e-ISSN: 2582-5208

International Research Journal of Modernization in Engineering Technology and Science

( Peer-Reviewed, Open Access, Fully Refereed International Journal )

Volume:06/Issue:06/June-2024 Impact Factor- 7.868 www.irjmets.com

# THE IMPACT OF BLOCKCHAIN TECHNOLOGY ON IMPROVING CYBERSECURITY MEASURES

**Nwakeze Osita Miracle**[*1]

[*1]Department Of Computer Science, Chukwuemeka Odumegwu Ojukwu University, ULI.

DOI : https://www.doi.org/10.56726/IRJMETS59388

## ABSTRACT

Blockchain technology features of decentralization, immutability, transparency, and cryptographic security, makes it promising in addressing cybersecurity issues and bringing about immense improvements in the field. The methodology entails a qualitative analysis of the published literature comprising of academic journals, industry reports, and cases to consider the aspects of blockchain that enhance cybersecurity, the use of blockchain in cybersecurity domains, emerging challenges, and solutions. Redundancy is reduced by avoiding single points of failure, data is less likely to be corrupted or manipulated, and transactions are more transparent when the protection of blockchains strengthens the architecture of digital systems. It is used in areas such as identity and access management, data privacy, financial transactions, Internet of Things (IoT) security, and other relevant areas that have shown great enhancement in the protection of sensitive information and counter tackling of cyber threats. Nonetheless, there are a few challenges that are still emerging when integrating blockchain with cybersecurity: scalability issues, regulatory and legal frameworks, technical challenges of integration, and high energy consumption. Possible solutions include technological advancements such as sharding and new consensus algorithms like Proof of Stake, as well as synergistic strategies for unifying blockchain with artificial intelligence and machine learning. Policy development and the formulation of best practices and principles can contribute to the achievement of safe and responsible blockchain implementation. This paper examines the ramifications of incorporating blockchain in cybersecurity, ways that can derive utility from its attributes, and ongoing approaches of handling its problems suggesting that more work is still needed in this dynamic area.

**Keywords**: Blockchain Technology, Cybersecurity, Decentralization, Regulatory Frameworks, Consensus Mechanisms.

## I. INTRODUCTION

Blockchain technology, which was initially formulated to support the digital currency called Bitcoin by Satoshi Nakamoto in 2008, is a distributed database that registers the exchanges of value in a manner that is unhackable and will not allow alteration across a chain of computers (Nakamoto, 2008). Blockchain being a distribution ledger technology it does not require a central control body and hence, offers a reliable and a secure platform for managing data (Mourtzis et al., 2023). It is worth noting that blockchain technology's application is not limited to cryptocurrencies but ranges through various fields such as supply chain management, finance, healthcare and cybersecurity especially (Wang et al., 2019). Whereas in terms of cybersecurity, because of its decentralised, relatively immutable and transparent book recording technology makes it a guidepost for improving security measures and fighting cybercrime (Habib et al., 2022; Yaga et al., 2018).

Cybersecurity, which is the protection of computer networks and systems from attacks, is a relatively emerging topic in today's technological society (Sule et al., 2021). Organizations have become victims of complex cyber threats, indicating a prevalence of traditional security solutions, The user is now in need of new approaches to security not because of extravagant desire, but due to necessity (Tounsi & Rais, 2018). The current debate in the academia on cybersecurity has highlighted the need to adopt security solutions that can effectively counter advanced persistent threats (APT) and other forms of attack. Nevertheless, vulnerabilities of centralized systems are still felt to a greater extent: if a certain system is attacked, it may hold all the information and experience a critical failure (Kshetri, 2017). This has inspired the investigation into decetralized solutions, with blockchain being among the most promising owing to its security (Zheng et al., 2017).

This is the reason that the present research has importance of offering the vast horizon of the blockchain technology how it can transform the cybersecurity measures. The current literature, though rich in terms of discourses, lacks sufficiently-filled spaces about blockchain's application and its efficiency in realistic cyberspace security situations. This work endeavours to fill this gap by reviewing selected use cases of blockchain in security including Identity management, data security, safer transactions, and IoT security. In addition, it will also discuss the key research questions concerning blockchain implementation in cybersecurity such as the questions of horizontal scalability, legal frameworks and norms, technical feasibility, and energy efficiency (Conti et al., 2018; Casino et al., 2019).

The primary research question guiding this study is: Blockchain technology can complement and improve on the present cybersecurity solutions in what ways, and what are the key obstacles that must be overcome to enable full integration of this technology? Through answering this question, the research will fill the gap that exists in literature by offering academic and practitioner advice on how to incorporate blockchain in the cybersecurity systems. Besides, the proposed solutions will contribute to the advancement of the theoretical perspective on the benefits of blockchain and would be useful for practitioners who work in this sphere (Zheng et al., 2018).

This research is relevant given the rising incidences and complexity of cyber-attacks noting that this warrants the need to have better security solutions. Blockchain technology process which has potentiality for decentralization, immutability, and transparency, can be used for boosting up cyber security. Therefore, this study seeks to contribute to the literature within the given field with the aim of increasing the understanding of how blockchain can be applied to address major cybersecurity issues and help enhance the creation of efficient and safe online structures, (Gupta, 2017; Makhdoom et al., 2019).

