Distributed Ledger Technologies in Supply Chain Security Management: A Comprehensive Survey

Mary Asante [1], Gregory Epiphaniou[1], *Member, IEEE* Carsten Maple[1], *Fellow, IEEE*,
Haider Al-Khateeb[2], Mirko Bottarelli[2], Kayhan Zrar Ghafoor[3]
[1]Warwick Manufacturing Group (WMG), University of Warwick, Coventry, CV4 7AL, UK
[2]School of Mathematics and Computer Science, University of Wolverhampton, Wolverhampton, WV1 1LY, UK
[3]Department of Software Engineering, College of Engineering, Salahaddin University-Erbil

Supply-chains (SC) present performance bottlenecks that contribute to a high level of costs, infiltration of product quality, and impact productivity. Examples of such inhibitors include the bullwhip effect, new product lines, high inventory, and restrictive data flows. These bottlenecks can force manufacturers to source more raw materials and increase production significantly. Also, restrictive data flow in a complex global SC network generally slows down the movement of goods and services. The use of Distributed Ledger Technologies (DLT) in supply chain management (SCM) demonstrates the potentials to to reduce these bottlenecks through transparency, decentralization, and optimizations in data management. These technologies promise to enhance the trustworthiness of entities within the supply chain, ensure the accuracy of data-driven operations, and enable existing SCM processes to migrate from a linear to a fully circular economy. This paper presents a comprehensive review of 111 articles published in the public domain in the use and efficacy of DLT in SC. It acts as a roadmap for current and future researchers who focus on SC Security Management to better understand the integration of digital technologies such as DLT. We clustered these articles using standard descriptors linked to trustworthiness, namely, immutability, transparency, traceability, and integrity.

Index Terms—**Distributed Ledger Technology, Supply Chain Management, Industry 4.0, Cyber Resilience, Data Sharing, Trustworthiness**

I. Introduction

Distributed Ledger Technology (DLT) is a growing area of interest for governments, industry and academia. DLT is a decentralized database located across multiple locations or among various users through consensus algorithms [1]. DLTs operate on peer-to- peer (P2P) networks with no centralised databases or trusted administrators. Features of DLT include transparency, immutability and resistance to censorship [2], [3]. Blockchain (BC) is the most widely known and deployed form of DLT. BC is a cryptographically secure decentralized database that generates a digital log of trusted and immutable transactions which are encapsulated into blocks, a process known as mining, and can be shared across either a public or a private network. According to Bellini et al [4], and Epiphaniou et al [5], all the blocks are timestamped, have their own unique identities, achieved through the hash of the Merkle tree, and the information from the previous block, connecting the blocks. Fig. 6 (b) is an illustration of how the Merkle tree transaction occurs. According to Siris et al [6], Sharma et al [7], and Soni et al [8], there are three main types of BC: Public, Private and Consortium. Public BC are permissionless networks which anyone can join. Private BC are permissioned networks only available for authorized users to join. Fraga-Lamas et al [9] state that a consortium or federated BC is a permissioned network made up of pre-selected and authorized users. Other DLTs that have recently been developed to compensate for the shortfalls of BC namely, scalability and Transactions Per Second (TPS), resulting in high energy consumption. These are Directed Acyclic Graphs (DAG), Hashgraph and Holochain. DAG, the second most used DLT stores its transactions in nodes [10]. It utilizes two previous transactions to validate each new transaction, thus bringing more consensus compared to BC [10]. DLT has many industrial applications including its use in the financial, agriculture, healthcare and energy sectors as well as the supply chain management.

The Supply Chain Management (SCM) is a series of complex global activities, processes and systems which transforms raw materials into goods and services, distributes and deliver them to the end-user. Stakeholders of SCM ranges from small scale raw material producers such as farmers to multinational organizations and governments. The complex global nature of the Supply Chain (SC) presents multiple problems to SCM such as visibility, traceability, scalability, data flow management, trust and associated costs [11]. Industry 4.0, offers an inclusive, holistic approach to SCM through the amalgamation of digital technologies such as DLT, cyber-physical systems (CPS), interconnectivity and access to real-time information to optimize the delivery of goods and services [12], [13]. A digital SC, with activities across the SC becoming much smoother, faster, more transparent, gaining and utilizing insights from real-time information across the entire chain. The authors produced Fig. 1, an illustration of the evolution and timeline for DLT, SCM and the Industrial Revolution based on the works of Xu et al [14] and Rahouti et al [15] on DLT, Stevens et al [16] on SCM and Ojo et al [17] on Industrial Revolution. Fig.1 demonstrates at a glance how the rapid changes in technology such as BC is impacting on Industrial revolution and SC. The SC stands to benefit significantly from the correct implementation of the appropriate DLT within the SC to improve efficiency, increase cyber resilience,

Distributed Ledger Technologies in Supply Chain Security Management: A Comprehensive Survey Corresponding author: G. Epiphaniou

optimize data sharing, gain competitive advantage and increase profit.This paper investigates the role of DLTs, such as BC in supply chain security management.

Zhang et al [18] described SCSM as 'managing potential risks such as privacy leakage and malicious members manipulation, which could happen to any part or process, appeared with enabling information technologies on SC'. Security threats to the SC vary from the physical to cyber threats. To manage these threats, SCM must adhere to the three core fundamental security principles governing the security and assurance of information and systems, the CIA triad, confidentiality, integrity and availability [19], [20], [5]. Achieving CIA in the SC will require risk management [21], security compliance, including compliance with standards [22], cyber resilience [9] and security frameworks and solutions [23]. To help current and future researchers navigate existing knowledge, the authors categorized the state of the art research work surveyed in this paper based on these key components of SCSM: security compliance, risk management, cyber resilience, security assessments and security frameworks and solutions. The taxonomy informed the clustering of special properties of DLT, such as immutability, consensus protocols and provenance, which contribute to making systems more secure into security aspects, enabling us to develop a comprehensive roadmap for current and future researchers.

The rest of the paper is structured as follows: Section II presents a comparison of related surveys in the field. Section III gives an overview of the evaluation criteria and a critical analysis of the extent to which DLT are used and their efficacy in Supply Chain Security Management. Section IV summaries the main findings and Section V gives the future of research directions. A conclusion is drawn finally in Section VI.

II. A Comparison of Related Surveys

The authors used Prisma, as a systematic literature review (SLR) protocol to obtain insights into DLT integration in Supply Chain Security Management (SCSM). Kitchenham et al [24] - [25], Keele et al [26] and Snyder [27] state that SLR must be robust and replicable. By using Prisma, the methodology employed by the authors is robust and can be replicated. A set of keywords were used to initially identify related studies to DLT integration in SCSM through database searches. Additional records were also identified through other sources. Keywords used in the search included "distributed ledger technology", "Distributed ledger technology in Supply chain", "Supply chain security management", "Blockchain", "Supply chain integration", "data sharing and data regulation in supply chain", "Supply chain security emerging technology", "supply chain bottlenecks" "Cyber Resilience", "Trustworthiness" and "Industry 4.0". A total number of 345 articles were initially identified. 50 duplicates were removed. The authors set and used inclusion and exclusion criteria to identify relevant state of the art literature before analysis. 60 articles which were not strongly correlated to the research topic were excluded. 115 were included in the qualitative analysis and 111 in the quantitative meta-analysis. The process employed is illustrated in Fig. 3.

Islam et al [28] conducted a critical review of BC technology using concept maps to depict their features and properties as well as their advantages and disadvantages, with a view of providing a better understanding of BC technology. They outlined thirteen properties of BC which are shared database, P2P transmission, timestamped blocks, immutable records, encrypted data transmission, disintermediation, computational logic, transaction dependency, transaction rules, distributed trust, multiple writers, validation and scalability. Some of the advantages include auditability and verifiability, reliability, robustness, cost reduction, enhanced security and independence from third parties. The disadvantages include latency, less throughput and permanent, immutable records.

Chowdhury et al [1] did a comparative analysis of DLT platforms using qualitative and quantitative criteria to assess a number of both private and public DLTs. Public DLTs are more widely used P2P networks employing consensus algorithms to ensure data stored in the ledger is immutable, thus offering a high degree of integrity. The extensive use of public DLT is due to high trust and confidence levels in addition to their transparency and accountability amongst unknown entities. Public networks are permissionless, anyone can join and any of the participants can have read/ write permission and the consensus process is anonymous. However, they are generally slow and less efficient compared to private and consortium networks [8]. Private DLTs have been developed to resolve the issues that public DLTs are faced with, such as scalability and high energy consumption. Access to Private DLT networks are only through authorization of known identifiable trusted entities. However, by so doing, security offered by immutability in private DLT is compromised. It is partially decentralized, with read/write permission restricted to authorized users and consensus is achieved through known authorized users, thus no mining is required, resulting in reduced overheads. Private DLT is hence more scalable, much faster and less energy-intensive. Consortiums are formed through a number of organizations coming together to form a network. They are similar to private networks with known and preselected participants. They are also partially decentralized, more scalable, much faster and less energy-intensive. However, according to Maple et al, consensus is achieved through a few pre-selected participants [29]. In selecting the appropriate DLT for integrating into the SC, consideration must be given to which DLT platform will be most suitable for the intended purpose whilst ensuring adequate security. For example, a consortium platform may be more suited to the SC as it allows different known organizations to openly share information in a secure manner. Private networks may be more suited for environments in which higher security is required and more sensitive data is shared.

Security by design of systems offering CIA assurance to systems and their users is highly desirable and mandatory in some cases. DLTs have inbuilt security due to their cryptography feature. Data can also be encrypted from the onset. DLT is thus able to address security flaws associated with AI and IoT [30] (see Fig 3. for key security aspects of DLT). However, there are security concerns about DLT associated with their distributed, decentralized and transparent nature which can be

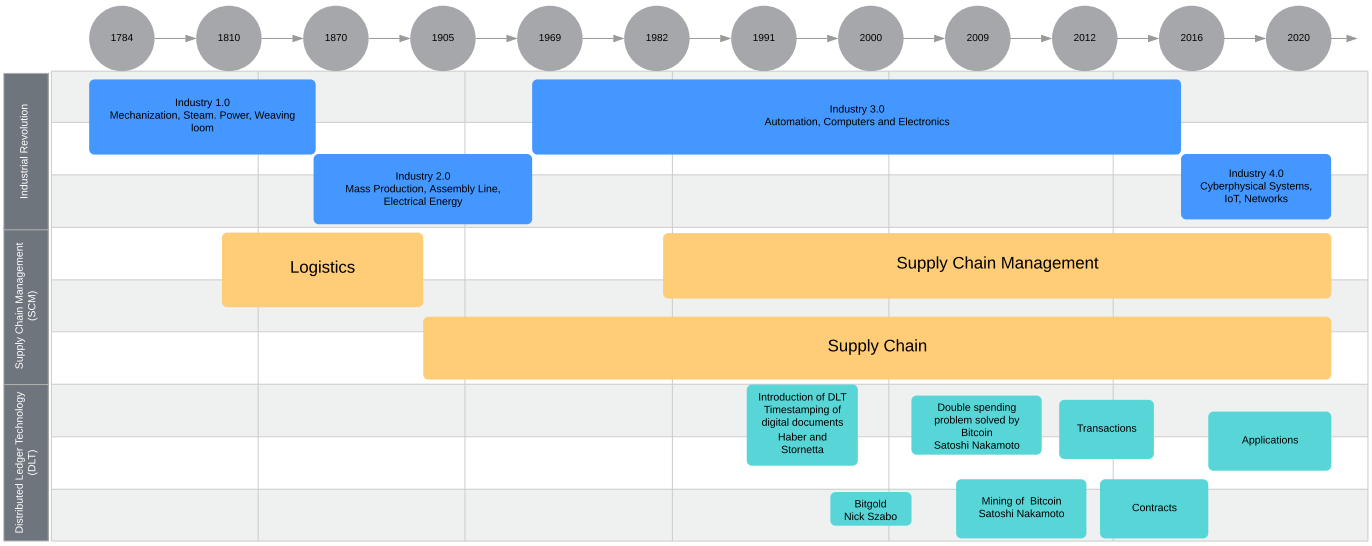


Fig. 1. Evolution and Timeline

exploited by threat actors who gain access to the information for malicious gain. These include a 51% attack which could lead to a DDoS, privacy leakage, scalability and selfish mining. There are also serious concerns about identity management and privacy in DLT networks as actors might be able to deduce identities of users and their linked transactions from the information distributed in the system [20].

In their survey, Rahouti et al [15] explored using ML techniques as countermeasures against the threats that BC technology, particularly Bitcoin faces. They highlighted that security concerns in Bitcoin networks stem from the financial and monetary gains that actors could potentially benefit from. These include pool hopping attack (transactional information is exploited for selfish mining), bribery, theft of private key through access to miners local networks and exploitation of known network vulnerabilities. Double-spending challenges have been resolved by the Nakamoto protocol. Newer DLT such as Ethereum is designed to overcome the shortcomings of Bitcoin, for example, features and functionality of smart contracts. Rahouti et al [15] suggest that ML could be employed to detect irrational behaviours and abnormal activities of participants of a network. These unusual activities will then be flagged for the necessary preventative action or corrective actions to be taken to minimize the damage they can cause. However, they concluded that research aimed at providing this solution is very limited.

Sharma et al [7] discussed the security challenges arising from the integration of BC and IoT. The challenges include lack of standards, secure integration, the complexity of communications, software updates, scalability, low fault tolerance, DDoS, Sybil attacks and validation and verification protocols. Single attacks on IoT devices can potentially affect the entire BC-IoT integrated network. The system can become inefficient due to large data sizes involved. They advocate incorporating malware detection mechanism for detection of malicious nodes and the development of IoT centric consensus protocols.

Soni et al [8] conducted a security analysis on BC. They stated that malicious actors could potentially change the structure of the entire chain, for example, in 51% attacks or a denial of service in DDoS attacks. Transparency and visibility of BCs means that all bugs and transactions are displayed across the entire network and can be exploited. Programming frauds can also be exploited, leading to piracy attacks. Further attacks include private key leakages due to theft, sybil and eclipse attacks.

Onishi [31] explored the security implications of integrating DLT into V2V communications. They explained that the move could enable malicious actors to hack into vehicle systems posing real risk to drivers and other road users. The actors may take over a vehicle communication system or that of a chain of vehicles and interfere with their communications with each other. It could also lead to the theft of personal information, driving history, GPS spoofing and eavesdropping. The tradeoff between safety and security as well as financial incentives in BC integrated applications are a major concern and a potential limitation to their application in the automotive industry. Consensus protocols resulting in smaller blocks being ignored could have safety implications for vehicles with small stakes in the BC network. There are also potential interoperability issues which may result in further safety security challenges.

Conti et al [32], and Shalini et al [33] explored security threats to Bitcoin networks and countermeasures to combat them. As the most established cryptocurrency, Bitcoin attracts a lot of interests from all kinds of parties. Bitcoin networks are subjected to continuous security threats. Consensus protocols such as PoW is employed to prevent double-spending. The suggested countermeasure for 50% attacks (block discarding and difficulty rising attacks) is to attach a financial penalty to the attacker nodes whilst rewarding the informants. To discourage selfish mining which leads to private forking and pool attacks, suggested solutions include timestamping blocks in the chain using Random Beacons to stop selfish miners allocating future timestamps to their blocks. Other suggestions involve

Fig. 2. Taxonomy: Distributed Ledger Technologies Integration in Supply Chain Security Management

the inclusion of a fork-resolving policy that proactively ignore blocks that are not published within a set time. ZeroBlock, a timestamp free solution operates on a similar principle which allows honest miners to reject blocks that are mined for longer than a set interval. Miners could also be encouraged to publish intermediate blocks by adopting the chain with the most amount of work not the longest in another proposal. A minor can be bribed by an attacker who uses the miners resources to gain more hash power. This is then used to roll out further attacks in the network subsequently. Counter-bribery, the suggested countermeasure could, however, be potentially very costly to operating managers. Secure wallet protection will safeguard against private key leakages and theft. The core protocols of Bitcoin and the P2P network infrastructure can be secured for improved security. Additionally, measures to improve the privacy and anonymity of miners are proposed.

