https://doi.org/10.51470/IJNS.2024.01.03.28

Crossref

NSF Nature Science Foundation PROTECT NATURE Regd.No. 114/2017

International Journal of Nature Science (IJNS)

Estd:2024

BLOCKCHAIN: AN IOT SECURITY SOLUTION

M.Jayakeerthi & Divya Jose J
Assistant Professor
Department of Computer Science
Nehru Arts and Science College,Coimbatore.

Article History

Volume:1, Issue:3, 2024

Received: 27th August, 2024

Accepted: 18th September, 2024

Published: 30th October, 2024.

Check for updates

Abstract: *The Internet of Things (IoT) has the potential to improve the capabilities of an intelligent platform by connecting billions of connected smart devices to solve global problems. However, careful consideration is needed in how it is used and implemented. Advancements in technology have led to the growth of cloud computing, robotics, IP-based networking, and artificial intelligence, making the IoT as disruptive as the Industrial Revolution. However, there are concerns about the security and privacy of the IoT, which are exacerbated by the rapid spread of related IoT devices, the possibility of using them in unsafe situations, and the ability of certain devices to automatically connect to other devices. High-profile incidents where a single IoT device is used to launch attacks into a larger network persist despite numerous security measures. To address security issues in an IoT context, a security paradigm that can stop any central attack on a larger IoT network, even if just one point of entry is compromised, may be necessary. Blockchain has shown potential in this regard, and despite its challenges, it has garnered interest as the newest generation of technology that conforms to end-to-end security criteria in an IoT setting.*

Keywords: *IOT, Block chain, Security Solution.*

Authors citation: M.Jayakeerthi and Divya Jose J BLOCKCHAIN: AN IOT SECURITY SOLUTION.Int.J.Nat.Sci.Vol.1(3). 2024.Pp:28-36. https://doi.org/10.51470/IJNS.2024.01.03.28

I. INTRODUCTION

According to the present trend, the Internet of Things is significantly changing people's lives and will continue to uncover innovative scientific and technological advancements that are integrated into the operation of smart devices and internet-connected apps. One example of revolutionary inventions is robotics. Applications, contactless payment systems, big data analytics, artificial intelligence, and other technologies are constantly consuming the internet, making a tremendous amount of information accessible at any time and from any place.They engage in uninterrupted interaction from one end of the world to the other. Because of this, the world is becoming more and more reliant on the internet to facilitate communication between various technologies, people, and systems. Many sectors are already using IoT-based solutions to create new or much improved technology. For example, doctors may now effectively monitor patients remotely and provide medication based on information gathered from the hospital's IoT environment thanks to the use of IoT solutions. It is safe to argue that nothing in the history of information technology has had a greater impact on humanity than the Internet of Things (IoT), which is widely considered to be the biggest frontier for improving humanity in a variety of ways. Millions of people have been satisfied with the adoption of the IoT, but it is not without its challenges. The Internet of Things has numerous benefits, but it also has disadvantages. Examples include cross-border computer assaults, IP-based network interception, identity theft, and data security and privacy issues. As more smart gadgets interact, it is hard to anticipate how many threats will be found. It is reasonable to presume that some of the many benefits of the IoT evolution also contribute to some of its disadvantages, without being overly critical. As a result, calls to prevent its abuse are stronger than ever.Additionally, blockchain technology is growing rapidly. Due to its decentralised, secure, and transparent nature, information and privacy breaches are difficult and nearly impossible to accomplish. Blockchain-based IoT solutions can be created to address information security and privacy concerns at scale because of its ability to regulate the sharing and access of critical data. Numerous industries are already testing and utilising blockchain, which is gradually emerging as the vital security component that the IoT ecosystem is lacking. Whether it actually offers a reliable answer to the security and privacy problems with the Internet of Things will become evident in due course.