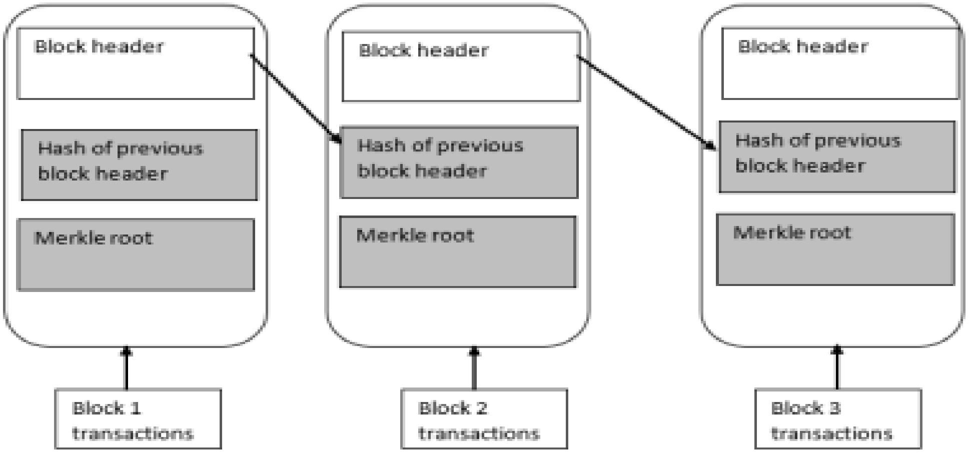

**Figure 1:** A Block Diagram (Mattew, 2019)

## II. OVERVIEW OF BLOCKCHAIN TECHNOLOGY

### 2.1 Defination and Basic Concepts

Blockchain technology is a distributed and decentralized system of recording transactions which are mirrored on many nodes in a network. Blockchain is a distributed system where instead of an organization, a group of computers holds the copies of the database popularly known as nodes. This prevents the populations from being controlled by a middleman or a single entity and increases the security of the system against intrusions (Nakamoto, 2008; Pilkington, 2016). Individual transactions are organized into groups by blocks, which themselves contain a timestamp, the data from the transaction, and the hash of the block that came before it; these are linked to form a chain, hence the name 'blockchain'. This structure makes it virtually impossible to try to fiddle with data that has been recorded as it will shift the subsequent data blocks and require the approval of the supermajority of the network.

Decentralization is inseparable from the use of blockchain technology. Since the records are shared across the network of nodes, blockchain eliminates the dependency on a centralized entity making it more secure than the centralized counterpart systems (Kshetri, 2018). Every node individually acts as the database that check and log transactions, making the system functional without any disruption even if some nodes of it are down (or controlled by the other party) (Zheng et al., 2017). Besides increasing the tolerance to faults, decentralization also enhances the control of the data to the people, thus posing a challenge to a single entity's control over the data.

Another notable feature of blockchain is its immutability. Any transaction once accrued and authenticated by the network, can hardly be changed or erased. This makes each block to have a unique hash number, which also includes the hash number of the previous block; thus, creating a secure chain (Narayanan et al., 2016). Any attempt at this would alter its hash would change the block which in turn will break the chain and inform the network of the change. This feature maintains the integrity and authenticity of the recorded data, making blockchain a dependable solution for applications that require strong security and trust.

Transparency is another impressive feature of the blockchain. It means that any or all blockchain transactions may be observed by all network participants. This increases both accessibility and traceability, allowing participants to monitor transactions and audit them without relying on a third party (Yaga et al., 2019). In the case of public blockchains like Bitcoin, this is done openly to every participant, making trust levels high among the participants. However, access to transaction data can be restricted to authorized users in private or permissioned blockchains, so transparency can be controlled and security is achieved.

The use of cryptographic security is essential since it ensures the integrity of blockchain technology. Payments are made more secure using cryptography such as use of Public-Private Key pairs, digital signatures, and hash functions (Conti et al., 2018). Each participant in the blockchain network has a pair of cryptographic keys: there is a public key that anybody can know, and the private key that is kept away from the public eye. Digital signatures made using the private key can help determine if the transaction is authentic and has not been modified; on the other hand, hashing algorithms ensure the blocks are securely linked. These cryptographic mechanisms provide a way of preventing the block contents from being changed and the block chain from being affixed with unauthorized data.

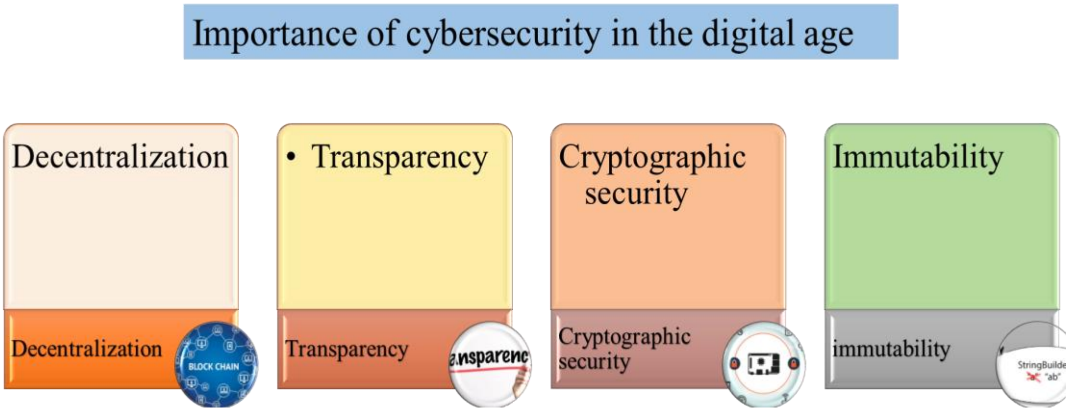

**Figure 2:** Key features of blockchain technology.

Source: Aurthor's computation

## 2.2 Histological Development

This historical evolution only points at the fact that blockchain technology has the ability to revolutionize and grow at a fast pace. Blockchain technology originated and was initially applied through the use of cryptocurrency known as Bitcoin that was created by an unknown person or a group of people referred to as Satoshi Nakamoto in the year 2008. In the whitepaper titled "Bitcoin: Bitcoin: A Peer-to-Peer Electronic Cash System," Nakamoto introduced the blockchain technology for Bitcoin which is an opensource technology to provide a decentralized and a secure way of executing peer to peer payments and transactions without resorting to intermediaries like banks (Nakamoto, 2008). This innovation eliminated the issue of double spending that had haunted the use of digital currencies and paved way for a new era of innovative online payment.

Although Bitcoin's blockchain was innovative, its primary use was initially for peer-to-peer electronic cash. Nevertheless, with the help of Bitcoin, the world received a glimpse into the potential of blockchain technology and became interested in this area. The next major breakthrough in the field was reached with the help of Vitalik Buterin, who developed Ethereum in 2015. Ethereum built on the basic blockchain application of secure financial transactions by extending the application to the use of smart contracts – self-executing contracts whose terms are embedded in the computer code (Buterin, 2014). This innovation enabled the usage of blockchain for intricate contractual terms, expanding its application range.