Xu et al [34] discussed the cost implications of security challenges in the maritime SC which could be up to $50 billion (loss cargo) and high administrative burden in a bid to prevent illegal activities and terrorism. Systems such as CargoNet, C-TPAT, and CSI are already in place to deal with the security threats, but they are heavily reliant on efficient and timely information sharing for them to be effective. According to Xu et al [34], the BC-based maritime management system

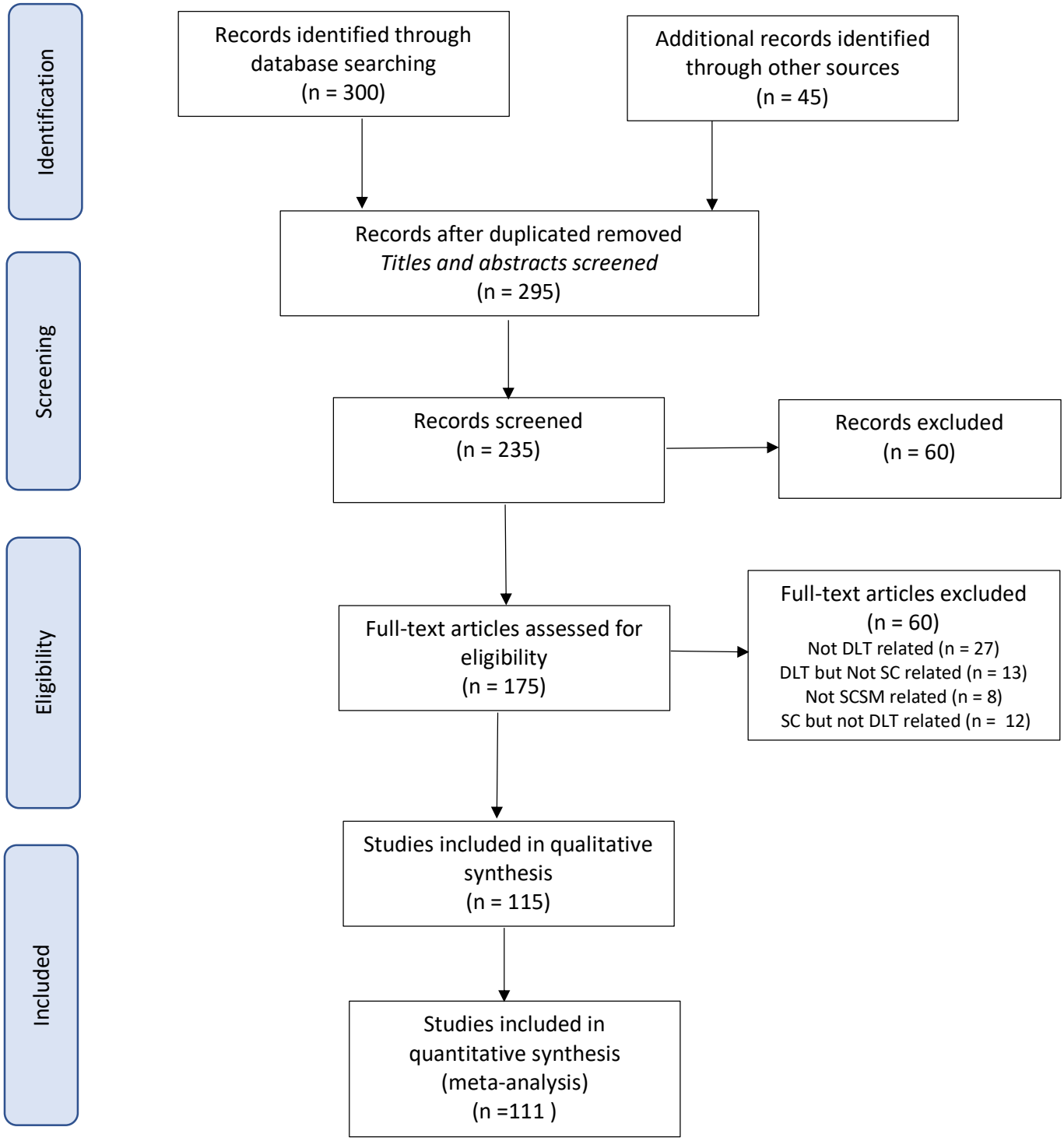


Fig. 3. Prisma SLR Protocol

provide all stakeholders real-time and instant information, resolving this issue. Information security assurance, CIA, is achieved in the system as follows: immutability preserves the information's integrity, confidentiality is afforded by the use of a private or consortium permissioned BC and the removal of single point of failure in the distributed network ensures availability at all times.

Mylrea et al [22] argued that security is not always on the priorities of suppliers and providers of the energy SC. This implies that EIoT systems do not have security by design. Process automation through the use of smart contracts and enhanced cyber resilience based on the inherent security features of BC will benefit the system greatly. This will ensure automatic updates and patch management. The authors advocated the use of permissioned BC, employing PoA consensus protocols for improving trust, integrity of the data whilst maintaining confidentiality. The system will be fast and scalable. Effective system functionality and availability is crucial in the EIoT environment. The use of smart contracts, together with the immutability of records, will ensure the integrity of the information. Protection of IP and the prevention of espionage are important considerations for critical infrastructure. It is absolutely essential that access to the system is controlled and information disseminated on a need to know basis which could proof challenging for BC technology. There are also concerns around interoperability of BC, optimization of the system and the security of the critical infrastructure. Interoperability issues may be resolved by the use of intermediate links between various BC and databases in the network.

Epiphaniou et al [5] conducted a detailed threat analysis of their framework. They stated that CIA assurance is an important security aspect of the system. High productivity levels and protection of proprietary are also essential features. BC naturally offers security enhancement to the system, but it also poses a threat to it due to its vulnerabilities. Spoofing at both the network and application levels which could facilitate man-in-the-middle attacks or unauthorized access to a secure permissioned network. DDoS attack, Cross Site Scripting and SQL injection threats are possible at the system's web interface. Data in transit could be tampered, affecting the CIA of the data. Information leakage is possible both at the user and system administration ends if the system is compromised or access control is bypassed. Data exfiltration is also possible through the exploitation of an unpatched vulnerability in the network. Multiple encryption of data stored and distributed in the system offer protection to redundant data. Malicious actors could gain privilege access by exploiting implementation vulnerability or misconfiguration. This will be prevented by the implementation of mandatory access control systems. Additionally, the trust model of permissioned networks could be exploited to gain access and to cause issues in the networks. However, mining related attacks are less likely due to the permissioned BC.

Salman et al [35] investigated BC approach to authentication, confidentiality, privacy and access control list, data and resource provenance, and integrity assurance for various services. These services include BC Public Key Infrastructure (PKI) and domain name services (DNS), BC Identity Based Cryptography (IBC), BC for securing Information-Centric Networking (ICN), BC Data Provenance and BC Trust Authentication for Decentralized Sensor Networks. Security challenges associated with the integration BC in these services like many applications are scalability, exploitation of information by actors who gain access and computation resource required for the P2P network. Further development is required to overcome the security challenges before full implementation of the services.

Hou et al [36] proposed a socio-technical framework, SEISMiC (SEcurity Industrial control SysteM supply Chains), to holistically deal with the security risks (physical, technical, human and organisational) associated with the complicated SC, the backbone of CPS such as Industrial Control Systems (ICS). ICS is used for managing critical infrastructures such as water treatment and distribution, gas and electricity supply as well as automation and manufacturing. Several standards have been developed to establish good practice for defining system security requirements, but they operate on the assumption that CPS infrastructure exist in isolation [93] without consideration for its SC. These frameworks include the National Institute of Standards and Technology (NIST) SP800-82 and SP800-82r2 and the UK Centre for Protection of National Infrastructure (CPNI) Good Practice Guide for Process Control and SCADA security. Through its integrated approach, SEISMiC gives a full projection of the entire security risks, leading early identification of risks and informed risks management decisions.

Alotaibi [37] investigated the use of BC security features to address IoT cybersecurity related risks. BC-IoT integration will provide security enhancements in several IoT environments. Resource capacities and capabilities of IoT devices will be securely enhanced by the decentralized, distributed, shared resources and immutability properties of BC. End-to-end traceability will help fight theft and loss of cargo, for example in the shipping industry by tagging and tracking products and sharing the data throughout the SC. Other security benefits are data privacy and anonymity, identity verification, authentication and CIA. Early detection of IoT device defects is essential for successful and secure implementation of BC-IoT systems.

Karamačoski et al [38] stated that security attacks associated with communication channels include eavesdropping, snooping, replay attacks, intentional data corruption and jamming. Security benefits of a distributed communication system include data encryption, the immutability of the records stored, the decentralized distribution of the coded message, privacy and increased security. Multi-layered security levels provide additional security to systems. DCC protocol is leveraged in wireless communication networks to ensure secure communication between nodes.

According to Perez et al [39], online transactions have four main security aspects requirements: confidentiality, authentication, data integrity and non-repudiation. According to the authors, the landscape of information security management systems is being shaped by BC technology. They came to two separate conclusions on the pros and cons of BC on Information system for online transactions. Firstly, off-chain addresses the issue of confidentiality and data integrity and

can be successfully implemented for Ecommerce. Secondly, BC technology is still a while away from global acceptance and implementation. They concluded that further development is required for online transactions to fully benefit from the security aspects.

Fraga-Lamas et al [9] outlined BC technology's key capabilities for cybersecurity which can be implemented in a decentralized security model based on the lightning network and smart contracts. It has four main stages: registration, scheduling, authentication and charging. It can be integrated into existing scheduling mechanisms to enhance the security of trading between electric vehicles and charging piles. Bugs in open source codes used can be exploited. The security benefits include integrity, transparency, security and automated data flow, resulting in better efficient and more affordable systems.

Vinayak et al [40] explored security vulnerabilities of smart contracts. Vulnerabilities associated with Oyente include transaction-ordering dependency which could be exploited by selfish miners. Timestamp dependency can be exploited to inflate prices by sellers. Mishandled exceptions may lead to false contracts and transactions. Re-entrance vulnerability and Integer overflow/underflow. In conclusion, the wait time between contract validation and signing can be exploited by malicious actors and selfish miners to the disadvantage of honest miners.

A. Cyber Resilience

Cyber resilience is the ability to maintain operation of a system when it is under attack. It is set by the system's risk acceptance threshold. Onwubiko [41] argues that cyber recover should be built into cyber resilience.

Consensus protocols in DLT contribute to cyber resilience of DLT systems. Shahaab et al [3] and He et al [42] argue that Consensus is at the core of any DLT. The security of data shared and stored in the network due to immutability of DLTs makes them invaluable to many industries including SC. Furthermore, Sharma et al [43] explains consensus mechanism as the decision making process which promotes and ensures fairness and equal opportunities in distributed networks whilst Saini et al [44] describes it as integrity maintaining algorithm. Shahaab et al [3] debate that it is difficult to achieve consensus in distributed systems as the protocols must be resilient to failure, network partitions, message delays, ordering and corruption. Unlike public DLTs which offer competitive consensus mechanisms, consensus in private DLTs are more through partnerships. Building resilience into DLTs to overcome challenges such as node failures, corruption and message delays can be easily achieved in private DLTs due to control and authority over the consensus-building process.

Wang et al [45] applied the game theory to consensus protocols during the mining process and explored how miners can take advantage of the incentive mechanisms of Nakamoto protocols in public networks. They argue that nodes will ignore bigger block sizes as they take longer to process and relay smaller nodes to remain competitive. They also highlight that mining of empty blocks has the same effect as DDoS.

Byzantine fault tolerance (BFT) is the mechanism of reaching consensus between nodes within the network which may have faulty nodes, either not responding or providing misleading information. Highly functional algorithms built into Practical BFT (PBFT) is based on the assumption that nodes are dishonest, thus rely on trusted nodes in the system [46]. Other forms of BFT are Stellar consensus protocol [47] and Delegated BFT. Proof of work (PoW), Proof of stake (PoS), Proof of Elapsed Time (PoET), Proof of Storage and Proof of Authority (PoA) are also types of consensus protocols for validating transactions [32], [43], [48], [47]. Monrat et al [46] made several suggestions for improvement such as standardization and testing based on selected criteria to determine the capability of the system. They suggested that traceability of BC could be relied on for ownership and integrity of assets, intellectual property (IP), copyrights and trade secrets.

Epiphaniou et al [49] described scalability as one of the major challenges of BC technology and other DLT. Kim et al [50] categorized scalability into three groups: Throughput, Cost and Capacity. The maximum potential of Throughput is restricted by the limit of block size and the time taken to produce them [51]. Costs associated with 'pay per transaction' makes it expensive for its users. By storing all transactions in the chain, the capacity required to keep the network working effectively becomes enormous. A varying degree of possible solutions proposed includes On-chain, Off-chain, Side-chain, Child-chain, and Inter-chain solution, all designed to make the network more scalable.

1) Risk Management

Risk management is the process of identifying, analysing, evaluating, treating and monitoring and reviewing any residual risk. Fu et al [21] acknowledge that the SC is subject to both internal and external risks. Barron et al [52] argue that the introduction of new technology into the SC introduces new risks, making SC risk management difficult. BC characteristics such as traceability, transparency and smart contracts can help with the identification of risks in the SC. Lu et al [53] classify SCS breaches as a special form of SC risk. They argued that ISO's concept of SCSM encompasses more than the traditional definition of risk management, it takes into account lessening the impact of breaches once they occur.

The potential benefits of improved traceability and transparency to the SCM include a reduction in transaction costs by removing third parties from the SCM, security enhancement and improvement in product quality as well as decreasing the time for getting goods and services to the end-user, leading to an increase in customer satisfaction. In their critical analysis of BC and traditional databases, Chowdhury et al [54] outlined parameters that could determine whether BC technology is used or a traditional database is used. They established that in use cases where trust, robustness / fault tolerance, redundancy or security are paramount, BC emerged as the preferred choice. However, if data confidentiality and performance are the key driving factors, then currently, traditional databases offer a better solution.

B. Security Assessments

Security assessments test the vulnerabilities and weaknesses in a system. Threat modelling may be used to identify vulnerabilities in a system. Traditional assessment of vulnerabilities

in IT systems and business processes mainly involve the use of penetration tests. Vulnerabilities in DLT systems are visible to the entire network and may be exploited by threat actors. Soni et al [8] in their security analysis on BC considered some of its vulnerabilities. Attacks on consensus protocols could give an adversary greater control in the BC. Control of 51% of the hashrate could lead to double-spends and stop others from participating in the consensus protocol [46]. Distributed Denial of Service (DDoS) attacks are costly to organisations as their services become unavailable to their users. The exploitation of fraudulent programming codes interferes with the security properties of BC. Private key leakage, where attackers gain unlawful access to an account's private keys and launch an attack on the network. In Eclipse attacks, adversaries stops nodes from connecting to genuine nodes. There are associated privacy risks where users can be de-anonymized. [8], [55] recognize that other DLT such as DAG offers solution to the security and privacy concerns.