The remainder of the paper is organised as follows: A description and definition of blockchain are provided in Section II. Providing a conceptual overview is Section III.The explanation of the Internet of Things, as well as its uses and related problems. Section IV explores how the blockchain's decentralisation and immutability features, which include the function of peer-to-peer networks, may help to reduce security risk issues with IoT solutions. The paper is concluded in Section V.

II. OVERVIEW AND DEFINITION OF BLOCKCHAIN

The concept of blockchain was first conceived in 2008 when Satoshi Nakamoto, who is believed to be an individual or group of individuals going by the name "Nakamoto," published a paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System," detailing the possibilities of a direct online payment from one party to another without the use of a third-party middleman. The paper discussed a way to combine data structures with different computer concepts and technologies to create an electronic payment system that is secured by cryptographic procedures, even though it did not directly mention blockchain. Nonetheless, efforts are underway to employ a computationally efficient technique for time-stamped digital documents that is impervious to backdating or alteration: a cryptographic-protected chain of blocks.Despite being first presented by Stuart Haber and W. Scott Stornetta in 1991, the pattern that most modern blockchain-based systems have adopted was found in Nakamoto's work. Notably, blockchain is the foundation of the fundamental architecture of Bitcoin, a cryptocurrency, and it is a great example of a field in which blockchain has been adopted since early 2009, when it first began to garner significant public interest. Blockchain has grown into one of the most significant technologies of our time and is now used in a variety of sectors outside of cryptocurrency, such as manufacturing, e-commerce, financial services, shipping, and even health. As of yet, there is no accepted definition of blockchain in any known language. It is widely acknowledged that blockchain-based innovations are showing great potential and transforming the information technology industry worldwide since they provide a secure solution that cannot be altered or controlled by a single entity. [6] defines blockchain as a distributed database system or technology that maintains an increasing collection of records or data that are validated by the nodes in the network. According to, "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 is the reason why the technology is resistant to data changes. According to this definition, blockchain technology is made up of numerous lists of immutable blocks connected by cryptographic techniques. Each block can contain a variety of data or transactions, as well as a time stamp, a unique reference number, and a pointer that can be used to identify the transaction in question as well as a transaction that occurred immediately before it. It is generally accepted that a technology developed with blockchain principles and protocols would be decentralised, unchangeable, irreversible, and impervious to tampering. Though at its core, blockchain technology is a way to securely store and distribute information, its true appeal is in its potential applications for conducting transactions and exchanging information between parties with undeniable transparency and without a central authority.

