Blockchain: A Security Solution for the IoT?

Nsima Udoh

***Abstract*—Whenever there are strong statements from people that the Internet of Things ("IoT") causes more evil than good, I wonder if the individuals that belong to such school of thought are inadvertently dismissing the opportunity to continuously extend the capability of an intelligent platform that arguably solves some of the world's greatest problems, made possible using billions of integrated smart devices connectivity. It is my view that the IoT like every other great invention can generally be used for both good and bad reasons, however, careful consideration regarding it implementation and use needs to be put in place. Technological advancements have reached a point where almost everything is wired up or connected wirelessly to the internet and the IoT has created opportunities for people to leverage on the benefits that comes with the interconnectivity of smart devices to collect data and make intelligent decisions. As evident in recent technological innovations, the advent of the IoT has led to significant progress in the field of science and technology. Today, the world has seen the widespread adoption of IP-based networking, breakthroughs in artificial intelligence, development of robotics capability, and the growth of cloud computing. These technological developments and many others are bringing about significant revolutionary changes, suggesting the IoT is as transformative as the industrial revolution. As appealing as these advancements may seem, there are many questions challenging the overall security and privacy aspects of the IoT. This challenge is amplified by other considerations such as the rapid spread of similar IoT devices, the ability of some devices to automatically connect to other devices, and the possibility of deploying these devices in unsecure environments. Even though many security considerations have been put in place to guard against malicious activities targeted against the proper use of the IoT, reoccurring high-profile incidents where a single IoT device has been used to infiltrate attacks to larger network persists. Addressing the security concerns in an IoT environment could be made more effective by the implementation of a security model that has capabilities to negate any central attack to a larger IoT network even when a single point of entry is compromised. Although not without its own challenges, blockchain seems to have this capability, and has arguably drawn attention as the next generation technology that suits the end-to-end security requirements within an IoT environment.**

***Index Terms*—IoT, blockchain, security.**

I. Introduction

Contemporary trend shows that IoT is playing a significant role in human lives, and it will continue to unveil new, brilliant, scientific and technological breakthroughs embedded in the capability of smart devices and applications that are connected to the internet. Ground-breaking inventions manifested in the form of robotics applications, contactless payment systems, big data analytics, artificial intelligence etc. are constantly getting absorbed into the internet, providing an immense amount of information to be accessed at any time and from anywhere. Every day, people see and make use of new smart devices that didn't exist few years back and a number of these devices are able to seamlessly interact with each other from one end of the world to another. As a result, the world has become more reliant on the internet to allow people, systems, and various technologies to communicate with each other.

Many industries are already adopting IoT-based solutions to create new and/or materially improved technologies. In medicine for example, IoT tools have been adopted to enable doctors to effectively monitor patients remotely and administer prescriptions based on information derived from the hospital's IoT environment [1]. To a large extent, IoT is considered by many as the biggest frontier improving humanity in diverse ways, and one could safely opine nothing in the history of information technology is impacting humanity more than the IoT.

As much as these advancements made possible through the adoption of the IoT has brought smiles to the faces of millions of people, it has its own challenges. The issues of data security and privacy, identity theft, IP-based network interception and cross border computer attacks to mention a few, are some of the associated setbacks that come with the many good prospects of IoT, and it is indeed difficult not to imagine the number of threats that will be uncovered as more smart devices continue to interact [2]. Without being overly critical, it is safe to imply that the amount of benefits surrounding the IoT evolution also contributes to its flaws; and as a result, emphatic demands to prevent its misuse are at an all-time high.

Equally, blockchain technology is rising rapidly due to its decentralised, secure, and transparent nature which makes information and privacy breaches difficult and almost technically impossible [3]. IoT solutions using blockchain can be built to address the challenges around information security and privacy at scale due to its ability to manage how critical information is shared and accessed. Blockchain is already being tested and implemented in several industries and it is gradually appearing to be the missing security link in the much-needed IoT environment. Whether it will be the ultimate solution to the IoT's security and privacy concerns in a very consistent way would be known over time.