Smart contracts are formed out of a set of programmable rules formulated in the system. Once the criteria for the rules are met, contracts are automatically formed between entities, signed and are binding [56]. These contracts are immutable, visible and accessible to all participants in the network, promoting trust amongst trustless entities. Sandbox style programming language, such as Solidity, Serpent, Low-level lisp-like language (LLL), Mutan and Viper, is one of two ways of presently supporting smart contracts in BC. Integrating them into the internal API of the network via containers is the second. The API methodology is deemed to be more attractive to private systems, notably used in the Hyperledger Fabric. Maple et al [29] describe a number of cryptographic techniques used for transactions signing within systems to authenticate the data source and to maintain its integrity. These include Elliptic Curve (EC), in which participants utilizes digital signature algorithms (DSA) such as Elliptic Curve Digital Signature Algorithm (ECDSA) using their private keys to sign transactions, which are then verified by the participants of the P2P network.

Potential applications of smart contracts can be in compliance, traceability, anti-fraud and anti-counterfeit controls and management of services. Several limitations associated with smart contracts were also highlighted including privacy / confidentiality, insufficient computational power for PoW on devices and high transaction costs by Golatowski et al [56]. Visibility of smart contracts enables the public to see all the transactions, these could be maliciously exploited and used against the BC.

Selfish mining gives miners an unfair advantage over other miners. Exploiting the mining strategy, selfish miners could withhold information in a private chain and grow it to the extent that gives them a bigger stake or reward [32], [45]. Selfish miners then release their chains to the main chain, creating forks, parallel chains to the main chain, which confuses other miners into believing that they are the genuine blocks. These forks can be exploited by malicious users, posing a security risk to the BC integrity. They also waste the time of genuine miners. [32], [33], [15] in their surveys highlighted some security risks to BC cryptocurrency, Bitcoin as double-spending, wallet attacks (client-side security), network attacks (DDoS, Sybil and eclipse) and mining attacks (withholding and bribery) [57]. Conti et al [32] discussed a series of countermeasures to combat the identified security threats.

Vulnerabilities in smart contracts are discussed in detail by Vinayak et al [40]. They identified smart contracts as a user-defined algorithm that runs on the BC. Smart contracts are permanent and cannot be altered once created. This creates a vulnerability which can be exploited by attackers who may already be part of the network. A tool, Oyente was used to analyse these vulnerabilities in financial transactions using the following categories: Ordering Dependency, Timestamp Dependency (can be altered by roughly 900 seconds), Mishandled Exceptions, Re-entrance vulnerabilities and Integer overflow / underflow. [40] refers to some essential conditions which needs to be incorporated in BC that are not currently available. However, it does not specifically state what these conditions are. Murray et al [58] in their survey recommended undertaking formal verification for smart contracts on DLTs using a number of frameworks or models. The purpose of which will be to increase trust levels in smart contracts. They also recommend establishing a library of formally verified, reusable blocks and patterns for developing the contracts.

C. Security Compliance

According to Yousef et al [11], the global complex SC could benefit from having minimum standards and requirements which various stakeholders should comply with. However, achieving security standardization in the global SC is difficult due to differences in government regulations around the world and organizations and suppliers having to comply with different rules depending on their home-base and their SC network.

Mylrea et al [22] describe how the increase in critical cyber assets, data speed and size requirements in Energy IoT (EIoT) led to the formation of the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) compliance requirements. The energy SC faces cybersecurity challenges as a result. The criticality of the threats is evident by the Federal Energy Regulatory Commission (FERC)'s order to NERC to deal with Cybersecurity SC risk management for industrial control systems software and hardware, and the networking and computing services associated with Bulk Electric System (BES) operations. This will require enhancement in technology and process improvement. Deploying BC in EIoT SC will help improve security, traceability and transparency.

Data privacy is becoming increasingly important with the growing commoditization of personal data in Industry 4.0 [13]. Onik et al [13] make a clear distinction between data privacy and data security. They argue that there can be data privacy breach without any technical or security breaches. Although strict security measures will contribute to data privacy protection, the lack of effective regulation, monitoring and accountability are the main reasons for data breaches. Management of data privacy risks is therefore required. Effectively managing Personally Identifiable Information (PII) to prevent their exploitation [59] by the use of various techniques, regulation and technology such as BC integrated solutions will

be key to ensuring data privacy. However, records on BC are permanent which is against general data protection principles in which an individual has the right to be forgotten.

Data privacy regulations such as GDPR (General Data Protection Regulations) aim to give the data owner a lot more ownership and control over their own data. This include control over who has access to the data and visibility of why they need access to their data, what they intend to use it for, where it is stored and how it is processed. Organizations within the SC may either be data controllers, data processors or both under GDPR. Both data controllers and processors have duties to protect the data, make their intentions for the use of the data very clear and also declare to the owner who else within their SC will have access to the data. There is also a requirement to ensure that the data is accurate, portable and must be destroyed if no longer needed or if the owner exercises their right to be forgotten. This may present a challenge to BC integrated platforms where the data once created is permanent and immutable. Salman et al [35] described an ideal BC-based data privacy solution, to be achieved through the introduction of BC layers, providing encryption over the data storage layer. As with other permissioned networks, the data owner will be able to define an access control list (ACL) through smart contracts or particular management transactions, which decides who can access their data in the network. [35] also discuss how BC technology can improve data provenance, tracking and integrity in the SC. A number of tried and tested use cases include Provenance and IBM SC, an enterprise project for tracking physical products and their journey through the various SC processes to the end-user. Several other startup organizations operate in this space too. It was however recognized that for full privacy guarantee to be met, more research is needed in order to achieve 100% privacy and anonymity in BC technology. Bernabe et al [60] investigate a user led approach to improve privacy in BC technology through the use of Self-Sovereign Identity (SSI) models. The solution allows users to retain more control over what details they share and whom they share it with.

Security of the hardware in DLT is reliant on those of the hardware in the systems. Belotti et al [61] highlighted some of the challenges in relation to DLTs such as performance evaluation, standardization, regulatory and governance due to the number of variations of DLT platforms available. These were suggested to be the reasons why DLT such as BC has not been widely adopted in industry including the SC. [61], [62] highlighted some of the work being done in an attempt to standardize DLT and BC platforms by a number of working groups: ISO/TC 307, Internet Research Task Force (IRTF), Decentralized Internet Research Group (DINRG), the W3C BC Community Group, OASIS/ISITC Europe BC Working Group and ITU-T.

Improving privacy and anonymity in BC were the main areas of focus in [63]. Park et al [64] state that although anonymity is at the heart of a P2P network, users and their activities can be traced using publicly available information on the chain. Measures employed to ensure anonymity and privacy such as Network anonymizers prevent mapping of IP addresses to Bitcoin addresses. Homomorphic commitment could be used to hide parts of transactions such as amounts and cash transfers. Zero-knowledge method will then be utilized as a mechanism for verifying the transaction amounts as described by Deng et al [65]. However, this is contradictory to transparency and traceability, which are key characteristics of BC technology. The paper concludes that researchers need to do more to discover effective ways of assuring anonymity and privacy of BC.

Mylrea et al [22] describe how the increase in critical cyber assets, data speed and size requirements in Energy IoT (EIoT) led to the formation of the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) compliance requirements. The energy SC faces cybersecurity challenges as a result. The criticality of the threats is evident by the Federal Energy Regulatory Commission (FERC)'s order to NERC to deal with Cybersecurity SC risk management for industrial control systems software and hardware, and the networking and computing services associated with Bulk Electric System (BES) operations. This will require enhancement in technology and process improvement. Deploying BC in EIoT SC will help improve security, traceability and transparency.

Data sharing within the traditional SC is limited due to organizations largely operating their infrastructure, technology and processes in isolation to other organizations within the SC. Traditional SC transactions are still heavily paper-based, requiring lots of manual entries due to the lack of interoperable systems. Intermediaries also play a major part in distributing documentation and information in the traditional SC, adding to operations costs. Individuals and third parties are easily identifiable from the information on documentation and as such are more prone to identity theft and exploitation by malicious actors. The need for secure end-to-end information sharing and greater visibility of customer demands coupled with the ability of suppliers to meet the demand in a timely fashion through available resources is driving the demand of the digitalized SC. Electronically sharing data securely throughout the SC will enable organizations to make informed decisions based on real-time data, which will help shape their business strategies and models [66], [67]. However, the ability of different organizations to fully integrate their infrastructure, technology and processes in order to realise end-to-end integration is hampered by the lack of standardized business processes, technology platforms and operation standards, rendering such attempts insecure, costly and ineffective. Information flow in Digital SC is controlled by central authorities who may present performance bottlenecks. The security aspects of DLT afforded by cryptographically encrypting data, timestamping, immutability of records, transactions through smart contracts, distributed and decentralized nature of the networks will help optimize information flow in the SC by providing better accountability, improve efficiency, enhanced security, increase visibility, reduce errors by automating transactions and processes and reduce costs by removing the need for intermediaries and central authorities [18], [68].

However, interoperability issues relating to DLTs are widely discussed in different surveys. A number of approaches have been proposed to address and establish interoperability among various DLT platforms and applications. These are classified as

interledger approaches [6]. The concept is to move towards a model that facilitates multi-ledger interconnection, one which enable users to benefit from the capabilities of interconnected systems. The study categorized the current approaches into 6 categories based on the initial application assumptions and Interledger Protocols (ILP). These are Atomic cross-chain transactions, Transactions across a network: Lightning and Raiden, Layered value transfer protocols (W3C ILP), Bridging approaches, Sidechains and Ledger-of-ledgers approaches. A shared rational for all the approaches is stated as the need to step away from the "one chain rules them all" model to more flexible and innovative ones. Siris et al [6] explored whether the different approaches support the transfer or the exchange of value, their interconnection trust mechanism, complexity, scalability and transaction cost. They concluded that the SC with its complex structure will benefit from Interledger approaches.

The opportunities, benefits and challenges for incorporating BC into various industrial applications were explored by [69], [70]. BC can offer capabilities to governments [71], authorities and organizations for the identification of individuals, organizations and entities. This may significantly cut down administrative cost and burden and improve information sharing across all the entities who have the need to know and access this information. The immutability of records, smart contract and transparency of transactions capabilities of BC all provide opportunities for enhancing security whilst optimizing industrial processes. In the Financial industry, BC can provide a secure registry for verifications and validations of transactions and to prevent overpayments of amounts owed. BC can also be used to increase transparency and auditability for financial transactions and financial settlement processes. BC can foster global P2P transactions, as seen in the cryptocurrency markets without the need for centralized authorities and intermediaries. Similarly, BC can be used in the Insurance industry for negotiating price, buying, claim processing and renewal activities. In the Healthcare industry, BC can be used for storing and sharing patients records (Electronic Health Records (EHR)) and make them readily available to different providers to improve patients care. It can also facilitate patient billing between providers and insurers. BC offers patients potential ownership and control to their health records. The security, privacy and integrity of patients sensitive data are some of the challenges that need to be overcome before the Healthcare industry fully embraces BC solutions. Other industrial applications of BC will be in the Logistics, Manufacturing, Energy, Agriculture and Food, Robotics, Entertainment, Construction and Telecommunication. In reality, BC technology can be securely deployed in any industry if the concerns around security, privacy, scalability, regulation, integration and skills can be adequately addressed.

Demir et al [72] argue that there are low trust levels in the utility industry, very little flow of data among entities and a central authority is required due to regulatory requirements. [72] observes that the ecosystem of the energy market is changing as more and more consumers are also producing energy through solar panels and in some cases, selling back to the grid. Siano et al [73] evaluate the use of DLT in the energy industry to promote P2P transactions. The concept of using DLT in the energy grid for all transactions will facilitate P2P networks without the need for a centralized control system, creating a virtual decentralized grid. The reliability of consensus protocols and smart contracts make DLTs the most suitable option for solving issues around the outdated traditional centralized energy networks in an efficient and sustainable manner.

Kshetri et al [23] explored using BC in the SC industry across Asia to improve traceability, improve efficiency, provide provenance and increase trust. They suggested that food safety and security can be improved with the use of BC technology. BC can be used to assure end-users that their food is from a sustainable, legal and ethical source. BC stores the full data set relating to the production, transportation, inspections and ownership, which can be made readily available to all stakeholders [74]. Additionally, Jaiswal et al [**?**] smart contracts will eliminate the need for intermediaries in the food SC, making it possible for producers to sell directly to end-users, thus reducing cost for the end-users whilst giving the producers more money. Kshetri et al [23] predict that future implementation cost of DLT will be lower, allowing for potential usage increase throughout the SC.

Fraga-Lamas et al [9] conducted a review of BC technologies in the automotive industry SC. They considered the benefits to all stakeholders along with their challenges. DLT technologies such as DAG can improve operational efficiencies, increase cyber-resilience and reduce cost by removing intermediaries. Whilst vulnerabilities posed by sources such as codes and infiltration of the SC by malicious actors could damage brand reputation and lead to potential financial losses or loss of life. Although optimistic about the use of DLT such as BC for trusted information sharing, various applications, for example, 'As a service' business models in the industry, strong recommendations were made on overcoming the challenges such as technical complexity, interoperability issues, standardization, legal aspects, infrastructure and architecture before full implementation [31], [75].

Juma et al [67] focussed on the use of BC and information sharing in optimizing Trade SC. They discussed how PoA can be used to reduce the administrative burden in trade processes. BC can be used to process and store all relevant information including the bill of laden, commercial invoice and certificate of origin. These will help customs officials identify the source of the goods, the distribution channels and the customer who ordered the consignment, making clearing process efficient. BC could be used to improve and optimize electronic trading solutions. BC technology could be used to enhance the validation processes to help prevent counterfeits in the Trade SC. Smart contracts could be implemented to improve traceability in highly regulated trade environments such as pharmaceuticals.

Dunphy et al [76] explored the role DLT can play in the development of new digital identity management systems. They discussed some of the known challenges that DLT could solve, including identity fraud, data breaches and lack of reusability of identities for different purposes. However, they argued that there ought to be a tradeoff as to which feature

of DLT, immutability, transparency or privacy is prioritized in the system design. They highlighted that DLTs provide financial incentives to miners at a cost to users, compared to free digital identity technology widely used now, developers may be discouraged from dedicating their time and resources in this area.

Weiss et al [77] explored the application of BC to spectrum management. Spectrum sharing may benefit from the decentralized nature of BC to remove the need for a single central authority and the use of smart contracts for secure transactions. Additional benefits may include an increasing speed in resource evaluation and better decision making processes. Spectrum management can be streamlined as certain roles in the traditional centralized management structure will no longer be required. The authors expressed concerns around the BC application reducing the income stream for policymakers and regulators due to potential easier access and low cost. They concluded that BC application to spectrum management would require profound architectural and operational changes.

Lallas et al [78] define Industrial IoT (IIoT) as "smart and cheap sensor based devices lying on top of machines or machine parts, to collect and process massive raw data and therefore to make intelligent decisions autonomously, without human intervention" [78].

Liu et al [79] explored the integration of BC and Machine Learning (ML) and their interrelationship for communication and networking systems. They argue that both BC and ML can mutually benefit from their respective strengths. ML can be enhanced by the inherent features of BC, resulting in improved data and model sharing, security and privacy, decentralized intelligence and increase trust in decision making. ML can also help BC optimize energy and resource efficiency as well as scalability. Smart contracts can become smarter with ML and security and privacy can be improved by deploying algorithms for detecting irregular behaviours and activities. The concept can be generally applied to IoT, big data and edge computing.