III. INTERNET OF THINGS: OVERVIEW, DEFINITION, APPLICATIONS, AND CHALLENGES

There are a wide range of physical, intelligent devices all around the world. These devices are equipped with software that, depending on their architectural designs, can provide specific services in order to transcend geographical borders. Additionally, these devices can connect via a variety of communication networks. These achievements were challenging to achieve with traditional computing techniques. These days, billions of devices connect a variety of commonplace items, including traffic light sensors, smart automobiles, and smart homes, among others, beyond time and location constraints by using contemporary computer capabilities. These new services and opportunities have the potential to significantly enhance business, technology, and economic growth, and the number of activities occurring online is growing exponentially. With so many technical platforms, systems, and applications that are connected online, it can be challenging to define exactly what the Internet of Things (IoT) entails.could be really difficult because there are a lot of events involved, and anything can intelligently connect to practically anything. According to [10], the Internet of Things is a network of linked objects, people, and data that are collectively referred to as "things." These Things can process and react to data from the real and virtual worlds by collaborating with intelligent hardware and software services. These tangible and intangible things have intelligent interfaces and are seamlessly integrated into the information system. "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," the statement reads. According to the definitions provided, there are countless possible uses for the Internet of Things, and many people agree that it has provided and will continue to provide a platform for the development of new scientific and technological abilities. Although the Internet of Things (IoT) has been defined and presented differently by various individuals and professional organisations, it is widely accepted that as more objects are connected to the internet, the technology will continue to progress and offer vast potential for the creation of new applications in almost any field that can be thought of. Many IoT-based solutions have been developed to improve quality of life and operational efficiencies across a wide range of industries. Some of these applications have expanded at a never-before-seen pace as a result of the consumerization of science and technology, while others are flourishing and deeply ingrained in all societies. For example, IoT has made it possible to develop new devices that are packed with state-of-the-art technology and enable remote patient monitoring. This helps medical professionals keep their patients safe and healthy. Thanks to several state-of-the-art IoT devices, the hospital's IoT ecosystem now allows patients to interact with their physicians more often. This makes it possible to track, collect, and evaluate relevant data about patient actions. This, in turn, helps to provide vital information that allows medical professionals to attend to patients' needs. quickly and accurately, saving lives before they are typically lost. The Internet of Things is transforming the healthcare sector by enabling the provision of innovative solutions for patients and healthcare providers. For instance, employing surgical robots to do a number of medical procedures or setting up a fitness sensor to track a patient's heartbeat. In the transportation industry, the Internet of Things platform has made it possible for smart traffic lights and cameras to keep an eye on the streets for weather, accidents, and traffic congestion. This scenario demonstrates the true potential of big data since these smart devices and intelligent equipment enable data in an Internet of Things environment to be monitored, gathered, and then sent to the transportation management authority to Use analytics and make informed decisions to improve passenger experiences, safety, and efficiency. The Internet of Things has also helped the financial services and e-commerce industries. The rapid digital transformation and growth of mobile technology in these sectors has led to an increase in the use of personal smart devices to access financial institution and e-commerce products and services. This has helped the industries generate data that can provide in-depth insights into consumer behaviour. For example, by examining a new customer's income and spending, an IoT-enabled banking app can rapidly determine if they are eligible for credit. Furthermore, more advanced authentication features in payment devices like contactless debit or credit cards, POS terminals, and ATMs are being included into IoT-based fraud protection solutions.For instance, Chinese e-commerce behemoths Tencent and Alibaba Group have already introduced facial recognition technology for purchase authentication, a Spanish bank has already adopted the technology, and Apple Inc. and Samsung have integrated fingerprint-compatible apps into their smartphones to do away with the need to enter a pin. It is evident that IoT-based technologies are flourishing, and businesses in the financial services and e-commerce sectors are utilising their benefits and potential to lessen the security risks that are prevalent in these sectors. Right now, the Internet of Things is arguably everywhere, and connected gadgets are being added to almost every part of our lives. As more activities go online, more information sources will become accessible, opening up new possibilities to expand the IoT's range of applications.

There are currently billions of IoT devices, and by 2025, 55.7 billion are anticipated to be connected. Despite a variety of conflicting predictions about the number of connected IoT devices that will soon be available on the market, it is indisputable that there will continue to be a substantial shift towards more internet-enabled products. Although this study hasn't included many instances of practical IoT applications, it's crucial to remember that the IoT has spurred a plethora of new discoveries. If all of the tech-inspired improvements that are currently occurring were ranked by their usability range, IoT would win out.continue to be among the few, if not the only, creations that have served as a basis for the creation of additional inventions.

However, in spite of the Internet of Things' many benefits, there are innumerable problems with its setup and operation. Numerous significant cyberattacks have been tied to the Internet of Things (IoT), often utilising vulnerable connected devices (such cell phones, security cameras, etc.) to support illegal activities. There have been many concerns about how to effectively protect the billions of internet-connected gadgets. 98% of IoT device traffic is not encrypted, according to Threat Report, meaning that the vast majority of sensitive and private data on the network is susceptible to various forms of assaults. The potential forOne could argue that because personal data and information are vulnerable to hackers, consumers and organisations are wary of the security features of IoT-enabled devices and platforms. Despite the efforts of numerous companies to customise the proper security standards for every IoT deployment, the centralised IoT architecture could no longer be entirely suitable for the expanding number of IoT devices and applications. The great majority of IoT-enabled products, to put this into perspective, rely on a centralised network model where all devices are identified, validated, and connected via cloud-based technologies. Thanks to these cloud technologies, devices connected in any way will have vast processing and storage capacities, independent of their distance from one another, allowing them to communicate solely through the internet. This method, which has been used to link general computing devices since the beginning of time and will support the quick growth of small-, medium-, and large-scale IoT networks, is raising concerns that it may not be able to meet the changing needs of IoT ecosystems in the long run, particularly with regard to security. Additionally, centralised network designs have a single point of failure due to their usage of a single gateway, which allows a single hacked device to grant access to the whole network. Central network architectures are also known to have poor interoperability when it comes to data interchange with other central infrastructures. This means that they are unable to sufficiently meet the constantly evolving and increasing demands for end-to-end data interchange between various systems. This is done in order to establish an ecosystem setting that allows for large-scale data interoperability without going against the security requirements of the entire network architecture.