Subsequent sections of the paper are structured as follows: Section II gives an overview and definition of blockchain. Section III provides a conceptual overview and definition of the IoT, discussing it applications and associated issues. Section IV discusses decentralisation and immutability (including the role of peer-to-peer network) features of blockchain and how they could help to mitigate the security

Manuscript received October 9, 2021; revised December 21, 2021.

Nsima Udoh is with Innovation Reliefs Specialist Group, RSM UK Tax and Accounting Limited, UK (e-mail: nsimaudoh@gmail.com).

doi: 10.18178/ijfcc.2022.11.1.580

challenges in IoT solutions. Section V concludes the paper.

II. Blockchain – Overview and Definition

The idea of blockchain was conceptualised in 2008 when Satoshi Nakamoto, believed to be a person or group of persons with the name "Nakamoto", released a paper, Bitcoin: A Peer-to-Peer Electronic Cash System, outlining the prospects of a direct online payment from one party to another without the use of an intermediary third-party. Despite not mentioning blockchain explicitly, the paper described an approach which combines data structures with several computing concepts and technology to develop an electronic cash system protected through cryptographic mechanisms [4]. Though, work on using cryptographic secured chain of blocks as a computational practical solution for time-stamping digital documents so that they could not be backdated or tampered with was introduced in 1991 by Stuart Haber and W. Scott Stornetta [5], it was Nakamoto's paper that contained the blueprint that most modern blockchain-based systems have adopted. Notably, Bitcoin's (a form of cryptocurrency) underlying architecture is built on blockchain, and it is a good example of an area where blockchain has been adopted since early 2009 when it first began to gain a lot of mainstream attention. Today, blockchain has evolved into one of the modern-day biggest inventions and has found its way into many applications beyond cryptocurrencies, covering numerous fields including financial services, transportation, e-commerce, manufacturing, and medicine amongst others.

In terms of definition, there is still no universally accepted phrase that explains what blockchain really is. What is widely acknowledged is that technologies built on blockchain architecture are showing tremendous potentials and are disrupting the information technology space on a global scale, since they provide a secure solution that cannot be tampered with or controlled by a single entity. [6] defined blockchain as a technology or a distributed database solution that maintains a growing list of data or records that are confirmed by the nodes participating in it. [7] opined "blockchain is a growing record of data or a type of data structure that is replicated on many computers, with these computers having the same information on them", this explains why the technology is resistant to data modification. For [8], blockchain is a technology that contains several lists of immutable blocks which are connected by the means of cryptographic mechanisms, with each individual block having a capability to contain multiple information or transaction, a distinct reference number, a time stamp, and a pointer which identifies an immediate previous transaction as well as the transactions themselves.

Given these definitions, a broadly accepted notion is that a technology that is developed based on blockchain principles and protocols would be decentralised in nature, immutable, irreversible and tamper resistant. While at its core, blockchain is a method of securely storing and distributing information, it is the potential uses of blockchain technology to perform transactions and share information between different parties with undisputable transparency and without a controlling central authority that makes it the real appeal [9].

III. IoT – Overview, Definition, Applications, and Issues

The world is filled with different kinds of smart physical devices. These devices have installed software which can provide specific services based on their architectural designs and can interconnect through numerous means of communication networks to overcome geographical boundaries. These feats were not readily achievable using traditional computing techniques. Today, billions of devices make use of present-day computing capabilities to extend connectivity beyond geographical boundaries to a diverse range of everyday things, such as, traffic light sensors, smart vehicles, and smart homes among others. This exponentially growing number of activities over the internet creates new opportunities and services that can significantly drive businesses, technology, and economic growth.