Moyne et al [80] explained that the implementation of smart manufacturing and Industry 4.0 may be heavily impacted by increasing security concern. Golatowski et al [56] explored the Integration of BC into IoT for SC optimization in Industry 4.0. They concluded that Blockhain and other DLTs lend themselves very well for integration into IoT and Industry 4.0 due to their distributed and decentralized nature along with other features. They also considered BC and Artificial Intelligence (AI) in terms of open access communication, traceability applications and proof of intelligence (PoI) and concluded that there is a great synergy between the two and recommend the integration of future developments.

Ali et al [62], Golatowski et al [56], Alotaibi et al [37] and Asif [81] explored the integration of BC technology into IoT, the process through which the internet connects devices, machines, objects and humans directly to each other, enabling them to conduct transactions including payments without intermediaries. This can be machine-to-machine (M2M), P2P, or peer-to-machine (P2M) [55]. Cybersecurity was stated as IoT's most critical and challenging barrier. It was recognized that it would be challenging to develop a generally applicable solution for all IoT applications. [37], [47] argue that the minimum security requirements are: anonymity and data privacy, authentication and identity management and data integrity, confidentiality and availability. [62] recommended holistic innovative security by design-based approach combining specific policies and best practice capabilities with specific technical countermeasures aimed at specific technology stacks to overcome security threats of IoT applications. Incorporating privacy-by-design into the build of IoT devices is the way forward to safeguard data privacy [82]. Skills shortage, issues with managing the enormous data accumulated through IoT devices and the lack of standardization and Interoperability were discussed. Most IoT solutions are cloud-based and centralized, integrating BC will enable them overcome some of these challenges by becoming decentralized, more transparent, giving better trust levels and confidence to all users. However, BC technologies themselves have constraints on preserving privacy, scalability [57] and may also be limited by constraints of IoT device capabilities.

Detailed discussions on proposed BC and other DLT based frameworks and solutions for the improvement and optimization of the SCSM can be found in Section III.

III. Evaluation Metrics and Critical Analysis

DLT presents exciting new opportunities as well as challenges for SCSM. The security and privacy of information across the entire SC networks are necessary for ensuring the supply of authentic quality goods and services, protection of trade and sensitive information, intellectual properties, copyrights, brand reputation, fraud prevention and anti-counterfeit measures. Zhang et al [18], Salman et al [35], Saini et al [44], Nalavade et al [20] and Epiphaniou et al [5] explain that with astronomical amount of data being produced and the speed of technological advancement, it is imperative to afford the maximum information security to the SC data in order to ensure their CIA at all times. Sudhan et al [83] state that "the unique nature of BC ensures the CIA of data stored and accessed in a decentralized manner". DLT has special properties which enable DLT integrated systems to have inbuilt data security and assurance, rendering the CIA of systems [84], [14], [85], [86], [28], [87], [8]. As a result, current research work in the area of DLT in SCSM was The authors clustered these properties of DLT based on their security aspects as illustrated in Fig. 4. 10 clusters were identified as crucial to DLTs providing and meeting the CIA of SC information: 1) Encryption 2) Authentication 3) Provenance 4) Consensus 5) Smart Contracts 6) Immutability 7) Transparency 8) Data Privacy 9) Decentralization 10) Distributed.

A. Integrity

Accuracy, consistency and completeness is at the heart of data integrity. DLT fundamentally offers high levels of data integrity to systems through its cryptographic techniques, single source of records, traceability, hashing and timestamping of data [47]. All stakeholders of the SC will have access to accurate data which has not been manipulated to suit any particular stakeholders' need [67]. However, DLT integrated systems have the challenge of balancing the need for privacy

and anonymity with integrity and as such considerations must be given to what the system's priorities are, for designing, building and implementation of systems [63].

1) Encryption

Data encryption is a fundamental feature for DLT. It enables BC users to remain anonymous to the network. Data encryption in public BC is achieved through hashing of the data or by the use of cryptographic techniques such as zero-knowledge proofs [65]. If data is cryptographically encrypted with public key, it can only be decrypted by known entities with the matching unique private key [37], [35]. The challenge for public P2P networks is that the information is available to the entire network and can be exploited by malicious actors. However, private networks and consortiums make use of techniques such as Hyperledger Besu to restrict information sharing to a need to know basis. Data must also be encrypted at rest to minimize the risk of being exploited.

2) Authentication

The authenticity of data in the SC is an important aspect of SC security. It ensures that the data is accurate, original and from a reliable source. It also ensures that individuals and entities are who they say they are, which is necessary in SC scenarios where there is regular exchange of goods, services, information and financial incentives. Data authentication in DLTs can be achieved through cryptographic keys [35].

3) Provenance

Data provenance provides confidence in the origin of the data and its evolution throughout the SC. For stakeholders to have high trust levels in the SC, it must be tamper-proof, traceable, changes tracked and available in usable formats. Data provenance is one of the key features of DLT which can be leveraged by the SC to increase trust levels [54], [88]. Potential applications can be for use in anti-counterfeits and anti-fraud measures, demonstration of ethically sourced products and to monitor product lifecycles.

4) Consensus

As discussed under Section II, consensus protocols are the backbone to establishing trust in BC and DLT networks. Consensus protocols such as PoW, BFT, PoS and PoET ensure that newly created blocks and nodes are genuine, valid and reward honest miners [89], [42]. It is achieved through voting or by agreement between participants in a P2P network for public BC or via selected participants in a private BC or a consortium. Consensus in public BC requires more computational power and is resource intensive. However, in private and consortium networks, the selection of known entities mean that complex voting systems can be avoided thus consensus mechanisms tend to be less resource intensive and more efficient [48].

5) Smart Contracts

Smart contracts enable transactions to take place in networks without human and manual intervention (see Section II). This reduces the number of potential errors, improve transaction rates and saves time. Smart contracts increase trust among trustless entities. Once created, the immutable, timestamped and tamper-proof contracts are distributed to the network [58]. In a complex SC, this will help simplify transactions, provide auditability, reduce administrative efforts by removing intermediaries and improve efficiency. However, security flaws and bugs within smart contract programming can be exploited [90]. Steps must be taken in the development life-cycle to control or eliminate such threats. This can be achieved through rigorous testing and quality assurance processes.

6) Immutability

Immutability is one of the features which make DLT appealing to the SC. The cryptographic hash functions provide immutability. Data once created cannot be altered by any of the participants of a DLT integrated system, as such, the data is deemed as reliable and trustworthy [91], [76]. Auditing processes in the SC can be enhanced with immutable records. End-to-end traceability of products and information across the SC will also be improved by leveraging this feature.

7) Transparency

Transparency makes auditing and inspection of the SC easier as the exact information and products can be traced in real-time [18]. Trust levels are high in transparent networks as transactions and any changes in the chain are visible to all users. Transparency can help prevent fraudulent activities in the SC as it will be easier to detect. It can help control prices of goods and services, with cost information being openly available to all users at every stage. This can be useful in scenarios where governments need to control prices of certain commodities such as food and drugs. It can also help organisations make informed decisions with regards to stocks and inventory as they will be able to effectively track and evaluate inventory across their SC. Transparency may, however be an issue in more secure environments such as in defence applications, where there is a need for secrecy and restricting information to need to know basis.

B. Availability

Information availability is about ensuring that authorized users are able to access the information in a usable format. The distributed and decentralized nature of DLTs enhances the availability of information by removing single points of failure and dependency on central authorities.

1) Decentralization

Bellini et al [4] defines decentralization as the removal of trusted central authorities from systems. Decentralization enables permissionless DLT-based systems to operate effectively and efficiently without centralized authorities. The data is also stored across multiple locations, removing the dependencies of any particular user, single point of failure, for the flow of information [11], [76], [44], [46]. This improves data availability, ensuring data is available to users in real-time, helping with the fulfilment of orders and relationship management. However, permissioned DLT are only partially decentralized as a governing authority still decides the type of consensus to use, who gets voting rights etc.

2) Distributed

DLTs are well positioned to meet the needs of the global SC, distributed around the globe. Yu et al [2], Chowdhury et al [1], and Belotti et al [61] explain that DLTs are themselves distributed in nature, spanning geographical locations, organizations, government agencies, producers, distributors

and consumers. DLT offers distributed trust among the SC. Participants receive copies of information created and stored in the distributed ledger in real-time. Weiss et al [77] argue that the the distributed nature of DLTs has the potential to speed up transactions in the SC by ensuring that data is readily available. It also helps eliminate single points of failure and the need for central authorities. Information systems can as a result be streamlined, become more efficient and cheaper to run.

C. Confidentiality

Data confidentiality is protecting the data against unlawful access, disclosure or theft and safeguarding its privacy. It is achieved by cryptographic techniques, encrypting and decrypting information. Confidentiality is harder to achieve in DLT networks, where information is distributed to all users. Although users are anonymous, all transactions are traceable hence users can be traced through their activity logs [39]. Future developments could help overcome this particular issue.

1) Data Privacy

Data privacy is about ensuring that data is only accessed by authorized entities and that unauthorized access to data is prevented, thus preserving the confidentiality [60]. It is arguably more difficult to maintain privacy in public networks compared to private networks and consortia [42]. Data privacy is discussed in detail under Section II of this paper.

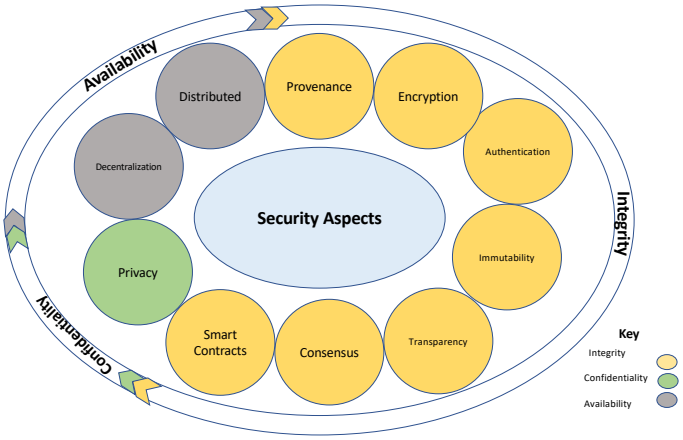


Fig. 4. Key DLT Security Aspects

Security by design of systems offering CIA assurance to systems and their users is highly desirable and mandatory in some cases. DLTs have inbuilt security due to their cryptography feature. Data can also be encrypted from the onset. DLT is thus able to address security flaws associated with AI and IoT [30] (see Fig 3. for key security aspects of DLT). However, there are security concerns about DLT associated with their distributed, decentralized and transparent nature which can be exploited by threat actors who gain access to the information for malicious gain. These include a 51% attack which could lead to a DDoS, privacy leakage, scalability and selfish mining. There are also serious concerns about identity management and privacy in DLT networks as actors might be able to deduce identities of users and their linked transactions from the information distributed in the system [20].

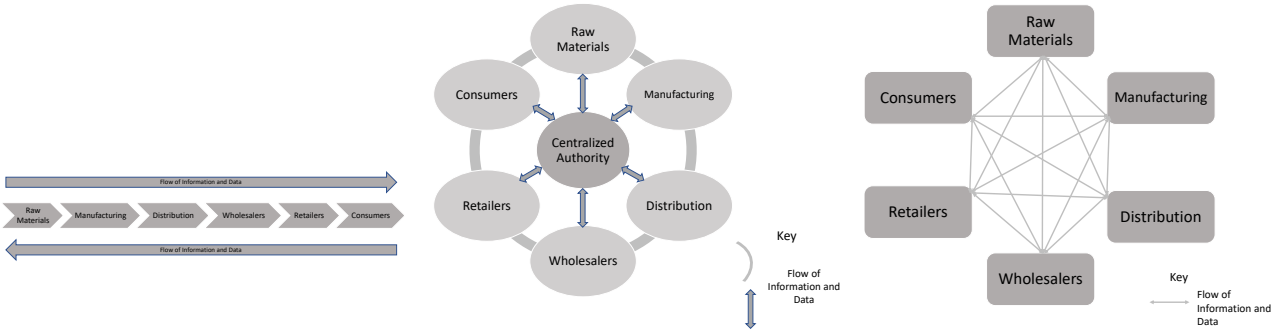
In their survey, [15] explored using ML techniques as countermeasures against the threats that BC technology, particularly Bitcoin faces. They highlighted that security concerns in Bitcoin networks stem from the financial and monetary gains that actors could potentially benefit from. These include pool hopping attack (transactional information is exploited for selfish mining), bribery, theft of private key through access to miners local networks and exploitation of known network vulnerabilities. Double-spending challenges have been resolved by the Nakamoto protocol. Newer DLT such as Ethereum is designed to overcome the shortcomings of Bitcoin, for example, features and functionality of smart contracts. [15] suggest that ML could be employed to detect irrational behaviours and abnormal activities of participants of a network. These unusual activities will then be flagged for the necessary preventative action or corrective actions to be taken to minimize the damage they can cause. However, they concluded that research aimed at providing this solution is very limited.

[7] discussed the security challenges arising from the integration of BC and IoT. The challenges include lack of standards, secure integration, the complexity of communications, software updates, scalability, low fault tolerance, DDoS, Sybil attacks and validation and verification protocols. Single attacks on IoT devices can potentially affect the entire BC-IoT integrated network. The system can become inefficient due to large data sizes involved. They advocate incorporating malware detection mechanism for detection of malicious nodes and the development of IoT centric consensus protocols.

IV. Supply Chain Data Management

In a traditional SC, data flows linearly up through the chain from suppliers to consumers and then back down to the suppliers. At each stage, the stakeholders can determine what information they share and whom they share it with. They can also manipulate the data to suit their agenda. Digital SC has a central database controlling data flow through the SC. The data can again be manipulated and a centralized authority controls the database. In a distributed SC, data flow is achieved through the distributed decentralized network, with copies of the same data available to all stakeholders. Once created, data cannot be altered. Updates and alterations are created as new transactions, providing total transparency and full historical records. Fig.5 (a), (b) and (c) shows a comparison of information flow in traditional, digital and distributed SC.

Ojo et al [17] propose that Optimizing the SC in Industry 4.0 will require an end-to-end integration of technology into the SC. The integrated technology needs to be interoperable, adaptable and secure. Information will be made available in real-time, adding value to the activities and processes of the SC [34]. Efficiency in SC can be achieved by eliminating intermediaries as the information in the decentralized system is available to all users [68], [92]. Communications between businesses across the SC will be improved with adequate data flow and management, leading to improved security and



(a) Traditional Supply Chain (b) Digital Supply Chain (c) Distributed Supply Chain

Fig. 5. Distributed Ledger Technologies for Supply Chain Optimization

better partnerships among industry in the SC [5]. DLT offers SCM the ability to share authenticated information which is validated by users of the network. Solutions and frameworks proposed for optimization of SCM and information sharing must be determined by applications and use cases [67], [22], [61]. A combination of public and private networks will have to be adapted based on the sensitivity of the information shared [91]. BC offers trusting partnership and opportunities for collaboration in the SC due to the transparency of information flow and transactions [54].