The Mirai attack is just one of many instances showing how frequently serious issues have arisen, raising the possibility that the centralised IoT network paradigm is susceptible to security flaws. The victims were the servers of Dyn, a company that controls a sizable amount of the internet's domain name system infrastructure. The attack was planned using the Mirai botnet software. Consequently, a distributed denial of service (DDOS) attack was initiated, wherein a computer network was configured to overload a server with traffic until it crashed.The strain causes major websites in the US and Europe, such as CNN, Reddit, Netflix, Twitter, the Guardian, and many more, to fail. Additionally, up to 50 million users' personal information was made public in 2018 due to a security breach brought on by technical flaws in Facebook's systems. Furthermore, in A 2018 investigation into the British Airways data breach found that the log-in credentials of a cargo handler employee at Swissport were not adequately secured, which facilitated the hackers' acquisition of primary access to the British Airways network and enabled them to obtain the personal information of approximately half a million customers. These are just a few examples of how a single system compromise exposed the broader network to more dangerous threats. The security of the Internet of Things remains a significant concern, despite the fact that its adoption has undoubtedly had huge benefits.

IV. IOT SECURITY THREATS: IS BLOCKCHAIN A VIABLE SOLUTION?

Blockchain offers a radically new paradigm for handling and storing data on the internet, which could eliminate IoT security problems in a number of ways. The decentralised nature of blockchain technology allows for the prevention of any kind of central attack that could compromise the network as a whole. A decentralised system gets its name from the fact that a community of nodes, as opposed to a single body, maintains the network. In a blockchain system, data is stored on several nodes. Before any data is added or removed from the network, it must be approved and validated by all participating nodes; this approval procedure helps to eliminate the single point of failure. Hostile actors would have to target particular network nodes in order to get around network security. Making use ofA blockchain system or network enables smart devices to actively participate in the validation process. This suggests that by looking for any deviations in preset acceptable behaviours, the network would be able to defend itself against any intrusion or security compromise. The decentralisation feature of blockchain technology allows network changes to be prevented without universal user permission. It is possible to swiftly isolate a network device that is functioning inappropriately or poorly to prevent it from being used to access sensitive data in the future. In contrast to centralised systems, where hackers can target and intercept the data transferred between a server and a device, there isn't a single server or gateway.Decentralised systems hence have a lower chance of a man-in-the-middle attack. The shared participation and openness that all participating nodes in a validation process experience may not always be desirable in every situation or organisation, even though decentralised systems encourage an equally dispersed power during decision-making. When choices require the consent and verification of all participating nodes, it can be difficult to coordinate the actions among the nodes; therefore, a conventional database system might be a good option. The more information that is hidden on a blockchain, the more difficult it is to compute, even though recent technology advancements indicate that there are ways to resolve this problem with blockchains (such as transacting under many blockchain addresses). In addition to the aforementioned, the peer-to-peer framework ofBlockchain technology does away with the need for intermediary services or third-party authorisation. Due to their shared consensus requirement and decentralised peer-to-peer network, blockchains are relatively resistant to security breaches. Peer-to-peer networks make it very difficult to shut down an entire blockchain network because, unlike centralised systems, where one must trust and rely on the integrity of an intermediary, other nodes would remain in place even if one node went down. The peer-to-peer blockchain framework, however, only raises a few small problems. Instead of using a central server (client-server) network strategy like earlier systems, the blockchain network's distributed ledger is maintained by every other user on a client-server network architecture.This requires a significant amount of computational power on each node to ensure a better outcome. Peer-to-peer networks improve security but significantly reduce efficiency, which is one of the main barriers to blockchain deployment in terms of cost, scalability, and general acceptance.Immutability, which promotes openness and ensures that system resources