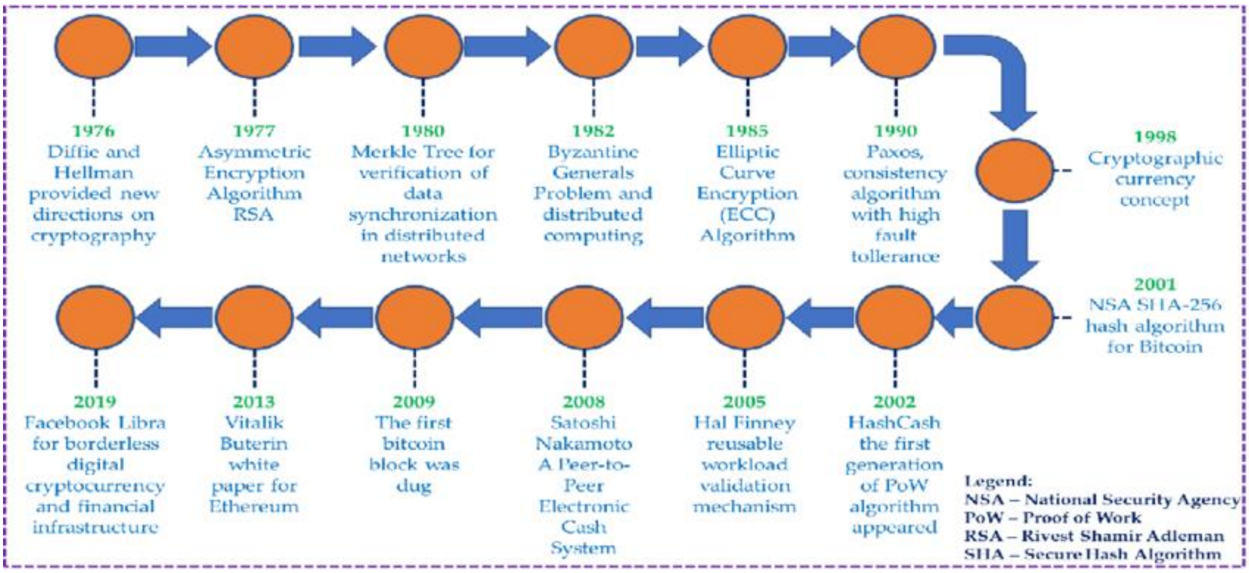
1976
Diffie and Hellman provided new directions on cryptography
1977
Asymmetric Encryption Algorithm RSA
1980
Merkle Tree for verification of data synchronization in distributed networks
1982
Byzantine Generals Problem and distributed computing
1985
Elliptic Curve Encryption (ECC) Algorithm
1990
Paxos, consistency algorithm with high fault tollerance
1998
Cryptographic currency concept
2001
NSA SHA-256 hash algorithm for Bitcoin
2002
HashCash the first generation of PoW algorithm appeared
2005
Hal Finney reusable workload validation mechanism
2008
Satoshi Nakamoto A Peer-to-Peer Electronic Cash System
2009
The first bitcoin block was dug
2013
Vitalik Buterin white paper for Ethereum
2019
Facebook Libra for borderless digital cryptocurrency and financial infrastructure
Legend:
NSA – National Security Agency
PoW – Proof of Work
RSA – Rivest Shamir Adleman
SHA – Secure Hash Algorithm

**Figure 3:** Historical milestones in blockchain evolution (Mourtzis et al., 2023)

Smart contracts transformed the use of blockchain by expanding its usage to different sectors in various industries. For example, in supply chain it has been used to improve the transparency and increase the ability of all stakeholders to monitor the flow of goods and their origin in real time (Kshetri, 2018). In the heath sector, blockchain technology has been used to protect patients' records which makes the data private and enhance the compatibility of health systems (Azaria et al. , 2016). Moreover, the financial field focuses on the growth of the blockchain technology for enhancing the effectiveness and safety of the financial transactions, including the cross-border payments, and securities trades (Peters & Panayi, 2016).

With the advancement in blockchain technology, multiple consensus algorithms emerged to solve the inadequacies of Bitcoin's point-of-work (PoW) that is expensive and slow. Other consensus algorithms such as the proof-of-stake (PoS), delegated proof-of-stake (DPoS), and Byzantine fault tolerance (BFT) were developed to improve the functionality and the capability of blockchain networks (Saleh, 2020). These have also helped in the expansion of blockchain solutions in new and complicated settings, which goes to show the flexibility of the technology.

This led to the emergence of permissioned and private blockchains that are tailored for enterprise requirements, which demand more control over data and transactions. In contrast to public blockchain systems that are accessible to multiple users, permissioned blockchains provide access to only selected users, thereby achieving the right balance between decentralization and controlled participation (Zheng et al., 2017). This has made the adaptation of blockchain technology easier mainly in the banking sector due to the regulatory compliance and data privacy.

### 2.3 Types of Blockchain

Blockchain technology can be broadly categorized into two main types: there are two types of blockchains, which are the public and the private blockchains and both have different use and properties.

Bitcoin and Ethereum are good examples of public blockchains, which allow anyone to join the network and contribute. These are distributed ledgers that are created without a central authority and rely on consensus to approve the state of the ledger. In regard to public blockchains, the openness and decentralization increase the levels of confidence as all the operations are public in the network. However, this openness leads to the problems of scalability and high energy consumption as in Bitcoin's Proof of Work (PoW) protocol (Nakamoto, 2008). Private blockchains are those which are accessible only to a certain number of individuals and are usually employed in organizations that require more control over their records. A private Blockchain network is also permissioned, this implies that only the individuals who are allowed to can be part of the network and contribute in the consensus. This makes private blockchains ideal for organizations, where transaction speed is important, and the information is sensitive due to regulatory requirements (Zheng et al., 2017). Some examples of such platforms are Hyperledger Fabric and R3 Corda that are created to cover the requirements of particular industries, including finance and supply chains.