SCM bottlenecks contribute to lack of trust, inefficiencies, high levels of costs, infiltrations of product quality, lack of information sharing and transparency. Eliminating these bottlenecks will require the use of DLT in SCM [49]. Yousef et al [11] advocate the implementation of BC at each of the critical stages of SCM, from raw material production through to delivery of order to customers. Features of DLT such as immutability, traceability, trust, transparency and the distributed nature of the network make them a natural choice for SCM optimization across all SC types [93], [68]. Products can be tracked in real time from their origin, through production to consumption [23], [37] using BC technology, providing an opportunity for end-to-end information sharing in the global SC [9]. There is however, a need to ensure that good quality information or data is input into the distributed SC network. The use of smart contracts will also help overcome some of the bottlenecks in SCM [74], [94], [22]. Utilizing electronic transactions in a BC based SCM improves efficiency through the reduction of human errors typically associated with traditional SCM [91].

Mushtaq et al [66] propose that BC can facilitate and simplify the automation of SC in Industry 4.0. This can be achieved through smart contracts and autonomous logistics for delivery of products. Data flow through BC presents opportunities for value analytics, enabling organizations to make reliable timely decisions, helping with the flow of goods and services in the SC. The SC will benefit from smart embedded devices' ability to create immutable data and to distribute autonomously to the network [62].

Ethical SCs are becoming more prevalent with consumers demanding transparency and visibility of the origin of the goods and services they consume and a better understanding of their SC. Divey et al [95] applied a couple of theoretical approaches to the application of BC in SCM. They stated that applying concepts of Game theory will ensure that no one stakeholder can monopolize the entire chain but also the fact that transactions are transparent, visible and immutable means that it is in the interest of all stakeholders to employ optimal strategies in their activities resulting in higher trust levels and better experience overall. Whilst the Grounded theory approach aims to improve social impact and resilience through increased transparency, reduced costs and increase efficiency [95]. However, for these benefits to be reaped by the SC, the entire SC must adopt BC which requires a degree of digital literacy and technical capabilities. The authors recommended that BC is built around existing frameworks and standards. Although this approach will potentially help more stakeholders integrate BC into their activities and networks, it may stifle innovation and creativity, thus slowing down or preventing further groundbreaking work.

Ensor et al [55] hailed Virtualized DLTs (vDLTs) as one of the novel advancements to improve BC technology and make them more scalable, faster, more affordable and more IoT friendly, optimizing Machine to machine (M2M), P2P and Peer to Machine (P2M) transactions. Networks of distributed virtual machines take the load off physical devices making them faster, scalable and affordable. vDLTs can help improve interoperability of DLTs. As mentioned earlier, Interledger solutions also improve scalability, speed and interoperability [6]. However, a lot more work and use cases are needed to test their capabilities.

Demir et al [87] explored the use of BC technology as a trusted provider in the SC of the parcel delivery industry. Their proposed framework, BIDAS utilizes BC technology in IoT networks, turning IoT networks into trusted systems for delivery transactions. This will remove the need for centralized authorities such as delivery companies, controlling the flow of data and information sharing. However, BIDAS focuses on IoT delivery businesses. It relies on users sharing high level of personal and business information which may be available to all participants in the BC. These can be exploited by malicious actors.

The global SC suffers financial losses due to loss of goods shipped around the world, difficulty in inspection of goods at various ports of entry/exit at international boarders, inability to trace goods through the entire product lifecycle and to

prevent the production and distribution of counterfeit goods. Xu et al [34] propose building a BC-based SCM system to help overcome a number of challenges in SCM including transparency, improvement in inspection process and fraud prevention. They suggest incorporating protocols with both best practice and inherent consensus mechanisms of BC to preserve the integrity of the data or information stored in the system. Single points of failure cannot affect the availability of data as each participant stores a copy of the whole BC. Sharing information in real-time will help improve instant access to the information by stakeholders. SCM security will be enhanced by closely aligning both the physical and cyber worlds, by using a mixture of hardware technologies such as RFIDs, GPS in smart containers and verified digital identities, the consensus protocols of BC-based system can determine and approve genuine transactions for distribution to the network.

The complexity of SCM along with the security challenges are illustrated in [96]. Vulnerabilities in the SC is categorized into Piracy, Trojan Insertion, Overproduction, Recycled, Remarked, Cloned, Out of Spec / Defective, Forged Documentation and Side Channel Attack. Bose et al [96] proposed a tool BLIC, BC-based protocol, designed to overcome these vulnerabilities. However, BLIC suffers from similar scalability issues to BC technology. The mechanism for overcoming these issues in BLIC could potentially pose security threats to the network as parts of it need to be undertaken offline, then reintroduced to the network. This can potentially be intercepted by adversaries.

Li et al [97] propose Node Community Clustering as a means of making BC more efficient. Nodes are placed on the same chain based on their communication tightness threshold. The concept of only nodes on the same chain storing what is deemed as relevant data but not irrelevant data, as well as just synchronizing with data of the nodes that join the chain minimizes the need for more storage space in the multi-chain network. Thus reducing the pressure on the network and increasing data query speed, leading to improved efficiency. However, these benefits can only be achieved through community partitioning rather than random clustering. This framework put nodes below the threshold at a disadvantage as they may be ignored.

Kozma et al [12] recommended the use of the Arrowhead Framework, a cloud-based solution as a collaboration, combination and control tool within the SCM. Eligible users can share tracking and feedback information. It is based on a partner system, where users are trusted, authorized and subscribed. However, the information generated about each system is stored locally in each user's local cloud. The user, therefore, determines which information is shared with other users, limiting transparency and data quality as information can be manipulated by the user before sharing. Integrating DLT into the framework will eliminate this issues of transparency and data quality.

Bellini et al [4] focused on Distributed Trust and Reputational Management Systems (DTRMS) and Distributed Reputation Management Systems (DRMS). DTRMS/DRMS are systems designed to collect, process and share user ratings to influence decision making of potential new users/buyers. Their analysis showed an upward trend in the uptake of BC in DTRMS/DRMS and integration of DLT into SC. This is not surprising given the main features of BC: decentralization, immutability, auditability and fault tolerance. BC offers enhanced security, privacy and trustworthiness. Reviews are authentic, traceable and transparent, addressing issues such as bad mouthing and bad-collusion attacks. They also indicated that there is a shift towards more private and permissioned systems in a bid for data privacy, control and cost management. They suggested that BC as a service is emerging as an option to overcome some of the limitations and constraints around transitioning from one technological solution to another. This will enable organizations to subscribe to services they require for them to effectively meet their customer needs without heavily investing in infrastructure, technology or the skills required to maintain them. Hence, decision makers of SCM can focus their resources and efforts on where they can add the most value to the goods and services they provide to consumers.

Kuperberg [98] considered a BC-based identity management from an enterprise and ecosystem viewpoint. Identity and Access Management (IAM) is embedded in the fabric of most technological solutions including that of Industry 4.0 and SCM. Its strengths lie in its security aspects such as privacy/confidentiality and non-repudiation. The ecosystems of the IAM marketplace is changing due to a number of factors such as reduced consumer trust, the reluctance of service providers to share information with each other and with big players, regulations, commercial awareness of data value, privacy concerns and lack of secure storing and sharing mechanisms. [98] argues that BC-based IAM must fulfil the same requirements and standards as conventional IAM. Most BC developers do not factor these into their requirement specifications and as such do not meet IAM's mandatory requirements. Kuperberg [98] concluded that although BC-based IAM offers high potential for enterprise and ecosystems, more work need to be done to ensure both users and service providers take advantage of the security, ease of use, data protection, transparency and reduced costs benefits whilst assuring compliance.

A. Security Frameworks and Solutions

This section presents a detailed analysis of the recent state of the art DLT-based frameworks and solutions (see Tables I - II) designed to solve the challenges identified in the previous sections. Fig.5 illustrates the integration of BC and smart contracts into the SC and Fig.7 illustrates BC integration into a CPS in the SC. Fig.6 (a) and (b) shows BC architecture and Merkle Tree hashing transactions.

Hasan et al [99] proposed a generic Ethereum BC-based solution for the creation of Digital Twins (DT), an adaptable solution for any organization requiring digital models. They defined DT as digitalized virtual models of real physical objects. The framework benefits from in-built characteristics of BC, guaranteeing security, traceability, accessibility, data provenance and immutability of all transactions. Smart contracts are incorporated for governance and uses InterPlanetary

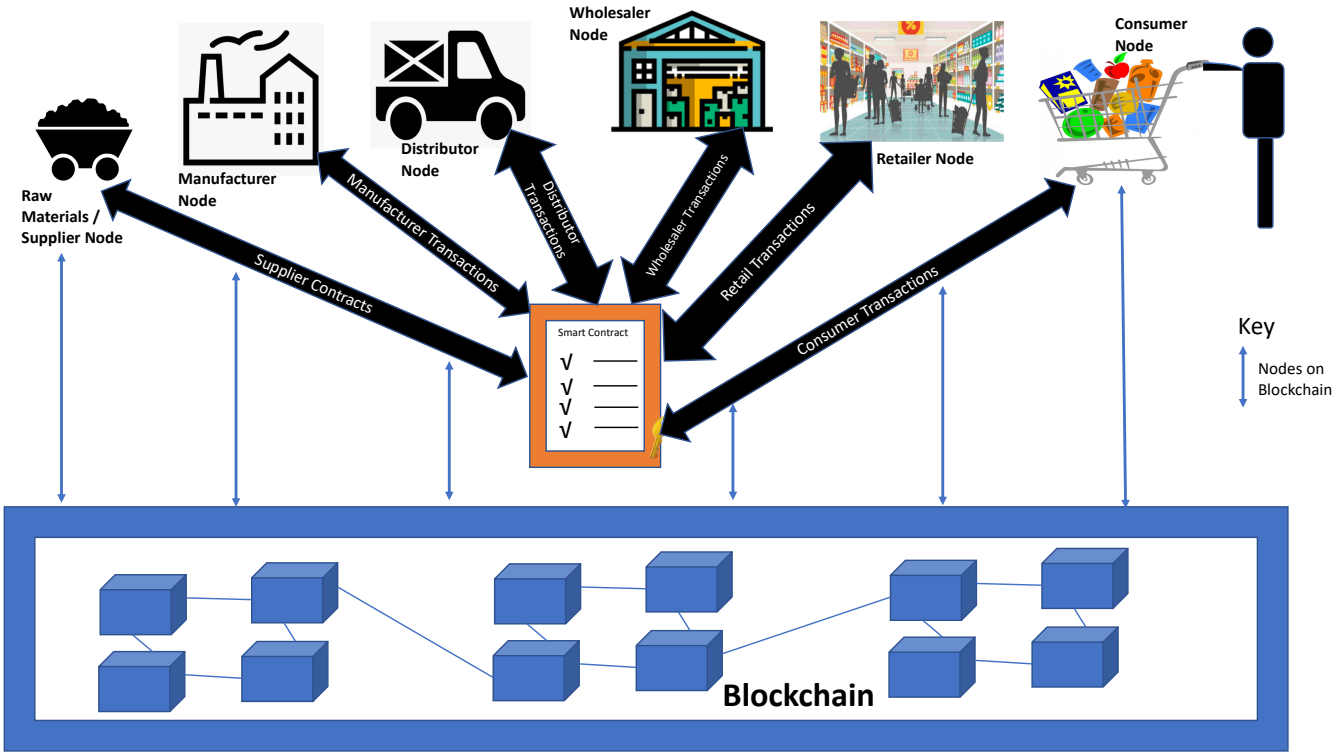
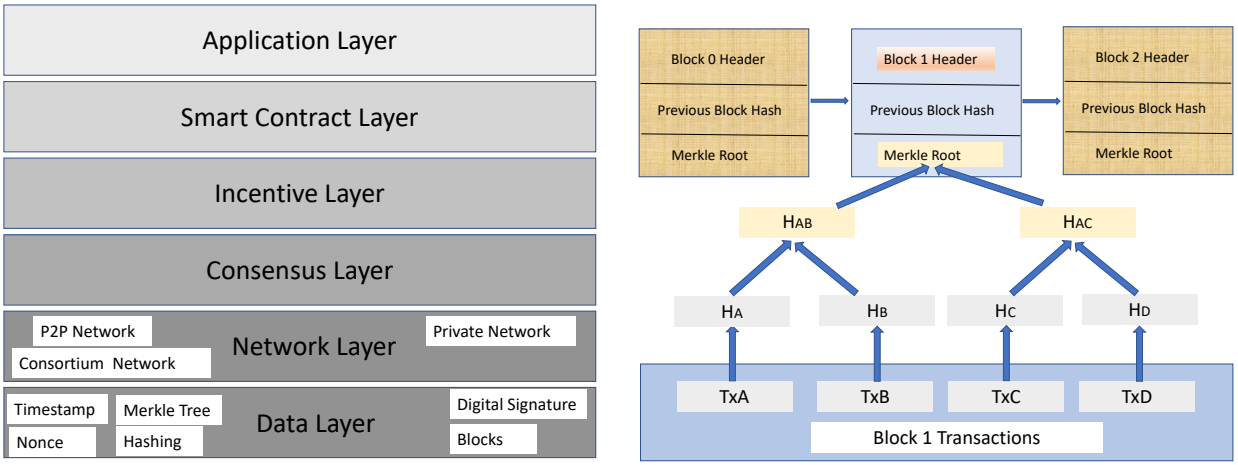


Fig. 6. Blockchain Integration into the Supply Chain



(a) Blockchain Architecture

(b) Blockchain Merkle Tree Transactions

Fig. 7. Blockchain Architecture

File System (IPFS) for information storage and sharing. The authors detailed the design, implementation and testing phases of their BC-based DT framework. They performed a security evaluation to ensure that trust and security requirements were met and cost analysis for feasibility of the solution. They concluded that the system was affordable, secure, reliable and maintainable.

A conceptual framework utilizing DLT and smart contracts as a trust-based incentive for the trading of food grains is suggested by Jaiswal et al [100]. Their framework incorporates smart contracts into four major areas of the food SCM: food grain supply, bidding, trading and utilization for food grain supply management. This is aimed at making product information such as type, quantity, price, origin and availability accessible across the SC network. It utilizes a PoA consensus for validation of transactions and nonce to avoid double-spending. It employs the Vickery auction method to ensure that participants bid honestly. User anonymity, immutability, transparency provides better trust and security in the network.