Given the plethora of interconnection of technological platforms, systems, and applications happening on the internet, defining what the IoT means precisely could be quite difficult as it encompasses a whole lot of events where anything can connect with virtually everything and interact in an intelligent manner. According to [10], the IoT is a system of interconnected objects, people and data collectively referred to as 'Things'. These Things have the capability to combine with intelligent software and hardware services to enable them process and react to information of the physical and the virtual world. In [11], "IoT is theoretically defined as a dynamic information system with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'Things' have identities, physical attributes and virtual traits. These physical and virtual Things use intelligent interfaces and are seamlessly combined into the information system". From the stated definitions, one could deduce that the use cases of the IoT will be endless, and many would agree that the birth of the IoT has provided and will continue to provide a platform for the development of new scientific and technological capabilities. While the IoT has been coined and presented differently by various individuals and professional organisations, a widely accepted view is that the technology will not cease to expand as more things gets connected to the internet, presenting a huge potential for the invention of new applications in almost every domain that one can think of.

In terms of real-world application, many IoT-based solutions have been developed to improve quality of life and to create operational efficiencies in various industries. Some of these applications have grown at an unprecedented pace due to consumerisation effect in the science and technology space while others are thriving rapidly and becoming solidly entrenched in every society. In healthcare for example, IoT has made it possible to develop new tools ladened with latest technologies that enable the remote monitoring of patients. This helps medical practitioners to deliver healthcare and keep patients safe and healthy. Similarly, many ultra-modern IoT tools now allow patients to spend more time interacting with their doctors via the hospital's IoT ecosystem. As a result, relevant information about patient activities can be monitored, collated, and analysed. This in-turn helps to provides vital information that can assist health professionals to respond to patients' needs

quickly and accurately in a manner that save lives faster than the average time. Whether it is the installation of a fitness sensor to monitor a patient heartbeat, or by using surgical robots to perform a series of medical operations, IoT is revolutionising the field of healthcare; making it possible to provide state-of-the-heart solutions for both the patient and healthcare professionals [12].

Within the transportation industry, IoT platform has made it possible for smart traffic lights and cameras to monitor the streets for traffic congestion, accidents, and weather conditions. In this context, the true potential of big data is uncovered as these smart devices and machines enable data in an IoT environment to be monitored, gathered, and subsequently relayed to the transportation management authorities to apply analytics and make intelligent decisions for improved passenger experiences, safety, and efficiency [13].

The IoT has also been useful in the financial services and e-commerce sectors. With rapid digital transformation and growth of mobile technology taking place in these industries, an increase in the use of personal smart devices to access financial institution and e-commerce products and services has helped the industries to generate data that can provide deep insights to consumers behaviour. For example, an IoT-enabled banking application can be used to easily assess a potential customer's expenditure and income to determine their suitability for credit facilities. Also, IoT-based fraud prevention systems implemented in payment devices, such as, contactless debit or credit cards, POS terminals, and ATMs now have smarter authentication features [14]. Illustratively, Apple Inc. and Samsung have incorporated fingerprint compatible applications on their mobile devices to eliminate pin entering process when completing an online transaction, e-commerce giants such as Tencent and Alibaba Group have already introduced facial recognition payments systems (nicknamed, 'pay with your face' or 'smile to pay') in China [15], and a Spanish bank have already rolled out facial recognition technology for authentication when making cash withdrawals at ATMs [16]. Evidently, IoT-based technologies are flourishing, and financial services and e-commerce businesses are leveraging on its benefits and capabilities to minimise the security risks that are prevalent in the sectors.

Arguably, the IoT is now everywhere and connected devices are constantly being integrated into almost every area of our lives. With the number of events taking place via the internet, the sources of information will continue to grow, opening further possibilities to expand the usability range of the IoT. Billions of IoT devices are already connected, with 55.7 billion forecasted to be connected by 2025 [17]. While there are several but differing projections as to the number of connected IoT devices expected to be in the market soon, it is undisputed that there will continue to be a massive shift towards more internet-enabled products. Few examples of real-world IoT applications have been highlighted in this paper, however, it is worth clarifying that the IoT has instigated a flood of many other inventions. If all the tech-inspired shifts unfolding today were ranked in terms of their usability range, IoT will remain one of, if not the only invention that has created a platform for other inventions to flourish.