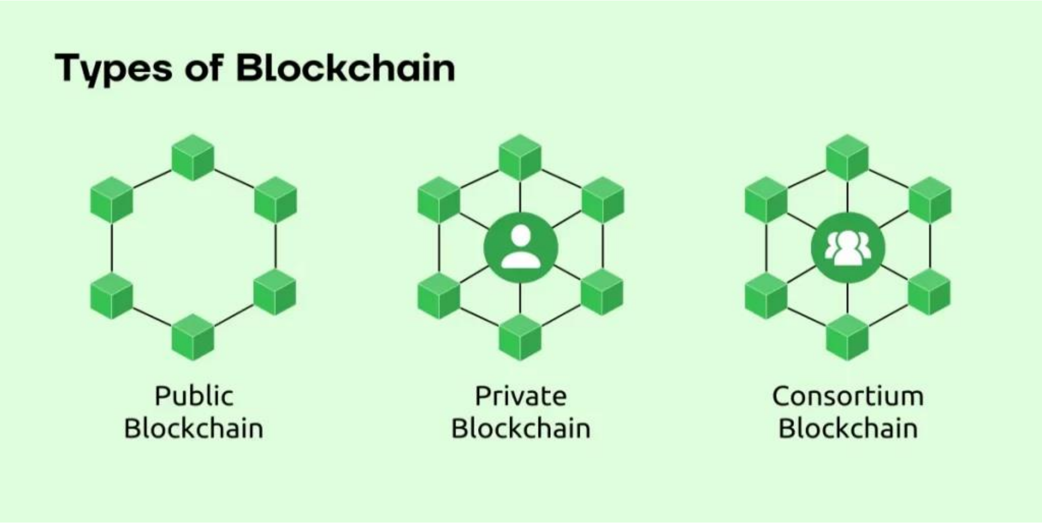

**Figure 4:** Types of Blockchain

**Consensus mechanisms** (Figure 5)

Consensus algorithms are an essential part of both the public and the private blockchains because they help all the members of the network to have a common understanding of the transactions being made and the state of the ledger. The best-known consensus algorithm is Proof of Work (PoW), which was used at the beginning of Bitcoin. In the PoW, miners have to solve difficult mathematical problems and the first one to do so is allowed to append a new block to the blockchain and gets paid. Even though PoW guarantees good security, it has disadvantages of high energy consumption and slow rate of processing transactions (Narayanan et al., 2016).

Proof of Stake (PoS) is another consensus mechanism that was created to solve the issues with PoW. In PoS, validators are selected to generate new blocks and approve the transactions in proportion to the number of coins owned and are willing to risk to “stake” for the process. This has the effect of greatly minimizing the energy utilized and the rate of transactions may be enhanced. PoS is applied in the Ethereum 2. 0 and Cardano blockchains among others (Buterin, 2014). Other types include Delegated PoS, a sub-type of PoS where a few chosen validators are in charge of the blockchain, making it more efficient and scalable (Larimer, 2014).

There are other types of consensuses called Byzantine Fault Tolerance (BFT) which are mostly applied in private blockchain. BFT algorithms, for example, the Practical Byzantine Fault Tolerance (PBFT), enable a network of distributed nodes to agree on a particular decision even when some nodes are faulty or even malicious. PBFT works well with a small number of participants, which is why it is used in private and consortium blockchains (Castro & Liskov, 1999). This mechanism increases the reliability and security of the network while at the same time increasing the network performance.

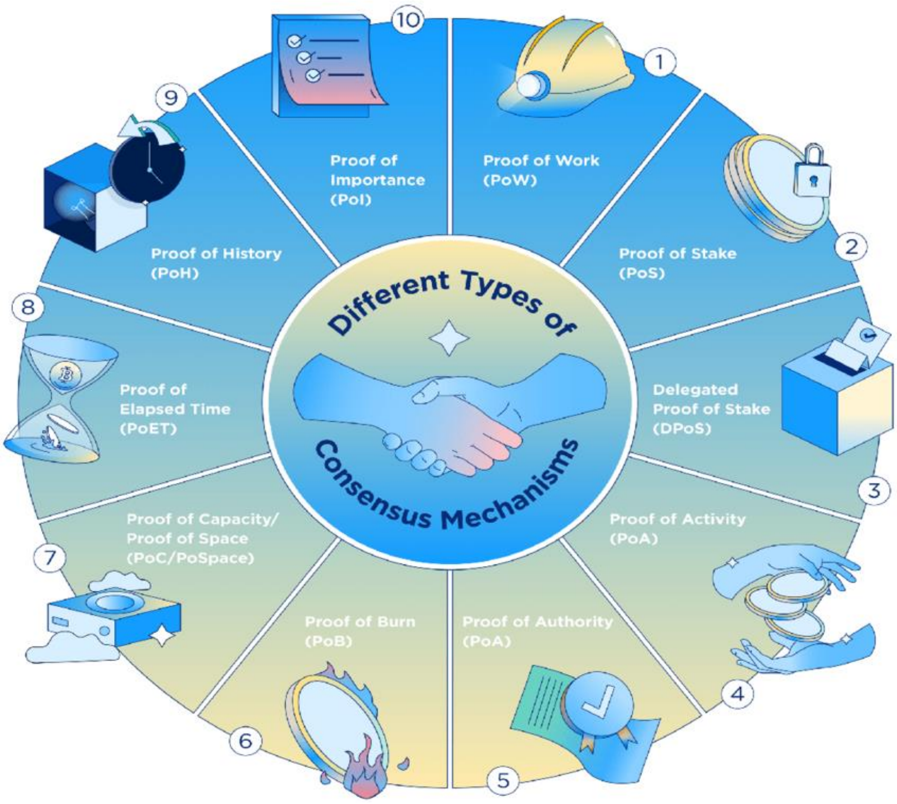
Different Types of Consensus Mechanisms
1
Proof of Work (PoW)
2
Proof of Stake (PoS)
Delegated Proof of Stake (DPoS)
3
Proof of Activity (PoA)
4
Proof of Authority (PoA)
5
Proof of Burn (PoB)
6
Proof of Capacity/ Proof of Space (PoC/PoSpace)
7
Proof of Elapsed Time (PoET)
8
Proof of History (PoH)
9
Proof of Importance (PoI)
10

**Figure 4:** Consensus Mechanisms in Blockchain Technology

Source: https://crypto.com/university/con-sensus-mechanisms-in-blockchain

## III. METHODOLOGY

The research method in this study involves the comprehensive analysis of the existing literature, cases and reports on the use of blockchain and the effects on cybersecurity. Primary sources were peer reviewed journals, conference papers and reports from cybersecurity firms and blockchain consortiums. This includes papers by professionals, white papers, and other papers that are associated with the regulations. Data was collected from peer reviewed journals that were retrieved from the IEEE Xplore, Google scholar and PubMed databases in order to capture both the recent and most related studies.

This study adopts a qualitative method to obtain results which in turn were synthesized so as to arrive at a general conclusion on the current and future prospects of blockchain in enhancing cybersecurity.