Lallas et al [78] proposed a generic end-to-end architecture solution based on IoT/Fog/Cloud Machine Conditioning Monitoring (MCM) system model incorporating BC, offering

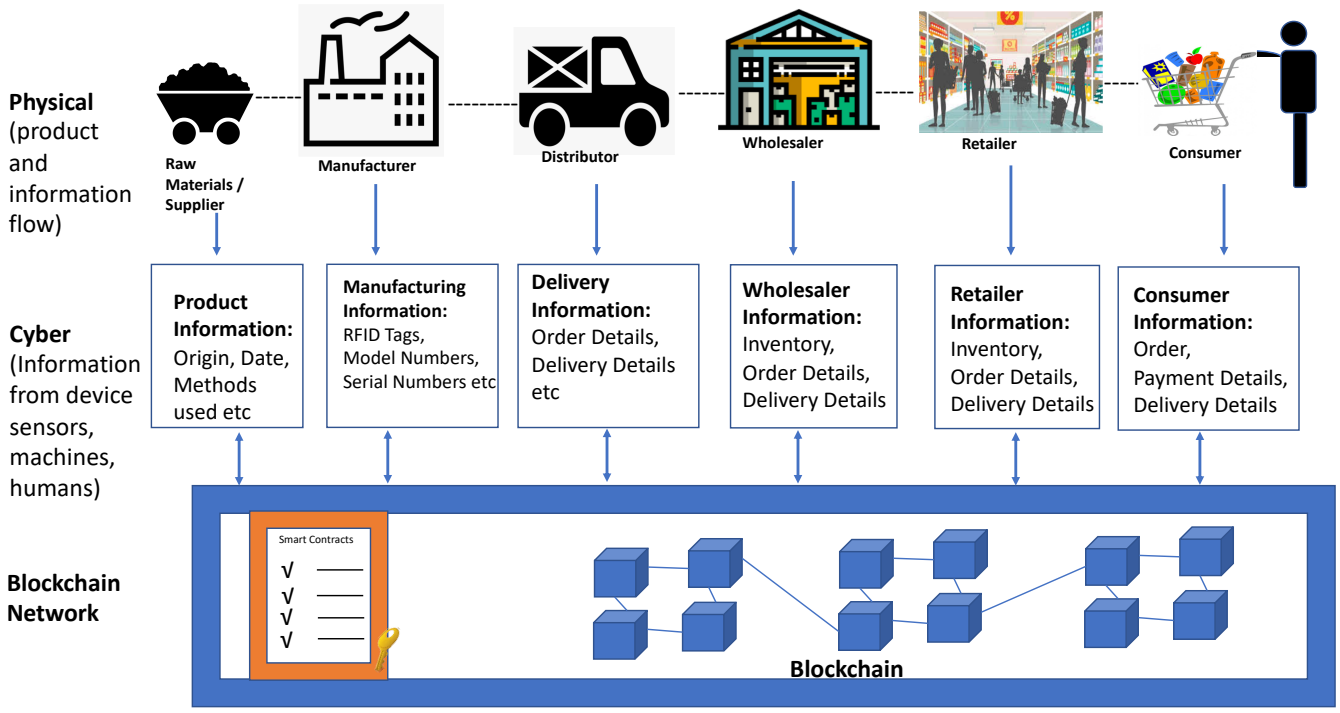


Fig. 8. Blockchain Cyber Physical Systems Integration into the Supply Chain

an efficient, faster and intelligent SC network. The architecture comprises of three well-defined layers, the IoT, Fog and Cloud, Decision layers and an integrated BC layer. Information from all the layers is stored on the BC, ensuring integrity, privacy, authenticity and non-repudiation of the data.

Zhang et al [101] created a cache layer to solve the risk of non-deterministic transactions. Their solution addresses the problem of read-write conflict and transaction order dependency on Fabric decentralized application (DApp) client.

Madhumidha et al [74] proposed a theoretical implementation of BC into a Provider-Consumer food traceability application in the agriculture SCM. This Ethereum-based solution utilizes tokens and smart contracts to integrate nodes within the SCM. It leverages the traceability and decentralization of BC to facilitate the continuous integration with IoT devices throughout the SC. This offers increased transparency, reduces error, minimizes product delay, eliminate unethical and illegal activities, resulting better management and increases trust levels.

Xu et al [34] proposed a simplified BC-based Maritime Cargo Management system. Their solution is designed on a permissioned BC as they argue that participants are known in the trade. Their system offers the benefits of BC features such as transparency, immutability, consensus protocols for validating participants and decentralized information storage and sharing. This leads to real-time information flow and an effective maritime SCM. Information accuracy in the system is guaranteed through enhanced vetting of participants, which is achieved through an integrated digital identity management system.

BLIC, BC-based solution by Bose at al [96], was introduced in Section II as a tool designed for overcoming security threats and vulnerabilities in the Integrated Circuits (IC) SC. At the heart of BLIC is a secure authenticating IC mechanism and a multi-level BFT and PoET algorithm built consensus protocols.

To reduce corruption and ensure food security, Shwetha et al [102] propose a BC-based Public Distribution Systems (PDS) integrated with IoT sensor module. This system will help track commodity movement in SC. The physical commodities are tagged with RFID (Radio Frequency Identification). All related information is stored in the BC and is widely available to all - public, government authorities and distributors alike. The transparent nature of decentralized transactions coupled with the tamper-proof quality of the data stored in the system will make it difficult for corruption within the PDS. However, it incorporates an access-controlled administrative console for authorities to use for secure auditing, trend analysis and reporting purposes. Although they argue that this is different from a centralized system, it may in reality be subject to the same levels of corruption that their system is designed to overcome.

Ramalingaiah et al [103] proposed a Bitcoin-based fund raising framework, the Laravel PHP Framework. Key features of Laravel Framework include built-in support for authentication, localization, models, views, sessions and routing mechanism. It also benefits from BC features such as decentralization, permissioned, consensus protocols, secure and trustworthy transactions. Sources of the funds raised become more transparent to participants.

Omar et al [104] suggest an Ethereum BC solution for smart phone counterfeiting and stolen devices, activities which cost industries billions of dollars. The solution is based on a decentralized identity management system in which devices are assigned unique and global digital identity, which are maintained throughout its lifecycle. It also relies on enabled traceability functions throughout the device's lifecycle. Transfer or change of ownership globally is validated and verified via the system. The authors chose BC due to its cryptographic identifiers, records immutability and provenance. Process automation is achieved through smart contracts. Devices are registered on a global registry from the point of production, maintained through the SC and transferred to the end-user. The registry holds the device's unique cryptographically generated digital identity, allocated by the manufacturer with their primary attributes, IMEI, model and serial numbers. Lost or stolen devices can be reported in real-time and the information distributed across the global network to alert users including operators, retailers and government agencies.

Li et al's [97]'s concept of using Node Community Clustering and BC-dividing strategy was introduced in Section II. It is designed to address storage problems and to ease pressure on CPS. The amount of cross-link communication data is reduced by the architecture of the system, creating a multi-chain structure which help reduce pressure on the system. Parallel processing in different clusters provides faster processing times, create more storage space and improve system performance. Node Communication Trust Relation model uses differences in the strength of communications between nodes to determine the community structure.

Ding et al [85] proposed a product traceability scheme based on the permissioned BC within a double-layer framework, designed to improve existing BC-based traceability systems. According to the authors, the weaknesses of existing systems include the lack of government regulatory agent participating in BC-based traceability systems, lack of adequate protection of private enterprise data and performance bottlenecks. Their proposed double-layer framework consists of a main layer, made up of a consortium BC and a sub-layer, made up of several private BCs. The stakeholders are government agencies, enterprises and consumers, enabling government agencies to participate in the consortium and for enterprises to protect their data on their private BCs. Interactions between the main and the sub layers are achieved through key nodes, via hash pointers (tamper-proof) and APIs (traceabillity). The consortium BC uses P2P consensus techniques whilst the private networks use star network techniques. Smart contracts are deployed in both the private networks and the consortiums. Government agencies nodes verify and audit information uploaded by the enterprise key node for new blocks. As the system is a permissioned system, the key nodes are assigned to known trusted entities, an important consideration for realizing product traceability with trusted and readily available product information. Auditing and monitoring by enterprises and regulators prevent the malicious writing of product traceability information. The use of private networks minimizes the chances of the data being tampered with and also improves the privacy of the data

Li et al [105] suggested a decentralized privacy-preserving timed execution solution for enabling users to schedule timed execution of transactions whilst protecting sensitive information, by employing an Ethereum-based system for scheduling the transactions. This system enables users sensitive information to be kept private and also allows users to be offline should they choose to do so during their scheduled transactions' execution, using on-chain functions in solidity to apply, schedule, execute and report transactions. A number of trusted users are chosen as trustees to oversee the execution. Their identities are also kept private. Inputs are only revealed to the network at the scheduled time. The system assumes that users are rational adversaries and not honest or semi-honest. Countermeasures are thus put in place to prevent misbehaviours such as advance identity disclosures, absent trustee and fake submission which could be exploited by adversaries. Users stand to lose their deposits if reported for a misbehaviour. They argued that their solution is cost effective due to low gas cost and saves time.

Xie et al [86] proposed a BC-based Trusted Trading Framework in E-commerce (ETTF), designed for achieving higher trading credibility. A collaborative peer BC protocol (PBP) which splits all peers into various committees, a trusted trading network (ETTN), used for storing all transactions. This prevents wastage of computational power. ETTP uses a peer validation selection protocol to randomly select committee members rather than standard consensus mechanisms such as PoW. It also has EPA, a propagation algorithm to reduce communication costs. Due to lack of openness and the ability for peers to tamper with the information, the authors incorporate an additional consensus mechanism, ECA which is deployed to all peers for enhanced security. They argue that their system performs better on throughput, latency and capacity due to the nearly linear network size in comparison with Bitcoin.

With a focus on tourism and hospitality, Bodkhe et al [90] proposed a BC-based framework, BloHosT (Block chain Enabled Smart Tourism and Hospitality Management) to foster direct and better engagement amongst stakeholders in the industry and to offer great experiences. The solution incorporates another framework, TeDL (Tourism enabled Deep Learning), which offers ratings to prospective tourists based on learned experience of former visitors. Transactions are achieved through smart contracts and consensus through Proof of Collaboration (PoC), Anonymity and privacy is guaranteed through the PoC based on Zero Knowledge Proofs (ZKP).

Epiphaniou et al [5] proposed Cydon, a data management platform for overcoming the limitations of traditional centralized data storage and processing solutions such as operational cost, auditability and security. The platform provides a secure environment for exchanging sensitive information. It consists of multi layered data management platform, layers of smart contracts, search and retrieve algorithms and a web portal for access. Transactions are executed by multiple smart contracts, verification is via Hyperledger Fabric in a private permissioned BC environment. Transactions are immutable, traceable and auditable once created and logged on the BC. The system offers differential data access and data flow levels for participants. This makes access to secure distributed data fast, eliminates single points of failure and ensures availability at

all times.

Ledwaba et al [106] modelled a DLT enabled smart microgrid for tackling energy poverty due to high cost, unstable grid and lack reliable energy supply in developing countries. The properties of DLTs: the immutability, distributed nature, cryptography, consensus, traceability, smart contracts and trust are leveraged on in the model for secure transactions. They designed a smart microgrid environment within which each household generates its own energy. The design, however, relies on mobile internet networks which are costly, unstable and unreliable. Ethereum BC was deployed on the Raspberry Pi 3 within IIoT network. The end result of the test showed that it was resource-intensive and very slow. They concluded that other DLTs such as DAG might be better suited for the model. They also identified other challenges that need to be overcome for the successful implementation of DLTs on IIoT devices and in the model.

Seitz et al [107] proposed the IIoT Bazaar, a marketplace for Fog Computing, AR and BC based IIoT applications. The design, location and function of the marketplace unite supply and demand. There are 8 main criteria which must be achieved for successful implementation: a transparent Open Platform which has the benefit of low barriers of entry to market for all parties, applications for installation on edge devices to facilitate end to end delivery, User-centric design, Independence achieved via decentralized system with no authority, payment models, on and offsite remote update management, flexibility and expandability and lastly, traceability. There is potential for human-machine interactions in the concept. The benefits of deploying BC are transparency and trust in a trustless environment, more participants and new marketplaces can be added to the network, smart contracts, immutability and traceability. The authors detailed their architecture, a case study and discussed the results which highlighted the limitations of the design and implementation of the system. They also made some recommendations for future development.

Abdellatif et al [108] designed a model based on matching in graph theory for optimal matching to meet the supply and demand of suppliers and users of the Edge Service Provider (ESP) for mobile BC. An optimal matching algorithm was proposed to improve efficiency in the system and to allocate the best possible resource to mobile users. This must be economically viable and profitable to the ESP.

Stodt et al [109] developed a methodology for integrating BC into maintenance processes incorporating all stakeholders to increase trust amongst them. The integration means maintenance processes can be automated and become more efficient. Transactions between stakeholders are carried out via smart contracts and stored on and distributed via the BC, a private permissioned, Hyperledger Fabric. The system provides a full immutable maintenance history for audit trail, better transparency, trusted information and enhance stakeholder experience. The streamlined system also ensure good quality maintenance and that no maintenance is overlooked.

Devi et al [110] proposed an architecture framework for integrating BC and IoT for Satellite monitoring. This is designed to improve security and data transparency. The BC nodes receive information from the IoT device sensors involved in the Satellite system. However, the framework has not been evaluated and its security level has not been designed.

Wang et al [94] proposed a BC-based product traceability system designed to facilitate information flow across the entire SC. The traceability process leverages decentralization, immutability and timestamped features of BC. To overcome the complexity of the SC, it splits users into nodes of suppliers, manufacturers, distributors, retailers, regulatory and consumers. Each node can have both supply and demand attributes. Multiple smart contract layers are built into the system for traceability of transactions in the SC. An event response mechanism is incorporated for identity and signature verification purposes to confirm the validity of transactions. Their security analysis confirmed that the system is fairly robust and that data is secure, tamper-proof and resistant to man-in-the-middle attacks.

Matzutt et al [111] argued that permanently storing information on BC puts systems at risk. They highlight that it is extremely difficult to preclude unintended content in BC networks. They investigated the design space of countermeasure heuristic techniques that stops the addition of harmful contents to the chain, easy to deploy and adaptable. They created a threshold rule which either allowed/denied the addition of content to the chain. Allowable content must be deemed computationally and financially viable. They argue that adding a financial cost as a deterrent will significantly reduce the amount of unintended content as users will only pay to upload content they intend to add. Content filtering and proofs of key authenticity are also requirements of the system. Countermeasures will ensure the information in the BC is accurate, relevant and minimize the risks to its users. However, they acknowledged that is unfeasible to totally eliminate insertion of unintended contents. Also, content inserters can quickly adapt to evade the detectors.

Sidorov et al [92] proposed a secure ultralightweight mutual authentication RFID protocol for integration in a BC enabled supply chain. Product traceability across the SC will be greatly improved due to enhanced visibility and transparency and thus prevents counterfeits. Permissioned BC is deployed for better security, privacy and scalability. The SC is split into nodes with different access levels similar to [94]. The system provides security to the SC against threats such as key disclosure, replay, main-in-the-middle, tracking and de-synchronization. It is also deemed to be efficient in storage, computational power and communication costs.

Dinh et al [47] introduced a benchmarking framework, BLOCKBENCH, for quantitative analysis of private BC with Turing-complete smart contracts as data processing platforms. The framework narrows down the BC design space into 4 distinct abstraction layers: the Application, Execution Engine, Data Model and Consensus. Ethereum, Parity and Hyperledger BC were assessed against the framework. Their results highlighted design tradeoffs that had to be made and performance bottlenecks in the system. They concluded that BC need further development for effective wider use.

Demir et al [72] proposed a BC-based system to be applied in disaster recovery. Disasters will trigger the activation of the system which all stakeholders will be required to register

for. The stakeholders include the victim(s), insurers, service providers, legal representatives, emergency services, repair / restoration service providers and government agencies depending on the nature of the disaster. To effectively manage the situation and restore services in an orderly manner, information gathered on the disaster, insurance assessments, schedules for restoring services, legal disputes and any other related activities can be logged on the BC and made available to all stakeholders. The distributed records will be immutable, the process will be transparent, and information will be available in real-time. This will assist in the situation being resolved much faster as bottlenecks normally due to waiting on others to provide information in disaster situations will be removed. the BC solution will also help prevent fraudulent claims.

Yu et al [2] introduced a virtualization for DLT (vDLT) framework to solve the challenges of DLT such as scalability. It is presented as a tool for evolution and simplification of system management and configuration. The system consist of a combination of physical and virtual resources. The two aspects are separated by a hypervisor-based virtual layer. A combination of virtual machines, links and nodes are deployed. A vDLT function (vDLTF) is defined as a functional block within a network infrastructure that clearly established external interfaces and functional behaviour. A vDLTF may be deployed across multiple VMs or containers. Financial incentives are built into the system to encourage contribution from nodes.