Conversely, in as much as the IoT has enormous benefits, the problems that come with its implementation and usage cannot be understated. The IoT on its own has in several instances been associated with major cyber-attacks, often involving the abuse of vulnerable connected devices (for example, mobile phones, surveillance cameras etc.) to facilitate malicious activities. Numerous concerns have been raised on how to effectively secure billions of devices connected to the internet. [18] Threat Report notes that 98% of IoT device traffic is unencrypted, suggesting that a vast majority of confidential and personal data on the network is susceptible to all forms of cyber-attacks. Given the likelihood of the exposure of personal data and information to attackers, one could argue that people, organisations, and businesses are wary of the security aspects of IoT-enabled devices and platforms. Even though many businesses have made efforts to tailor the right security requirements to every IoT deployment, a number of risks seen with IoT solutions especially in recent times suggests that the centralised IoT model is no longer fully suitable for the increasing number of IoT devices and applications [19]. To put this into context, a vast majority of IoT enabled products relies on centralised network model whereby all devices are identified, authenticated, and connected through cloud-based technologies. These cloud technologies have huge processing and storage capabilities, and any sort of connectivity between devices will have to exclusively go through the internet regardless of the distance between them. While this approach has connected generic computing devices from time immemorial and will continue to support the rapid growth of small-medium-large scale IoT networks, there is a growing concern that it will not be able to respond to the growing needs of the IoT ecosystems overtime, particularly in security. More so, centralised network design has a single point of failure i.e. they use a single gateway whereby a compromise to a single device can allow access to a whole network. In addition, centralised network models are known to have limited interoperability when it comes to data exchange with other centralised infrastructures – they have limited capability to effectively cater for the dynamically changing / growing requests for end-to-end data exchange across various systems, to provide an ecosystem environment where data interoperability can be achieved at scale without compromising the security requisites of an entire network infrastructure.

Time after time, the world has witnessed major incidents suggesting that the centralised IoT network model is arguably susceptible to security breaches, the *Mirai* incident is one of the examples proving this. The victim was the servers of Dyn, a company that controls a significant part of the internet's domain name system infrastructure. The attack was orchestrated using a software called the *Mirai* botnet. The result was a distributed denial of service attack (DDOS), in which a network of computers infected with special malware, were programmed into bombarding a server with traffic until it collapses under the strain, bringing down major sites such as the likes of Twitter, the Guardian, Netflix, Reddit, CNN and many others across Europe and the USA [20]. Also, in 2018, software flaws in Facebook's systems allowed a security breach that exposed the personal information of nearly 50 million users [21]. Furthermore, in

2018, an investigation into British Airways data breach which led to the details of about five hundred thousand customers to be harvested by attackers revealed that the access to log-in credentials for an employee of cargo-handler Swissport were not securely protected, which ultimately made it less challenging for the hackers to obtain primary access to the British Airways network [22]. These are just few examples where a single system breach exposed the wider network to bigger threats. While it is evident that the advent of IoT has brought about great merits; the problem of its security remains a key concern.