## IV. BLOCKCHAIN FEATURES ENHANCING CYBERSECURITY

### A. Decentralization

Decentralization is one of the constituent elements of the block-chain technology that brings tremendous improvement to the aspects of security. Since transactions are recorded on the distributed ledger, blockchain does not require a central authority, thus minimizing possibilities of the occurrence of single points of failure. Conventional centralized structures can be vulnerable to attacks where the hacker gains full control of a particular server or database for example, the Equifax data breach in 2017 that saw the personal data of about 147 million people exposed (Equifax, 2018). However, a decentralized blockchain network has the copies of the ledger for all the nodes in the network making it extremely hard to attack. For instance, the Bitcoin network currently has over 10,000 nodes in 2021 and has been hacked severally but remains safe (Bitnodes, 2020).

Decentralized security models show that this approach is actually very sound. For instance, Inter Planetary File System (IPFS) is a peer-to-peer communication that utilizes chain of blocks in its working. As a result of data distributed in a global network of nodes, even when some of them become malicious or unresponsive, the data is safe and accessible. This model increases the accessibility and reliability of data and that makes it a useful tool for secure data sharing (Benet, 2014).

### B. Immutability

Another important characteristic of blockchain technology is immutability, which safeguards the data from alteration and duplication. If a transaction occurs within a blockchain it cannot be reversed or deleted which offers a wealth of benefits for a permanent record. This is done through cryptographic hashing in that every block created has a unique hash that is linked to the previous block to form a chain. Deloitte's study revealed that 32% of the organizations view immutability as one of the most significant strengths of blockchain technology when it comes to record integrity (Deloitte, 2019).

Some examples include the roles of blockchain in fighting data tampering as illustrated by case studies. For instance, in the pharma sector, IBM has provided an instance where the firm applied its blockchain offering, IBM Food Trust, to track the origin of drugs and therefore guard against the distribution of fake drugs. The block chain maintains every activity in the supply chain starting from production up to delivery, thus, offering unchallengeable evidence of the genuineness of the drug in question (IBM, 2018). Likewise, Estonian authorities have integrated the use of blockchain technology to safeguard electronic health records and guarantee that the information is accurate and unmodified (e-Estonia, 2020).

### C. Transparency and Traceability

Transparency and traceability are two strengths that could be observed in the blockchain solution, which helps improve cybersecurity by providing higher visibility in a transaction's history. This form of record-keeping is transparent with all the participants in the blockchain network able to see and authenticate the transactions. PwC report also shows that 84% of executives are of the view that blockchain can enhance the aspect of transparency in business processes (PwC, 2020). Some examples of the application of the approach are given in examples of fraud detection and accountability. For instance, in the financial markets, block chain is applied to develop tamper-proof record of transactions to minimize fraudulent activities and improve compliance with the laws. Supply chain management through blockchain means enables tracing of goods and products in real-time, hence minimizing fraud and guaranteeing that products are procured and dealt with in the right manner. Currently, Walmart applies the blockchain technology for tracking food products; this has enhanced the traceability of products as it takes only a few seconds to track the origin of a product as compared to several days (Walmart, 2018).

### D. Cryptographic Security

Cryptographic security is the foundation of the blockchain transaction since it determines the level of reliability. Cryptographic methods used in blockchain include public and private keys, digital signatures and cryptographic hashing. Every participant has two cryptographic keys; the private key, used for signing of transactions is unique to the participant thereby securing the transaction while the public key is used in confirming the signature. This mechanism ensures that only the right persons are authorized to perform transactions hence protecting the data.

When compared with the tradition method of encryption, it is clear that the cryptographic level of blockchain is very strong. Classic encryption methods like the symmetric and asymmetric encryption are based on data key exchange and control that can be difficult to manage at large. Blockchain also incorporates decentralized and distributed cryptographic methods that make security more reliable as it lacks a centralized key management system. For instance, the cryptographic technique used in mining new Bitcoin blocks by solving complex mathematical problems is SHA-256, which is believed to have a 1 in 2^256 chance of a successful attack (Narayanan et al., 2016).

## V. APPLICATIONS OF BLOCKCHAIN IN CYBERSECURITY

### A. Identity Management

Blockchain technology has created new opportunities for the identity management by offering effective and secure models for identity verification. The traditional forms of identity management are always at risk as they use databases that can be hacked by the attackers. While blockchain-based systems for identity management are more centralized, they offer better security and privacy due to decentralized and immutable ledgers. These systems use cryptographic methods to ensure that identity information is stored in a secure way and can only be accessed by those who have been permitted to do so (Zyskind et al., 2015). It is noted that blockchain identity management market size is accounted for USD 17.46 billion and is projected to reach USD 1,441.54 billion at the compound rate of 87.7% by 2030, which signifies the integration of this technology (Langaliya & Gohil, 2023).

Some of the secure methods in identity verification include self-sovereign identity (SSI) where users have complete control over their identities through blockchain. This helps to remove the middlemen, thus lowering the chance of losing financial or sensitive information. For example, there is Sovrin – the SSI based on the blockchain that enables users to control their digital identities safely. Through allowing people to share just the relevant data with the service providers, Sovrin increases the privacy and security (Protocol, 2020).

### B. Data Protection

Blockchain ensures data security by providing an immutable record for sensitive information, data cannot be changed and is secure. The data created within the blockchain is safeguarded to ensure it cannot be altered or read by anyone without proper authorization. This characteristic ensures no one can change the information that is placed in the blocks of blockchain hence making it suitable for protecting important information (Narayanan et al., 2016). A blockchain technology market report estimates the global market for this technology may be worth USD 394.60 billion by 2028, for example, because of increased need for data protection solutions (Grand View Research, 2021).

Some examples of how blockchain is applied to protecting data are in the health sector and the financial sector. Blockchain is applied in the healthcare environment for securing electronic health records (HERs) so that the data contained in them would not be altered or accessed by unauthorized individuals. For instance, the MIT Media Lab's MedRec project employs the blockchain technology in handling and protecting EHRs while ensuring an open and unalterable database of the patients' information (Azaria et al., 2016). In the financial world, blockchain is used to safeguard the ledger data and prevent such possibilities as fraud. For example, Nasdaq adopted blockchain in the issuance of private securities where it improves the security of the records by increasing the protection against fraud (Benedetti et al., 2021).