Onishi [31] proposed an integration of BC into VANET (Vehicle Ad-hoc Network), a vehicle-to-vehicle (V2V) communication network to address its security risks. It is anticipated that VANET will play a crucial part in the implementation of vehicle crash warning applications, playing a major part in road safety. VANET can, for example, warn drivers about vehicles in their blind spot. V2V communications have short latency and do not require infrastructure. Leveraging of these characteristics to incorporate crash warning applications in V2V communications will enable vehicles to share information such as their location, speed, the direction of travel and distance with nearby vehicles, thus issuing advance warnings about potential crashes. However, V2V communication needs to access centralized servers in order to exchange security keys and certificates (issued by the Certification Authority). The certificates will require frequent multiple updates on an ongoing basis to prevent malicious attacks. A major security challenge for VANET is the inability to detect malicious nodes in the network. It is also susceptible to security weaknesses in wireless networks such as jamming, eavesdropping and tampering. The integration of BC will allow the VANET network to store and transparently share information including dates, locations etc securely to help drivers in making safety decisions. BC can also improve product traceability in the automotive industry. In addition, this will be beneficial to insurers, government agencies, emergency services and road assistant service providers. However, infrastructure will be required for the synchronization of individual ledgers.

Mylrea et al [22] suggested a BC-based Software, Patch and Configuration Management Configuration System for the automation of the NERC CIP compliance process. All information relating to critical cyber assets will be securely stored on the permissioned BC. The distributed and decentralized features of BC will help minimize the administrative effort required for compliance leading to cost reduction and efficiency. Immutability of records and transparency leads to improved auditability, monitoring and compliance of the system. Visibility and accessibility are greatly enhanced throughout the SC. The software development lifecycle will be greatly enhanced as global teams will be able to better coordinate their work, schedules and processes of integrating various modules through a secure, verifiable, transparent and accountable platform.

Al-Zaben et al [59] presents BC-based Personally Identifiable Information Management System (BcPIIMS) designed for PII management. The off-chain BC design utilizes both local and distributed ledgers for the preservation of a trust-based PII lifecycle. This is achieved through the separation of PII (stored on a local database) and non-PII with hash of PII (stored in BC). The concept works on the assumption that PII on the local system can be deleted at anytime, thus BcPIIMS is GDPR compliant, secure and transparent. The BC nodes are divided into user, controller and processor. The consensus mechanism employed is the Round Robin scheduling system which requires participating nodes to generate blocks in rotation for validation. Transactions including agreements and consent are carried out via smart contracts. The controller is responsible for separating the data into PII (stored locally) and non-PII and for hashing the PII before its addition to the BC. Data authenticity is ensured as the system gives users greater access and visibility of their PII as they can track it through the hash value provided by the controller. Users right to amend inaccurate data about them and also to erasure (Right to be forgotten) can be achieved by amending or deleting PII on local drives. Security is afforded through consensus between participating nodes. Transactions once created are immutable. Changes and updates are through a new consensus from all parties. Consensus roles must be intelligible, easily accessible and supported by all parties for transparency and verification purposes. Users can be assured that their PII is secure as they can trace the entire PII lifecycle via the system.

Karamačoski et al [38] proposed an implementation of DSS (Distributed Storage System) and BC for the purposes of a Distributed Communication Channel (DCC) system. As a communication channel the DCC is designed for exchanging information through multiple physical channels. They propose applying the procedures of data shredding made by the DSS coding matrix in a communication scenario, implementing DSS coding schemes in a distributed communication system. DSS matrix is used for data generation and encoding. The encoded information is distributed for reliability. Receiving nodes then reconstruct the original message. Reliability is further increased by the addition of redundant data which helps if there is interference in the communication. The integrated system will be benefited from automation through smart contracts, enhanced security and privacy, distributed networks and the immutability of records, an essential aspect for audit trial of communications. There are two security levels The first one is the information-theoretic secrecy provided by the DSS encoding process and the second, the implemented

encryption in the pre-encoding or post-encoding stage. The BC provides a secure public database for encoding matrix and encryption key exchange.

Perez et al [39] proposed a mechanism for a BC-based modification to SHA256 security protocol through smart contract to secure online transaction procedures. The mechanism leverages security, privacy, trust and transparency features of BC for authentication and non-repudiation. [39] also suggest integrating BC and off-chain database to develop a personal data control management platform which focuses on confidentiality and data integration. They argue that designing algorithms with low computational power will be more efficient and operationally cheaper than on-chain solutions. Off-chain transactions will occur outside the BC but will later be transferred to the BC. The BC architecture must be lightweight, reliable, efficient and affordable. The platform will be permissioned requiring users to register. However, it is worth noting that off-chain storage will require management effort. There may also be potential interoperability and scalability issues. In addition, there may not be any cost savings due to the costs of off-chain storage.

The BIDAS (a BC and IoT delivery assurance on supply chain) framework proposed by Demir et al [87] was introduced under Section II. BC is employed to optimize information flow in parcel delivery operations of the SC. A number of initiatives already exist in this area leveraging various technologies to improve customer and other stakeholder experience. However, there are still issues with effective information flow, which may lead ultimately to loss of parcels and errors in the delivery of wrong parcels or parcels to wrong addresses. The ability to fully automate the parcel delivery processes by integrating BC with IoT (device sensors) will be extremely beneficial to all stakeholders, ensuring parcels are delivered on time anytime of the day, all year round. BIDAS provides a decentralized framework, incorporating all stakeholders, improving accessibility and removing the need for centralized authorities in the SC. BC produces permanent, immutable records which the framework relies on to apply the principles of the Agency theory to resolve the issues with loss of information, thus increasing transparency and trust. Smart contracts are used for order, sales and payment transactions, which are recorded on the system at each stage of the parcel delivery SC. BIDAS incorporates existing traditional delivery data entities, for example, Order, Order Item, Delivery Item and Receiver, making it easy to adopt. However, like most BC-based systems discussed, there are concerns around data privacy due to total transparency BC offers. This can be overcome by implementing an identity and consent system, which restricts the amount of PII information shared with third parties. A JSON-LD lightweight linked data standard, compliant with RESTful services and unstructured databases, will hold all sensitive information such as delivery addresses, keeping them confidential. One of the main benefits of the framework is that humans sign off the successful delivery of the order, removing ambiguity associated with autonomous vehicles and drones. Other limitations are similar to that of most BC-based systems such costs, tradeoffs between privacy and transparency as well as availability.

Zou et al [89] proposed a practical BC-based accountability infrastructure for crowdsourcing and online service industry. This leverages the immutability feature of BC and is built on trust models. They argue that there are three accountability infrastructure principles aimed at maintaining a source of truth for service transactions (PR1), addressing implementation practicality issues (PR2) and enabling the platform's transition to a decentralized architecture (PR3). Their suggested consensus protocol, Proof-of-Trust (PoT) for crowdsourcing platforms, must overcome the issues associated with current ones such as scalability, performance, resourcing and security shortfalls. PoT is a hybrid architecture, the trust element, which combines with incentive measures to tolerate Byzantine faults and overcome unfaithful behaviours linked to open public networks. The BC integrated infrastructure will give the online service industry distributed governance and accountability. There are four different stages involved in the PoT consensus protocol to ensure that there is separation of roles and consistency in the validation process leading to fairness and security. The authors concluded that PoT provides agreement, validity, performance, scalability, fairness and security. However, they acknowledged that PoT does not provide liveness guarantee and also in some cases, there may be deadlocks in PoT due to the involvement of the even number of decision-makers.

Shen et al [84] presents a BC-based business model of data sharing in multiple clouds. It is a consortium BC in which known and identified selected users are authorized, enhancing data privacy and security. It uses Shapley value for fair distribution of revenue amongst users and leverages the tamper-proof and immutability features of BC for trust and transparency. In the proposed business model, all stakeholders (data owners, miners and third party) are incentivised to willingly share factual information and to preserve its integrity, increasing trust in the system. Transactions are undertaken via smart contracts. The authors conclude that their system could encourage collaborative data sharing in multiple clouds.

Xu et al [14] present an integrated Ethereum BC-based information service solution, using smart contracts and Node.js technology for fulfilling user requirements such as ordering, trading, information tracking and queries. The system comprises of a consortium BC made up of four-layered physical architecture, including a service layer, application layer, contract layer and on-chain storage and relational database storage, which enhances data base query efficiency of the system. Digital signatures are used for the authentication, verification and validity of signature information and smart contracts based on solidity programming are deployed to help with transaction management. The system has four management modules: system management for managing registrations, changes and information publication, tracing module for tracking of information and goods, process management for managing basic SC functions such as orders, receipts and deliveries and reputation management module for evaluating reputation. All participants are pre-selected following an application to join the consortium and approval by the management organization. Each enterprise operates an Ethereum node and are able to generate new transactional data for distribution in the P2P network. The consensus network is made up of producers,

logistics providers and distributors. Consumers can access the system when querying operations but do not form part of the consensus network. The system is designed to enhance information sharing in the SC, improve overall efficiency and to ensure that information shared is verified and authentic.

V. Main Findings

The complexity of SC together with its related infrastructure results in the production of copious amounts of data being generated every second of the day throughout the entire year. There is a need to ensure that data flows transparently and seamlessly through the chain and more importantly, to assure the CIA of the data. By its nature, the SC is full of trustless entities [11], [72], [100], [74], [109]. The advent of Industry 4.O adds an even more complicated layer of security challenges for SCM [80]. Data is generated, processed, stored and distributed across platforms, applications and devices, each of which comes with their own security risks. There is an apparent lack of standardization, regulations and collaboration among entities [36], [7], [61], [62], [31]. DLT offers huge capability and opportunities for overcoming most of the challenges identified in this survey Tables I and II summarize proposed DLT integrated frameworks and solutions, designed to overcome current challenges in SCSM. They highlight the types of DLT that the frameworks or solutions will be suitable for and specific DLT which they are based on. Evidence from available research show that a lot of the solutions and frameworks designed for integrating DLT such as BC and Ethereum into various applications in across industries are still in their infancy. Frameworks and solutions addressing SC security and interoperability issues such as those proposed by Xu et al [34] and Onishi [31] are more likely to be ahead of the others. Although a huge amount of investment is going into the development of DLT, stakeholders air on caution as DLT presents their own challenges. There is a need for a holistic transparent end-to-end security management which provides all stakeholders with visibility. If there is a joint effort among all stakeholders to develop the right solution, it will have a higher chance of successful implementation. A greater understanding of types of DLT platforms, which consensus algorithm to use, the best rules for smart contracts will help stakeholders in choosing the best solution they require [29].

Although Bitcoin BC has been commercially available since 2009 and generally widely accepted in the financial industry, its application, as well as the applications of other BC and DLT in IoI and IIoT, are largely limited to research and prototypes. The huge amount of research coupled with well documented security concerns and breaches make industries cautious in adopting and implementing BC. A good evaluation is required in deciding which BC technology to use as there are so many variants of the technology [61], [40], [42], [93]. Given that DLTs themselves do not, as a rule, integrate with each other, users may have to access several applications in order to use different services. This could result in a user having several private keys in their wallet, which could put them at serious risk if they are subject to key leakage.

Smart contracts offer huge potential for SCM and make it easy to automate processes and contract transactions. Copies of the transactions are distributed to all parties. This removes the bottlenecks of central and controlling authorities as well as intermediaries.

VI. Future Research Directions

DLT has emerged as strong and impactful technology to the SC. DLT such as BC and Ethereum offers dynamic solutions across industries and have great potential for integration seamlessly into IoT, ML, RFID, augmented reality and all other aspects of Industry 4.0. Although DLT offers substantial benefits, it faces several challenges in its development and implementations. Future researchers can explore leveraging DLT to address the security challenges of the SCM adequately. Research into improving the confidentiality of data stored and distributed in DLT networks whilst maintaining transparency, tamper-proof and immutable benefits will help improve privacy of the participants and protect them from exploitation by malicious actors. Improving traceability, visibility and auditability in the complex global SC will enable better tracking products and information throughout their entire lifecycle, thus helping in the fight against theft, fraud, conterfeit goods and loss of cargo.

Further work is needed on the different ways that DLT can enhance mission assurance to existing SCM systems. Most industrial systems are designed for organizational and operational benefits, not necessarily with security in mind. Yet with more transactions being done online, the SC is evermore susceptible to attacks such as DDoS, information leakage, reputational damage due to security breaches and fines by regulatory authorities. Researchers can help organizations develop and implement secure DLT-based infrastructure, to minimize or eliminate such threats. Finally, specific interventions could enhance understanding on the adoption barriers for stakeholders and the measurable impact DLT can have on operations and activities. Organizations will be able to undertake cost-benefit analysis of DLT-based solutions to their operations and SC, but equally, be able to grow and develop by exploring new business opportunities that such solutions may present to them such as understanding their markets and competition better.

VII. Conclusion

The SC itself is a distributed complex network across the globe. Having distributed integrated technical solutions which spans the entire chain from the production and supply of raw materials through to the delivery of the end product or service to the end-user seems like the natural solution to most of its problems. Bottlenecks and challenges of SCM which stops and/or interferes with the flow of information and products through the global SC have been identified and discussed in detail. SC optimization can be achieved by the implementation of DLT-based solutions which offers process improvement through streamlining and efficiency by removing intermediaries and the need for central controlling authorities, increasing trust in the SC through transparency and increased visibility and enhanced data flow across the SC. Administrative burden in SCM can be greatly reduced and Information sharing will be significantly improved resulting in

TABLE I
FRAMEWORKS AND SOLUTIONS

Author	Framework / Solutions	DLT Platform Used	Type of DLT	Future Development
Hasan et al [99]	A BC-Based Approach for the Creation of Digital Twins	Ethereum BC	Permissioned Permissionless	Implement a complete solution composed of private BC nodes Explore using Hyperledger Fabric and Hyperledger Besu Development of frontend DApp
Jaiswal et al [100]	A Conceptual Framework for Trustworthy and Incentivized Trading of Food Grains using Distributed Ledger and Smart Contracts	Ethereum BC	Permissionless	Incorporate government policies, demand prediction, guidelines to farmers etc in the BC Improve scalability of the framework Explore capabilities of IoT integrated BC further
Lallas et al [78]	A generic framework for a Peer to Peer BC based Fog Architecture in Industrial Automation	Ethereum BC	Permissioned Permissionless	Apply resource allocation policies to the fog nodes on a pharmaceutical manufacturing case study
Zhang et al [101]	A Solution for Risk of Non-deterministic Transactions in Hyperledger Fabric	Hyperledger Fabric	Permissioned	Evaluate the performance of the cache solution on various environment Build Fabric network based on distributed deployment Replace consensus with Kafka or other algorithms Implement the global cache layer
Madumidha et al [74]	A Theoretical Implementation: Agriculture-Food Supply Chain Management using BC Technology	Ethereum BC	Permissionless	Not stated in the paper
Xu et al [34]	Binding the Physical and Cyber Worlds: A BC Approach for Cargo Supply Chain Security Enhancement	BC	Permissioned	Consider integrating existing cargo security improvement hardware such as smart GPS/container
Bose et al [96]	BLIC: A BC Protocol for Manufacturing and Supply Chain Management of ICs	BC	Permissioned	Deploy variants of zero proofs and encryption schemes Use alternative transaction techniques Add signature schemes and access control
Shwetha et al [102]	BC - Bringing Accountability in the Public Distribution System	Ethereum BC	Permissioned Permissionless	Not stated in the paper
Ramalingaiah et al [103]	Study of BC with Bitcoin based Fund Raise Use case using Laravel Framework	Bitcoin BC	Permissioned	Implement a complete solution composed of private BC nodes Explore using Hyperledger Fabric and Hyperledger Besu Development of frontend DApp
Omar et al [104]	Smart Phone Anti-counterfeiting System Using a Decentralized Identity Management Framework	Ethereum BC	Permissioned Permissionless	Incorporate the W3C credentials into the framework
Li et al [97]	BC Dividing Based on Node Community Clustering in Intelligent Manufacturing CPS	BC	Permissioned	Not stated in the paper
Ding et al [85]	Permissioned Blockchain-Based Double-Layer Framework for Product Traceability System	BC	Permissioned	Apply the concept to other BC applications
Li et al [105]	Decentralized Privacy-preserving Timed Execution in BC-based Smart Contract Platforms	Ethereum BC	Permissioned	Not stated in the paper
Xie et al [86]	ETTF: A Trusted Trading Framework Using BC in E-commerce	BC	Permissioned	More applications of BC integrated solutions in E-commerce Improve consensus mechanisms and algorithms to achieve better security and efficiency
Bodkhe et al [90]	BloHosT: BC Enabled Smart Tourism and Hospitality Management	BC	Permissioned	Implement a complete BC-based infrastructure for tourism and hospitality, which provides end-to-end security to all stakeholders
Matzutt et al [111]	Thwarting Unwanted BC Content Insertion	BC	Permissioned	Develop countermeasures further to fully compliment each other
Devi et al [110]	Integration of BC and IoT in Satellite Monitoring Process	BC	Permissioned	The same system can be enhanced by applying various consensus algorithms for the same to predict the performance parameters
Demir et al [87]	BC and IoT for Delivery Assurance on Supply Chain (BIDAS)	BC	Permissioned	Implementation of the BIDAS guided use case with a Hyperledger BC platform
Zou et al [89]	A Proof-of-Trust Consensus Protocol for Enhancing Accountability in Crowdsourcing Services	BC	Permissioned	Add a mechanism to work around the rare situation of consensus deadlock
Shen et al [84]	BC-based Incentives for Secure and Collaborative Data Sharing in Multiple Clouds	BC	Permissioned	Not stated in the paper