IV. Blockchain – A Viable Solution to the IOT Security Threats?

Blockchain has the potential to remove IoT security concerns in various ways given that it offers a radically different paradigm for storing and managing information on the internet. The decentralised nature of blockchain technology has the capability to negate any sort of central attack which could lead to the compromise of the entire network. In a decentralised system, there is no governing authority or a single person looking after the network, but instead, a group of nodes maintains the network, making it decentralised. In a blockchain system, data is stored on various nodes. Before adding or removing any data on the network, all participating nodes must approve and verify it – this approval process helps to eliminate the single point of failure. Perpetrators of malicious activities would have to target individual nodes on the network to breach the network security. Using a blockchain system or network makes it possible for smart devices to actively participate in the validation process. This means the network would be able to guard against any breach or security compromise by validating predetermined satisfactory behaviour for any anomalies. The decentralisation feature of blockchain technology helps to ensure no change is allowed on a network without a shared agreement from all the network participants. Once a device on the network is identified as not behaving correctly or as it should, it can be readily isolated to prevent it from being used to gain further access to sensitive information. Unlike centralised systems where hackers can target and intercept the information sent between a server and a device, there is no single server or gateway in decentralised systems, meaning that the possibility of a man in the middle attack is mitigated. Nevertheless, with decentralised systems, the shared participation and transparency enjoyed by all participating nodes in a validation process may not necessarily be ideal in every situation or organisation as it advocates an evenly spread authority during decision making. When decision making requires all participating nodes approval and verification, it can get difficult to coordinate the activities across the nodes; as such, a regular or traditional database system may be a viable option. Although recent trends in technology indicates there are strategies (for example, transacting under multiple blockchain addresses) to avoid this problem with blockchains, the more information that is hidden on a blockchain, the heavier the burden to compute, generate and verify its transactions [23].

In addition to the above, the peer-to-peer architecture of blockchain removes the need for an intermediary or third-party authorisation. The distributed peer-to-peer network, when paired with a common consensus requirement, gives blockchains a comparatively high degree of resistance to security breaches. Unlike centralised systems where one need to trust and rely on the integrity of an intermediary, even if one node goes down in a peer-to-peer network other nodes would still be present; thus, making it highly challenging to take down an entire blockchain network. Peer-to-peer blockchain framework, nevertheless, raises few concerns. Instead of a central server (client-server) network approach as with traditional systems, the distributed ledger on the blockchain network is maintained by all other users on the system. This requires a considerable amount of computational power across each node to ensure a better outcome. Even though a peer-to-peer network provides an improved level of security, it significantly decreases efficiency, and this acts as one of the main barriers of implementing blockchain in terms of scalability, costs, and mass adoption [24].

Immutability is another definitive property of blockchain-based systems which promotes transparency and ensures that system resources or data cannot be altered or corrupted. This feature has the potential to incorporate a quick, cost effective and efficient auditing process, and bring more trust and integrity to the data shared or stored on the internet. In blockchain systems, each transaction that is verified and validated by the participants on a network is timestamped and embedded into a 'block' of information, cryptographically secured by a hashing process that connects to and integrates the hash of the previous block, joining the chain as the subsequent chronological update. The hashing process of a new block always incorporates a set of data from the previous block's hash output. This connection in the hashing process makes the chain incorruptible i.e., it is not feasible to alter or delete data after it has been verified, validated, and placed in the blockchain. If attempted, the subsequent blocks in the chain would repudiate the attempted tampering (as their hashes would not be valid). In other words, if data is tampered with, the blockchain will break, and the reason behind it can be readily identified. This characteristic is not found in traditional or centralised systems underpinning most IoT setups, where information can be modified, breached, or deleted with ease [25]. Blockchain as an immutable system clearly has significant security benefits; however, a problem it suffers from is that information written on a blockchain platform cannot be removed. Having an unalterable history of transactions may seem like the answer to many contemporary business problems, and it is, in several ways. But think of what happens when sensitive datais accidentally published or there are records out there that need to be erased if no longer needed. Similarly, think of what happens if an individual living within the European Union wants to exercise their rights of privacy (in-line with the General Data Protection Regulation) by requesting that their information be erased from a system. An immutable system makes it next to impossible to have such information removed given that all or majority of a network participant will have to agree on the terms, which is no small feat. Immutability and distributed control make blockchain a

disruptive technology and they are also the source of blockchain's greatest strengths; however, depending on the scenario, they can also present unintended consequences [26].

Altogether, a critical examination of some key features of blockchain as highlighted above suggests it is a technology that can appreciably improve the security aspects of IoT systems, albeit, it has its own drawbacks like every other emerging invention. While the prospects of merging blockchain with IoT for enhanced security sounds like a match made in heaven, the idea of combining the two technologies is still maturing and requires careful consideration, to achieve a viable outcome. Today, trends within the industry suggest that the adoption of blockchain solutions by mainstream sectors (such as, financial institutions, insurance, supply chain, government) is gaining momentum and the qualities of blockchain technology makes it one of the most revolutionary tools of the contemporary era that can complement the security aspect of IoT systems.