### C. Secure Transactions

Smart contracts enable also safe financial operations and the implementation of various operations through the blockchain technology, thus minimising the possibilities of fraud. Smart contracts are digital contracts where the contract terms are coded into the smart contracts program. These contracts enable transactions to be made when specified conditions are met without the intervention of third parties and without one's input, hence the reduced chances of making a mistake (Buterin, 2014). In a study carried out by Juniper Research (2018), it showed that blockchain technology is critically important in secure transactions and it was estimated to process a transaction value of USD 1.3 trillion by the year 2023.

Some examples of reforming the financial system through blockchain include the usage of Ripple – an electronic payment network based on the blockchain technology. Ripple is an efficient solution that allows real-time cross-border transactions, and it also has significant security and lower costs. Currently, many organizations such as Santander and American Express work with Ripple to enhance streamlining of the payment system. An example of ASX is already in the process of transitioning its current clearing and settlement system into a new blockchain system to improve its security and effectiveness (Thuvarakan, 2020).

### D. IoT Security

Internet of Things (IoT) is a network of smart gadgets, connecting them through the internet leads to a lot of security issues. Blockchain makes it easier to address these issues because it is mainly a decentralized platform for managing IoT devices. Consequently, self-identity and self-authentication of the IoT devices can be implemented by the help of blockchain preventing other malicious devices to connect and gain access to the data (Christidis & Devetsikiotis, 2016). Research conducted by IDC in 2020 revealed that the global spending on blockchain solutions for IoT security is projected to reach USD 3 billion by 2024 highlighting on the solution's significance within IoT.

Blockchain has been supporting IoT security in various ways, for instance, the IBM's Watson IoT platform utilizes blockchain in the security of IoT information. It offers an immutable blockchain platform upon which the history of the IoT data is captured thus making it nearly impossible to temper with. Currently, IBM has implemented its thoughts in supply chain and automotive industries for boosted IoT devices security (Reddy, 2021). Another example is the IOTA project which employs the block chain like structure known as the Tangle in order to provide security to IoT networks. IOTA's Tangle is more efficient when it comes to the use of IoT devices because it utilizes less computational power as compared to other blockchains, Popov (2018).

## VI. EMERGING ISSUES AND CHALLENGES

### A. Scalability

Scalability has become one of the biggest problems that the blockchain world has ever faced. As the number of transactions rises, the actual capacity of blockchain network deteriorates or the ability of the network to handle the number of transactions grows weak. For instance, Bitcoin can process roughly 7 transactions per second while; Ethereum can process about 15 transactions per second (Rankhambe et al., 2019). In contrast, conventional payment systems, for example, Visa, can manage up to 24 000 operations per second, which showcases the scalability issue (Rankhambe et al., 2019).

Solutions and current research efforts are aimed at tackling these challenges of scalability. The Layer 2 solutions, including the Lightning Network for Bitcoin and Plasma for Ethereum's blockchain, seeks scalability through a nested model of executing transactions and settling blocks of them off the main chain. These solutions can scale the transaction throughput and effectively relieve the congestion at the same time to a great extent. Another prospective approach is sharding – the division of the large blockchain into several smaller ones, called shards. Ethereum 2. 0 has no plan towards adoption of sharding to enhance scalability of its firm (Kim, 2020).

### B. Regulatory and Legal Issues

Depending on the jurisdiction, blockchain can be legal or face numerous regulatory issues due to its maturity. National and international authorities are still struggling to determine the proper legal status of cryptocurrencies and applications based on blockchain. For instance, in the United States the SEC has deemed some tokens to be securities which puts them under the highest set of standards while on the other end, countries like Malta have highly embraced blockchain technology setting very favorable regulations (Karisma et al., 2023).

Data privacy concerns and compliance issues further cannot be overemphasized. Among such variations are those posed by the General Data Protection Regulation (GDPR) in the European Union especially in reconciliation to right to be forgotten in blockchain implementations. It has been agreed earlier that due to blockchain's decentralised nature, it becomes hard to alter or delete information and therefore it hard to meet GDPR regulation. Such issues are in the works with solutions like Zero-knowledge proofs and off-chain data for solving these issues while trying to retain all the strength of block chain (Benet, 2014).

### C. Technical Complexity

When incorporating blockchain with conventional systems, it has impracticable technical challenges. Most legacy systems are not compliant with the architecture of decentralized networks and hence require major enhancements or, in some cases, replacement. This integration challenge can be significant forms of adoption hurdles, especially for industries dependent on dated infrastructure (Mssassi & El Kalam, 2023).

Thus, the necessary technical competence and resource demands are significant. Blockchain development is quite complex since it entails knowledge and skills in cryptography, distributed systems, and consensus protocols. Additionally, an article published by Hired shows that the need for blockchain developers rose by 517% from the previous year, indicating the shortage of qualified personnel in this domain (Hired, 2018). Professionals must be trained and sought to ensure the stability of the blockchain solutions within organisations and support can be costly.

### D. Energy Consumption

Blockchain systems have high energy requirements, especially for those that utilize PoW consensus protocols. For instance, the energy consumption used for mining bitcoins did exceed the energy consumption of some countries in a year. As of 2021, according to Jamali et al. (2024), the Bitcoin's network energy consumption reached approximately 121.36 tetra-Watt annually, something like Argentina's energy consumption.

The implication of such excessive energy usage to the environment is that it pollutes the environment by emitting carbon and degrading the environment. Hence, it is crucial to make the use of blockchain applications sustainable as the demand for the technology continues to increase. Other models are even more efficient, for instance, the Proof of Stake (PoS) and other combined approaches. Ethereum, for instance, which transitioned from PoW to PoS with Ethereum 2.0, has set its goal to bring down its energy consumption by a staggering of approximately 99.95% (Asif & Hassan, 2023). Furthermore, constant advances in renewable energy sources for mining operations and also efficient consensus algorithms that may not consume a lot of energy are still crucial in dealing with environmental effects of the technology (Krause & Tolaymat, 2018).

## VII. FUTURE DIRECTIONS AND RESEARCH

### A. Innovations in Blockchain Technology

The constant advancements in technologies as well as constant advancements in the blockchain are at the moment calling the shot in this sector; with relative discloser indicating to more enhanced, secure and scalable conformation of the blockchain. Sharding, sidechains, as well as Layer 2 solutions, have been incorporated to contain the scalability issues that affect blockchain systems. By splitting a blockchain into smaller parts, sharding can increase speeds or throughput of transactions. For instance, sharding in Ethereum 2.0 would increase its TPS from 15 to an estimated 100,000 TPS (Rankhambe et al., 2019).