or data cannot be altered or compromised, is another essential feature of blockchain-based systems. This feature can increase the integrity and trust in the data that is kept or exchanged online by adding a quick, inexpensive, and efficient auditing process. In blockchain systems, every transaction that is verified and accepted by network users is timestamped and incorporated into a data "block," which is then cryptographically protected by a hashing operation that links to and incorporates the hash of the previous block, joining the chain as the subsequent chronological update. Every time a new block is hashed, a set of data from the hash output of the previous block is included. Once data has been verified, reviewed, and uploaded to the blockchain, it cannot be altered or removed due to this connection made during the hashing process. The subsequent blocks in the chain would reject any attempts at manipulation since their hashes wouldn't be correct. In other words, the blockchain will crash and the reason will be clear if data is changed. This feature is present in traditional or centralised systems, which form the core of most Internet of Things implementations and make it simple to alter, compromise, or remove data. Unquestionably, blockchain's immutability has significant security benefits, but it also has a disadvantage in that data uploaded into a blockchain network cannot be altered. Having an immutable transaction history may seem like the answer to many of today's business problems, and in some ways, it is. But think about what occurs when records must be removed if they are no longer needed or when private information is inadvertently made public. Additionally, think about what would happen if a resident of the European Union tried to use the General Data Protection Regulation to get privacy treatment.that their data is removed from a system. An immutable system makes it almost impossible to get such information erased because the parameters of the removal would need to be agreed upon by the majority of network users, which is a challenging undertaking. The distributed control and immutability of blockchain technology make it They are a disruptive technology and the source of blockchain's biggest benefits, but they can also have unintended consequences.

Even if blockchain has its own drawbacks, like any freshly created invention, a careful examination of some of its key qualities, as listed above, suggests that it is a technology that might greatly improve the security features of IoT systems. Even while it would seem like a perfect fit to combine blockchain and IoT for increased security, the two technologies are still in their infancy and need thorough research before they can produce a practical outcome. According to current market trends, blockchain technology is being adopted more and more by mainstream businesses, such as governments, supply chains, insurance, and financial institutions.Blockchain technology is one of the most innovative tools of the present day that can improve the security aspect of Internet of Things systems due to its features and momentum.

V. CONCLUSION

By exploiting three relevant characteristics of blockchain technology, this study has illustrated how it may be applied to enhance IoT security. The security events connected to IoT devices make it clear that a plan to lower the risks involved needs to be implemented. It is widely acknowledged that the primary characteristics of blockchain, including immutability, decentralisation, and peer-to-peer architecture, provide security features in a manner that makes cyberattacks difficult to carry out technically. Nonetheless, there are situations where it might be more sensible for a business to choose a traditional or centralised arrangement.IoT environment.

A lot of people believe that blockchain would resolve every issue with IoT security. However, good news is never without its drawbacks. Whether it is the Internet of Things, blockchain technology, or any other creation, it is reasonable to say that technological improvements will always have an impact, either positively or badly. As previously said, it is certain that the Internet of Things will continue to grow and spur numerous new discoveries, but its associated security vulnerabilities have proven to be detrimental. Although employing blockchain as an IoT security solution won't guarantee a flawless result, recent developments have shown that a number of mainstream businesses are more interested in reaping the benefits of this reliable and long-lasting technology. To properly handle whatever disadvantages it may have, the optimum approach and strategy must be chosen. Between 2017 and 2018, there was a 400% rise in demand for blockchain engineers in the US, and major giants like Facebook, IBM, Amazon, and Microsoft were all actively looking for candidates. This signifies a substantial change in the IT sector towards a broader application of the technology. Without a doubt, blockchain provides features that were before unthinkable.

