misra S, Koyuncu M. A deep neural network-based advisory framework for attainment of Sustainable Development Goals 1–6. *Sustainability* 2020; 12: 10524. doi: 10.3390/su122410524
19. Okewu E, Misra S, Fernadez-Sanz L. Deep neural networks for curbing climate change-induced farmers-herdsmen clashes in a sustainable social inclusion. *Journal of The Problems of Sustainable Development* 2019; 14(2).
20. Shotayo N. How wanted Nigerian carried out over $31m fraud scheme in U.S.-FBI. Pulse.ng, 11 September 2022.
21. Odoh I. I received death threats over NIN, SIM registration-Pantami. *Leadership News*, 16 September 2022.
22. Elike S. Ahmed Idris: How former AGF Stole Funds With TSA. *GIFMIS, IPPIS-EFCC, AllNews*, 29 July 2022.
23. Oyibo E. How suspended AGF, Ahmed Idris Stole Billions by Compromising IPPIS, GIFMIS and TSA. *Abuja Reporters*, 28 July 2022.
24. Odunsi W. N109.5bn fraud: EFCC reveals how sacked AGF Idris stole with TSA, GIFMIS, IPPIS, indicts Yari. *Daily Post*, 29 July 2022.
25. Akinnaso N. Nigeria's whistle-blower policy. *Punch News*, 27 December 2016.
26. Oluwasemilore I. A critical analysis of Nigeria's freedom of information act. *The Gravitas Review of Business & Property Law* 2018; 9(2).
27. News Express. Corruption: ICPC indicts former senior military and police officers, top civil servants. *News Express*, 10 September 2022.
28. Osariemen S. NSA: 54,000 fraudulent payroll entries detected in IPPIS. *The Nation*, 9 September 2022.
29. Ogugua A. Technology Key to Curbing Corruption, Illicit Financial Flows, PRNigeria. *Authoritative and Credible News Platform*, 2 September 2022.
30. Ogunjimi OIA, Oladosu OA, Afolorunso AA, Olukumoro O. Fraud detection using data mining: An overview. *Advances in Multidisciplinary & Scientific Research* 2022; 8(2).
31. Shoker A. Blockchain technology as a means of sustainable development. *One Earth* 2021; 4(6): 795–800. doi: 10.1016/j.oneear.2021.05.014