Also, improvements in the consensus algorithms are vital. Ethereum in particular, has transitioned to using Proof of Stake (PoS) that, in relation to energy consumption, is 99.95% less energy consumptive than Proof of Work (PoW) (Asif & Hassan, 2023). Additionally, combining aspects of both Proof of Work and Proof of Stake makes them a reasonable compromise in between. Quantum-resistant solutions are also being considered by blockchain networks to mitigate the risk that comes with quantum computing as it poses a threat to present and future cryptographic mechanisms (Zheng et al., 2017).

### B. Interdisciplinary Approaches

Integrating blockchain with other developing technologies such as AI and machine learning (ML) will definitely create new possibilities for invention and usage. Blockchain will be improved by AI by performing better, smart contracts, better usage of energy in blockchains as well as modern analytical engines for blockchain data. For instance, AI algorithms can forecast and control the flow of the blockchain network, hence eliminating latency issues (Dinh et al., 2018).

Machine learning and blockchain can work together in improving security by utilizing anomaly detection and analysis. With help of ML algorithms, it is possible to find patterns of a transaction, which can be a security threat in real-time, and thus, to add a layer of protection against cyber threats. The AI in blockchain market is expected to rise from USD 184 million in 2019 to USD 704 million in 2024, presenting the enhancement of the relations between AI and blockchain (Xu and Yin, 2019).

Another exciting interdisciplinary perspective is the interconnectivity of IoT with blockchain. Thus, with the use of blockchain, secure ways to manage IoT devices and its data can be established since it provides decentralized solutions to the problem. For instance, IBM IoT Watson tracks data using blockchain technology to ensure the data is of high confidence, secure, trusted, and transparent (Santos & Moura, 2019).

### C. Policy and Regulation

In the current world, there is need to develop complicated legal systems to provide for the security as well as the ethical usage of block chain. Various governmental authorities and global legislation offices are in the process of defining how this technology can be used effectively and where – especially in finance, healthcare and SCM. For instance, the European Union's 5th Anti-Money Laundering Directive (5AMLD) contain provisions related to control of cryptocurrencies and blockchain infrastructure of financial services, to increase the overall transparency and reduce the risk of illegitimate operations (Gibbs, 2023).

It also covers issues related to data protection and the GDPR as well as the use of the technology and its integration into the 'Internet of Things' and other applications. Such operational concepts like zero-knowledge proofs and off-chain storage are used to address issues of both blockchain's structural inviolability and data protection regulations. These technologies can be adopted to assist organizations in following the data privacy laws while using the blockchain benefits.

In addition, cross-border collaboration and non-technical specification are fundamental to ensuring that more civilizations integrate blockchain technologies. Even big organizations like the International Organization for Standardization (ISO) are coming up with global standards for blockchain that address issues like security, privacy, and compatibility (ISO, 2020). These standards can enhance the interoperability and possibility of the global collaboration along with innovation within the blockchain sector while creating a united and safe environment within the Industry.

## VIII. CONCLUSION

In the further perspectives, the applicability of the blockchain in future threats and risks of cybersecurity is enormous. With the further development of the technology in areas like sharding, improved consensus mechanisms, and interactions with AI and IoT, it can only be stated that blockchain is well equipped for the future, for instance, securing digital assets and sensitive data, and enabling safe and secure transactions.

Blockchain has implications not only for the conventional cybersecurity but also for the new and innovative domains like Decentralized Identity, IoT-Security, and Smart Contract Compliance. The continuous development of regulatory measures and adoption of international standards will help extend block-chain's recognition and application in conventional cybersecurity systems.

To leverage blockchain technology for cybersecurity, much more research and engagement and more innovation is needed. Promoting the use of blended methodologies with an integration of AI, ML, IoT, and blockchain aims at creating new ideas for solving emerging cybersecurity threats. In addition, developing combined efforts between academics, industry, and authorities in charge will contribute to informative synergies concerning proper implementation of blockchain technologies.

The cybersecurity experts, government and regulatory bodies, and technology experts therefore need to keep abreast with the developments in block chain technologies, act as knowledge brokers, and be advocates for proper use of blockchain with high standards of security. Thus, only through collaboration, it is possible to create a strong and reliable digital environment that will use the potential of blockchain for a better future.

## IX. REFERENCES

[1] Asif, R., & Hassan, S. R. (2023). Shaping the future of Ethereum: Exploring energy consumption in Proof-of-Work and Proof-of-Stake consensus. Frontiers in Blockchain, 6, 1151724.

[2] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016, August). Medrec: Using blockchain for medical data access and permission management. In 2016 2nd international conference on open and big data (OBD) (pp. 25-30). IEEE.

[3] Benedetti, H., Nikbakht, E., Sarkar, S., & Spieler, A. C. (2021). Blockchain and corporate fraud. Journal of Financial Crime, 28(3), 702-721.

[4] Benet, J. (2014). Ipfs-content addressed, versioned, p2p file system. arXiv preprint arXiv:1407.3561.

[5] Bitnodes, S. (2020). Global bitcoin nodes distribution. URL: https://bitnodes. earn. com/# global-bitcoin-nodes-distribution, 1, 19.

[6] Buterin, V. (2014). A next-generation smart contract and decentralized application platform. white paper, 3(37), 2-1.

[7] Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and informatics, 36, 55-81.

[8] Castro, M., & Liskov, B. (1999, February). Practical byzantine fault tolerance. In OsDI (Vol. 99, No. 1999, pp. 173-186).

[9] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. IEEE access, 4, 2292-2303.

[10] Consensus Mechanisms in Blockchain: A Beginner's Guide. Crypto.com. Available online: https://crypto.com/university/con-sensus-mechanisms-in-blockchainn (accessed on 20 November 2022).

[11] Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of bitcoin. IEEE communications surveys & tutorials, 20(4), 3416-3452.

[12] Deloitte. (2019). Deloitte's 2019 Global Blockchain Survey. Retrieved from https://www2.deloitte.com

[13] Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. IEEE transactions on knowledge and data engineering, 30(7), 1366-1385.

[14] e-Estonia (2020). Blockchain Technology - frequently asked questions. https://e-estonia.com/ wp-content/uploads/2020mar-nochanges-faq-a4-v03-blockchain-1-1.pdf

[15] Equifax Inc. (2018). "Equifax Announces Cybersecurity Incident Involving Consumer Information," 7 September 2017. [Online]. Available: https://www.equifaxsecurity2017.com/2017/09/07/equifax-announces-cybersecurity-incident-involving-consumer-information/. [Accessed 2 June 2024].