V. Conclusion

Employing three relevant characteristics of blockchain, this paper has highlighted that the technology can be leveraged to enhance the security of the IoT. The security breaches associated with IoT systems makes it clear that there is a need to incorporate a strategy to mitigate the related risks. The principal characteristics of blockchain (such as immutability, decentralisation, peer-to-peer architecture) is generally believed to offer security capabilities in a way that makes cyber-attacks technically difficult to achieve. That said, there are instances where it may be more viable to adopt a centralised or traditional system within an IoT environment.

Blockchain is often expected to provide answers to all challenges associated with IoT security. All the same, there always exists drawbacks alongside the good tidings. No matter the progressions made in the field of technology, be it IoT, blockchain or any other invention, it is safe to say technological advancements will never cease to be consequential either in a positive or negative way. As alluded to above, it is obvious that the IoT will continue to instigate many other inventions and will continue to flourish; nevertheless, associated security vulnerabilities have proven to be detrimental. Implementing blockchain as a security solution for the IoT would by no means guarantee a flawless positive result; however, recent trends have shown that many mainstream sectors are seemingly enjoying the perks of such a robust and reliable technology so far. Therefore, it is essential to find the right approach and strategy that can adequately manage any downsides it has. Between 2017 and 2018 the demand for blockchain engineers in the United States grew by 400 per cent, with technology giants such as, Microsoft, Amazon, IBM and Facebook all recruiting talents in this space [27]. This symbolises a big shift towards a wider adoption of the technology within the IT space. One thing that is undisputed is that blockchain provides capabilities that were not possible in the past, but whether it would effectively cater for the security and privacy flaws tainting the positives that IoT has brought in the most reliable way, only time will tell.

Conflict of Interest

The author declares no conflict of interest.

Author Contribution

The author confirms sole responsibility of conducting the research, analysing the information, and writing the paper.

References

[1] T. K. Jaimon, L.C. Katrina, G. Enying, and C. Paul, "The internet of things: Impact and implications for health care delivery," *Journal of Medical Internet Research*, vol. 22, no. 11, November 2020.

[2] S. Kumar, P. Tiwari, and M. Zymbler, "Internet of things is a revolutionary approach for future technology enhancement: A review," *Journal of Big Data*, no. 111, 2019.

[3] L. Stephan, S. Steffen, S. Moritz, and G. Bela, "A review on blockchain technology and blockchain projects fostering open science," *Journal of Frontiers in Blockchain*, vol. 2, p. 16, 2019.

[4] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," *National Institute of Standards and Technology*, 2018.

[5] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," *Journal of Cryptography*, 1991, vo. 3, pp. 99-111.

[6] J. Yli-Huumo, D. Ko, S. Choi, and K. Smolander, "Where is current research on blockchain technology? – A systematic review," PLOS ONE, October 2016.

[7] L. Popovski, G. Soussou, and P. B. W. Tyler, "A brief history of blockchain," *Legaltech News*, An AML Publication, May 2018.

[8] GSMA. (2018). Distributed ledger technology, blockchains and identity. [Online]. Available: https://www.gsma.com/identity/wp-content/uploads/2018/09/Distributed-Ledger-Technology-Blockchains-and-Identity-20180907ii.pdf

[9] J. Daniel, A. Sargolzaei, M. Abdelghani, S. Sargolzaei, and B. Amaba, 'Blockchain technology, cognitive computing, and healthcare innovations," *Journal of Advances in Information Technology*, vol. 8, no. 3, August 2017.