REFERENCES

[1] T. K. Jaimon, L.C. Katrina, G. Enying, and C. Paul, "The internet ofthings: Impact and implications for health care delivery," *Journal ofMedicalInternetResearch,*vol.22,no.11,November2020.

[2] S.Kumar,P.Tiwari,andM.Zymbler,"Internetofthingsisarevolutionaryapproachfor futuretechnologyenhancement:Areview,"*JournalofBigData*,no.111,2019.

[3] L.Stephan,S.Steffen,S.Moritz,andG.Bela,"Areviewonblockchaintechnologyandblockchainprojec tsfosteringopenscience,"*JournalofFrontiers inBlockchain*,vol.2,p. 16,2019.

[4] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technologyoverview,"*NationalInstituteofStandardsandTechnolog*y,2018.

[5] S.Haberand W.S.Stornetta,"Howtotime-stamp adigitaldocument," *JournalofCryptography*,1991,vo.3,pp.99-111.

[6] J. Yli-Huumo, D. Ko, S. Choi, and K. Smolander, "Where is currentresearch on blockchain technology? – A systematic review," PLOSONE,October2016.

[7] L. Popovski, G. Soussou, and P. B. W. Tyler, "A brief history ofblockchain,"*LegaltechNews*,An AMLPublication,May2018.

[8] GSMA.(2018).Distributedledgertechnology,blockchainsandidentity.[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,'Blockchaintechnology,cognitivecomputing,andhealthcareinnovations," *Journal of Advances in Information Technology*, vol. 8,no.3,August2017.

[10] ISO/IECJT1.(2014).Internetofthings(IoT)preliminaryreport.(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 andsmart environment perspective," *Journal of Ambient Intelligence andSmart Environments*, vol. 11, 2019, pp. 45–69, DOI 10.3233/AIS-180506.

[12] IgorInc.(2020).IoTinhealthcare:Enhancingmedicalenvironmentswithinnovativesolutions.[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 SecureFoundation to Leverage IoT for Improved Passenger Experiences*,2020.

[14] N. Joshi. (2018). What are the opportunities for IoT in the

financesector.[Online].Available:https://www.allerin.com/blog/what-are-the-opportunities-for-iot-in-the-finance-sector

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

[16] CaixaBank.(2020).PressRelease:'CaixaBankdeploysATMswithfacialrecognitiontechnologythroughoutSpain.[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 demandsrethinkoflong-termstoragestrategies.[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] Unit42. (2020).IoT threatreport.[Online].Available:https://unit42.paloaltonetworks.com/iot-threat-report-2020/

[19] S. Khvoynitskaya. (2020). Blockchain for IoT security – A perfectmatch. [Online]. Available:https://www.itransition.com/blog/blockchain-iot-security

[20] N.Woolf.(2016).Majorcyber-attackdisruptsinternetserviceacrossEurope and US. [Online]. Available:https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

[21] M.IsaacandS.Frenkel,'Facebooksecuritybreachexposesaccountsof50 millionusers," *TheNewYorkTimes*,September 2018.

[22] D.K.Morrow,'Cyberattackprobe:HowBritishAirwayssecurityflawslet datatheft unfold," *FlightGlobalPremium*,2020.

[23] G. Greenspan and M. Chain, 'Blockchains vs centralized databases," *Four Key Differences Between Blockchains and Regular Databases*,March2016.

[24] T. K. Sharma, 'Blockchain and role of P2P network," *Insights andResources,Blockchain Council*,2020.

[25] G.Iredale.(2020).101Blockchains,'6Keyblockchainfeatures.[Online].Available:https://101blockchains.com/introduction-to-blockchain-features/#prettyPhoto

[26] M. Somers, 'The risks and unintended consequences of blockchain,"MITManagement School,June2019.

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