[16] Gibbs, T. (2023). Evolution of Legal and Regulatory Responses to Money Laundering Risks Related to Virtual Assets: The Examples of the European Union and the US. In CYBER LAUNDERING: International Policies and Practices (pp. 197-233).

[17] Grand View Research. (2021). Blockchain Technology Market Size, Share & Trends Analysis Report by Type. Retrieved from https://www.grandviewresearch.com/ [Assessed 3 June, 2024]

[18] Gupta, M. (2017). Blockchain for Dummies. John Wiley & Sons.

[19] Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing. Future Internet, 14(11), 341.

[20] Hired. (2018). State of Salaries: 2018. Retrieved from https://hired.com/state-of-salaries-2018

[21] IBM. (2018). IBM Food Trust. Retrieved from https://www.ibm.com/blockchain/solutions/food-trust

[22] IDC. (2020). Worldwide Spending on Blockchain Solutions Forecast to Reach $4.3 Billion in 2020. Retrieved from https://www.idc.com/getdoc.jsp?containerId=prUS46294020

[23] Jamali, A., Ali, N. I., Brohi, I. A., Kanasro, N. A., Murad, M. U., & Jamali, A. A. (2024, January). Exploring Relationships among Bitcoin's Market Price, Energy Consumption and Carbon Dioxide Emissions: A Machine Learning Approach. In 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC) (pp. 1-6). IEEE.

[24] Juniper Research. (2018). Blockchain: Key Vertical Opportunities, Trends & Challenges 2018-2030. Retrieved from https://www.juniperresearch.com/ [Assessed 3 June, 2024].

[25] Karisma, K., & Moslemzadeh Tehrani, P. (2023). Blockchain: Legal and Regulatory Issues. In Sustainable Oil and Gas Using Blockchain (pp. 75-118). Cham: Springer International Publishing.

[26] Kim, C. (2020). Ethereum 2.0: How it works and why it matters. Coindesk: https://www. coindesk. com/wp-content/uploads/2020/07/ETH-2.0-072120. pdf.

[27] Kincaid, A. (2018). Discussion of the Potential of Blockchain in Finance.

[28] Krause, M. J., & Tolaymat, T. (2018). Quantification of energy and carbon costs for mining cryptocurrencies. Nature Sustainability, 1(11), 711-718.

[29] Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. International Journal of information management, 39, 80-89.

[30] Langaliya, V., & Gohil, J. A. (2023). Innovative and secure decentralized approach to process real estate transactions by utilizing private blockchain. Discover Internet of Things, 3(1), 14.

[31] Larimer, D. (2014). Delegated proof-of-stake (dpos). Bitshare whitepaper, 81, 85.

[32] Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. (2019). Blockchain's adoption in IoT: The challenges, and a way forward. Journal of Network and Computer Applications, 125, 251-279.

[33] Mathew, A. R. (2019). Cyber security through blockchain technology. Int. J. Eng. Adv. Technol, 9(1), 3821-3824.

[34] Mourtzis, D., Angelopoulos, J., & Panopoulos, N. (2023). Blockchain integration in the era of industrial metaverse. Applied Sciences, 13(3), 1353.

[35] Mssassi, S., & El Kalam, A. A. (2023, October). Leveraging Blockchain for Enhanced Traceability and Transparency in Sustainable Development. In International Conference on Advanced Intelligent Systems for Sustainable Development (pp. 162-177). Cham: Springer Nature Switzerland.

[36] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. Decentralized Bus. Rev. 2008, 21260

[37] Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press.

[38] Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money (pp. 239-278). Springer International Publishing.

[39] Pilkington, M. (2016). Blockchain technology: principles and applications. In Research handbook on digital transformations (pp. 225-253). Edward Elgar Publishing.

[40] Popov, S. (2018). The Tangle. Retrieved from https://iota.org/research/academic-papers

[41] Protocol, A. (2020). Token for Self-Sovereign Identity and Decentralized Trust. Technical Report.

[42] PwC. (2020). PwC's Global Blockchain Survey 2020. Retrieved from https://www.pwc.com

[43] Rankhambe, B. P., & Khanuja, H. K. (2019, September). A comparative analysis of blockchain platforms–Bitcoin and Ethereum. In 2019 5th international conference on computing, communication, control and automation (ICCUBEA) (pp. 1-7). IEEE.

[44] Reddy, K. R. K., Gunasekaran, A., Kalpana, P., Sreedharan, V. R., & Kumar, S. A. (2021). Developing a blockchain framework for the automotive supply chain: A systematic review. Computers & Industrial Engineering, 157, 107334.

[45] Saleh, F. (2021). Blockchain without waste: Proof-of-stake. The Review of financial studies, 34(3), 1156-1190.

[46] Santos, M., & Moura, E. (2019). Hands-On IoT Solutions with Blockchain: Discover how converging IoT and blockchain can help you build effective solutions. Packt Publishing Ltd.

[47] Sule, M. J., Zennaro, M., & Thomas, G. (2021). Cybersecurity through the lens of digital identity and data protection: issues and trends. Technology in Society, 67, 101734.

[48] Thuvarakan, M. (2020). Regulatory changes for redesigned securities markets with distributed ledger technology. The Knowledge Engineering Review, 35, e14.

[49] Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & security, 72, 212-233.

[50] Walmart. (2018). Walmart's Blockchain Solution Aims to Improve Food Safety. Retrieved from https://www.walmart.com

[51] Wang, Y., Han, J. H., & Beynon-Davies, P. (2019). Understanding blockchain technology for future supply chains: a systematic literature review and research agenda. Supply Chain Management: An International Journal, 24(1), 62-84.

[52] Xu, Minghui, Yihao Guo, Chunchi Liu, Qin Hu, Dongxiao Yu, Zehui Xiong, Dusit Niyato, and Xiuzhen Cheng. "Exploring blockchain technology through a modular lens: A survey." ACM Computing Surveys 56, no. 9 (2024): 1-39.

[53] Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. arXiv preprint arXiv:1906.11078.

[54] Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International journal of web and grid services, 14(4), 352-375.

[55] Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H., 2017, June. An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (BigData congress) (pp. 557-564). Ieee.

[56] Zyskind, G., & Nathan, O. (2015, May). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE security and privacy workshops (pp. 180-184). IEEE.