[10] ISO/IEC JT1. (2014). Internet of things (IoT) preliminary report. (2014). [Online]. Available: https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/internet_of_things_report-jtc1.pdf

[11] J. Chin, V. Callaghan, and S. B. Allouch, 'The internet-of-things: Reflections on the past, present and future from a user-centred and smart environment perspective," *Journal of Ambient Intelligence and Smart Environments*, vol. 11, 2019, pp. 45–69, DOI 10.3233/AIS-180506.

[12] Igor Inc. (2020). IoT in healthcare: Enhancing medical environments with innovative solutions. [Online]. Available: https://www.igor-tech.com/news-and-insights/articles/iot-in-healthcare-enhancing-medical-environments-with-innovative-solutions

[13] A. Lucent, 'The internet of things in transportation," *Build a Secure Foundation to Leverage IoT for Improved Passenger Experiences*, 2020.

[14] N. Joshi. (2018). What are the opportunities for IoT in the finance sector. [Online]. Available: https://www.allerin.com/blog/what-are-the-opportunities-for-iot-in-the-finance-sector

[15] P. Luana. (2020). China's guidelines for facial recognition payments stress biometric data protection' Biometric Updates. [Online]. Available: https://www.biometricupdate.com/202001/chinas-guidelines-for-facial-recognition-payments-stress-biometric-data-protection

[16] CaixaBank. (2020). Press Release: 'CaixaBank deploys ATMs with facial recognition technology throughout Spain. [Online]. Available: https://www.caixabank.com/comunicacion/noticia/caixabank-atms-with-facial-recognition-technology-throughout-spain_en.html?id=42302#

[17] International data corporation (IDC). (2020). IoT growth demands rethink of long-term storage strategies. [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prAP46737220#:~:text=IoT%20Growth%20Demands%20Rethink%20of%20Long%2DTerm%20Storage%20Strategies%2C%20says%20IDC,-SINGAPORE%2C%20July%2028&text=IDC%20predicts%20that%20by%202025,from%2018.3%20ZB%20in%202019

[18] Unit 42. (2020). IoT threat report. [Online]. Available: https://unit42.paloaltonetworks.com/iot-threat-report-2020/

[19] S. Khvoynitskaya. (2020). Blockchain for IoT security – A perfect match. [Online]. Available: https://www.itransition.com/blog/blockchain-iot-security
[20] N. Woolf. (2016). Major cyber-attack disrupts internet service across Europe and US. [Online]. Available: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet
[21] M. Isaac and S. Frenkel, 'Facebook security breach exposes accounts of 50 million users," *The New York Times*, September 2018.
[22] D. K. Morrow, 'Cyberattack probe: How British Airways security flaws let data theft unfold," *Flight Global Premium*, 2020.
[23] G. Greenspan and M. Chain, 'Blockchains vs centralized databases," *Four Key Differences Between Blockchains and Regular Databases*, March 2016.
[24] T. K. Sharma, 'Blockchain and role of P2P network," *Insights and Resources, Blockchain Council*, 2020.
[25] G. Iredale. (2020). 101 Blockchains, '6 Key blockchain features. [Online]. Available: https://101blockchains.com/introduction-to-blockchain-features/#prettyPhoto
[26] M. Somers, 'The risks and unintended consequences of blockchain," MIT Management School, June 2019.
[27] United Nations Conference on Trade and Development (UNCAD). (2021). Technology and information report 2021. [Online]. Available: https://unctad.org/system/files/official-document/tir2020_en.pdf

Nsima Udoh received the B.Sc degree in computer with electronics with First Class Honours from Lead City University, Ibadan, Nigeria, in 2009, and a postgraduate masters degree in international relations and security from the University of Westminster, London, United Kingdom in 2011. Currently, he is an R&D associate director (software specialist), working as part of the Innovations Reliefs Specialist Group at RSM UK Tax and Accounting Limited, United Kingdom. He is directly involved in providing technical advice on innovation reliefs for software development and ICT projects. He is a member of the IEEE, IAENG, IACSIT and United Nations Association of Great Britain and Northern Ireland. His main area of research includes emerging technologies and 'responsibility to protect'