TABLE II
FRAMEWORKS AND SOLUTIONS

Author	Framework / Solutions	DLT Platform Used	Type of DLT	Future Development
Epiphaniou et al [5]	Electronic Regulation of Data Sharing and Processing Using Smart Ledger Technologies for Supply-Chain Security: Cydon	Hyperledger Fabric	Permissioned	Further performance testing and refinement of the algorithm and its associated distributed applications for different BC Ability to store Cydon token permissions directly in the BC network for audits
Ledwaba et al [106]	Developing a Secure, Smart Microgrid Energy Market using Distributed Ledger Technologies	Ethereum BC	Permissioned	Detailed investigation into the full capabilities and limitations of running DLTs on IIoT edge processing devices Improve efficiencies of Proof of Work or Proof of Stake consensus mechanisms Reduction of the implementation requirements needed to improve compatible with IIoT SoC architectures
Seitz et al [107]	Fog Computing as Enabler for BC-Based IIoT App Marketplaces	Ethereum BC	Permissioned Permissionless	Extend to M2M collaborations by using Smart Contracts for autonomous machines Evaluate the findings of the studies and the acceptance of the system Combine the IIoT Bazaar with the idea of Seamless Computing
Abdellatif et al [108]	Graph-Based Computing Resource Allocation for Mobile BC	BC	Permissioned Permissionless	Not stated in the paper
Stodt et al [109]	Formal Description of Use Cases for Industry 4.0 Maintenance Processes Using BC Technology	Hyperledger Fabric	Permissioned	Enhanced automation of the maintenance processes to allow machines to trigger smart contracts A wider usage of sensors would allow for a greater integration of BC and machine Utilize ML as a predictive model to initiate maintenance prior to an occurring fault
Wang et al [94]	Smart Contract-Based Product Traceability System in the Supply Chain Scenario	Ethereum BC	Permissioned	Realize formatted upload of data by using IoT technology, reduce the possibility of manual input errors Through QR code technology, promote the process of product source querying, improve consumer consumption experience, and simplify the consumer operation process
Sidorov et al [92]	Ultralightweight Mutual Authentication RFID Protocol for BC Enabled Supply Chains	BC	Permissioned	Not stated in paper
Al-Zaben et al [59]	General Data Protection Regulation Complied BC Architecture for Personally Identifiable Information Management	BC	Permissioned	Future research direction is to develop a fully-fledged PII tracking and managing system for a secure PII flow
Karamačoski et al [38]	BC for Reliable and Secure Distributed Communication Channel	BC	Permissioned	Not Stated in the paper
Dinh et al [47]	Untangling BC: A Data Processing View of BC Systems	Ethereum, Parity, Hyperledger Fabric	Permissioned Permissionless	Develop countermeasures further to fully compliment each other Sharding and decoupling the layers for optimization Embracing new hardware primitives Supporting declarative language
Demir et al [72]	Utility BC for Transparent Disaster Recovery	BC	Permissioned	Not stated in paper
Yu et al [2]	Virtualization for Distributed Ledger Technology (vDLT)	BC	Permissioned	Future work is in progress to implement the proposed vDLT in different applications, including supply chain, smart cities, etc
Onishi [31]	A Survey: Engineering Challenges to Implement VANET Security	BC, DLT	Permissioned	Future work to practically explore the integration of BC and overcoming their security challenges
Mylrea et al [22]	BC for Supply Chain Cybersecurity, Optimization and Compliance	BC	Permissioned	Implement and evaluate the integration of BC into the critical electricity infrastructure and assess its cyber security resilience
Perez et al [39]	Modified SHA256 for Securing Online Transactions based on BC Mechanism	BC	Permissioned	Add Agent-based smart contracts Identify the performance in terms of payloads and other factors in consideration to validate the speed and security
Xu et al [14]	Manufacturing Industry SCM Based on the Ethereum Blockchain	Ethereum BC	Permissioned	Ethereum compatible consensus mechanisms to improve the system performance Propose a reasonable and applicable evaluation method or algorithm for different suppliers in the SC Strengthen the links with the Internet of Things by developing communication mechanisms for direct communication between IoT sensors and BC

huge savings in costs. DLT has inbuilt security features such as provenance, immutability, consensus protocols and smart contracts which offers a higher degree of cyber resilience to systems. DLT systems are more reliable and less prone to data loss due to their distributed, decentralized and the tamper-proof nature of records stored. As a rule, DLT affords two of the three aspects of CIA: data integrity and availability. Future improvements will lead to improved confidentiality. However, these same features which make DLT solutions attractive to the SC, as well as other areas, are prone to exploitation by adversaries. Identities of individuals including sensitive information, their transaction histories and other activities can be traced through logs on the DLT network. This could lead to identity theft, private key leakages, theft of IP, copyrights and trade secrets. If the breach occurs on a critical infrastructure, it could lead to espionage and trade wars. Challenges such as technical complexity, interoperability, standardization, legal aspects, infrastructure and architecture present barriers to the full integration of DLT into the SC. [31]. However, several DLT-based frameworks and solutions are being developed, enhanced and improved to provide the much needed solutions to these well documented problems. Future research could focus on amalgamating concepts, frameworks and solutions, bringing together knowledge, experience and skills of researchers and practitioners in the field to help address the issues.

REFERENCES

[1] M. J. M. Chowdhury, M. S. Ferdous, K. Biswas, N. Chowdhury, A. S. M. Kayes, M. Alazab, and P. Watters, "A comparative analysis of distributed ledger technology platforms," *IEEE Access*, vol. 7, pp. 167 930–167 943, 2019.

[2] F. R. Yu, J. Liu, Y. He, P. Si, and Y. Zhang, "Virtualization for distributed ledger technology (vdlt)," *IEEE Access*, vol. 6, pp. 25 019–25 028, 2018.

[3] A. Shahaab, B. Lidgey, C. Hewage, and I. Khan, "Applicability and appropriateness of distributed ledgers consensus protocols in public and private sectors: A systematic review," *IEEE Access*, vol. 7, pp. 43 622–43 636, 2019.

[4] E. Bellini, Y. Iraqi, and E. Damiani, "Blockchain-based distributed trust and reputation management systems: A survey," *IEEE Access*, vol. 8, pp. 21 127–21 151, 2020.

[5] G. Epiphaniou, P. Pillai, M. Bottarelli, H. Al-Khateeb, M. Hammoudesh, and C. Maple, "Electronic regulation of data sharing and processing using smart ledger technologies for supply-chain security," *IEEE Transactions on Engineering Management*, pp. 1–15, 2020.

[6] V. A. Siris, P. Nikander, S. Voulgaris, N. Fotiou, D. Lagutin, and G. C. Polyzos, "Interledger approaches," *IEEE Access*, vol. 7, pp. 89 948–89 966, 2019.

[7] T. Sharma, S. Satija, and B. Bhushan, "Unifying blockchian and iot:security requirements, challenges, applications and future trends," in *ICCCIS*, Oct 2019, pp. 341–346.

[8] S. Soni and B. Bhushan, "A comprehensive survey on blockchain: Working, security analysis, privacy threats and potential applications," in *International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, vol. 1, July 2019, pp. 922–926.

[9] P. Fraga-Lamas and T. M. Fernández-Caramés, "A review on blockchain technologies for an advanced and cyber-resilient automotive industry," *IEEE Access*, vol. 7, pp. 17 578–17 598, 2019.

[10] F. M. Benčić and I. Podnar Žarko, "Distributed ledger technology: Blockchain compared to directed acyclic graph," in *IEEE ICDCS*, 2018, pp. 1569–1570.

[11] S. Yousuf and D. Svetinovic, "Blockchain technology in supply chain management: Preliminary study," in *IOTSMS*, Oct 2019, pp. 537–538.

[12] D. Kozma, P. Varga, and G. Soós, "Supporting digital production, product lifecycle and supply chain management in industry 4.0 by the arrowhead framework – a survey," in *2019 IEEE 17th International Conference on Industrial Informatics (INDIN)*, vol. 1, July 2019, pp. 126–131.

[13] M. M. H. ONIK, C. KIM, and J. YANG, "Personal data privacy challenges of the fourth industrial revolution," in *ICACT*, Feb 2019, pp. 635–638.

[14] Z. Xu, Y. Liu, J. Zhang, Z. Song, J. Li, and J. Zhou, "Manufacturing industry supply chain management based on the ethereum blockchain," in *IEEE IUCC and DSCI and SmartCNS*, Oct 2019, pp. 592–596.

[15] M. Rahouti, K. Xiong, and N. Ghani, "Bitcoin concepts, threats, and machine-learning security solutions," *IEEE Access*, vol. 6, pp. 67 189–67 205, 2018.

[16] G. C. Stevens.

[17] O. O. Ojo, S. Shah, A. Coutroubis, M. T. Jiménez, and Y. Munoz Ocana, "Potential impact of industry 4.0 in sustainable food supply chain environment," in *IEEE ICTMOD*, Nov 2018, pp. 172–177.

[18] H. Zhang, T. Nakamura, and K. Sakurai, "Security and trust issues on digital supply chain," in *IEEE (DASC/PiCom/CBDCom/CyberSciTech)*, Aug 2019, pp. 338–343.

[19] B. A. Sabbagh and S. Kowalski, "A socio-technical framework for threat modeling a software supply chain," *IEEE Security Privacy*, vol. 13, no. 4, pp. 30–39, July 2015.

[20] A. Nalavade, D. Rawat, and H. Kanakia, "Blockchain technology: Most secure database," in *ICICCS*, June 2018, pp. 1356–1362.

[21] Y. Fu and J. Zhu, "Big production enterprise supply chain endogenous risk management based on blockchain," *IEEE Access*, vol. 7, pp. 15 310–15 319, 2019.

[22] M. Mylrea and S. N. G. Gourisetti, "Blockchain for supply chain cybersecurity, optimization and compliance," in *RWS*, 2018, pp. 70–76.

[23] N. Kshetri and E. Loukoianova, "Blockchain adoption in supply chain networks in asia," *IT Professional*, vol. 21, no. 1, pp. 11–15, 2019.

[24] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," 2007.

[25] B. Kitchenham, P. O. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering–a systematic literature review," *Information and software technology*, vol. 51, no. 1, pp. 7–15, 2009.

[26] S. Keele *et al.*, "Guidelines for performing systematic literature reviews in software engineering," Tech. Rep. 1, 2007.

[27] S. Snyder, "Literature review as a research methodology: An overview and guidelines," *Journal of Business Research*, vol. 104, pp. 333–339, 2019.

[28] I. Islam, K. M. Munim, S. J. Oishwee, A. K. M. N. Islam, and M. N. Islam, "A critical review of concepts, benefits, and pitfalls of blockchain technology using concept map," *IEEE Access*, vol. 8, pp. 68 333–68 341, 2020.

[29] C. Maple and J. Jackson, *Selecting Effective Blockchain Solutions: Euro-Par 2018 International Workshops, Turin, Italy, August 27-28, 2018, Revised Selected Papers*, Jan 2019, pp. 392–403.

[30] I. Acharjamayum, R. Patgiri, and D. Devi, "Blockchain: A tale of peer to peer security," in *IEEE SSCI*, 2018, pp. 609–617.

[31] H. Onishi, "A survey: Engineering challenges to implement vanet security," in *IEEE ICVES*, Sep. 2018, pp. 1–6.

[32] M. Conti, E. Sandeep Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Communications Surveys Tutorials*, vol. 20, no. 4, pp. 3416–3452, Fourthquarter 2018.

[33] S. Shalini and H. Santhi, "A survey on various attacks in bitcoin and cryptocurrency," in *ICCSP*, April 2019, pp. 0220–0224.

[34] L. Xu, L. Chen, Z. Gao, Y. Chang, E. Iakovou, and W. Shi, "Binding the physical and cyber worlds: A blockchain approach for cargo supply chain security enhancement," in *IEEE International Symposium on Technologies for Homeland Security (HST)*, 2018, pp. 1–5.

[35] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Communications Surveys Tutorials*, vol. 21, no. 1, pp. 858–880, Firstquarter 2019.

[36] Y. Hou, J. Such, and A. Rashid, "Understanding security requirements for industrial control system supply chains," in *IEEE/ACM SEsCPS*, May 2019, pp. 50–53.

[37] B. Alotaibi, "Utilizing blockchain to overcome cyber security concerns in the internet of things: A review," *IEEE Sensors Journal*, vol. 19, no. 23, pp. 10 953–10 971, Dec 2019.

[38] J. Karamačoski, N. Paunkoska, N. Marina, and M. Punčeva, "Blockchain for reliable and secure distributed communication channel," in *IEEE IAICT*, July 2019, pp. 91–97.

[39] M. R. L. Perez, B. Gerardo, and R. Medina, "Modified sha256 for securing online transactions based on blockchain mechanism," in *IEEE HNICEM*, Nov 2018, pp. 1–5.

[40] M. Vinayak, H. A. Pal Singh Panesar, S. d. Santos, R. K. Thulasiram, P. Thulasiraman, and S. S. Appadoo, "Analyzing financial smart contracts for blockchain," in *IEEE iThings and IEEE GreenCom and IEEE CPSCom and IEEESmartData*, 2018, pp. 1701–1706.

[41] C. Onwubiko, "Focusing on the recovery aspects of cyber resilience," in *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, June 2020, pp. 1–13.

[42] Q. He, N. Guan, M. Lv, and W. Yi, "On the consensus mechanisms of blockchain/dlt for internet of things," in *IEEE SIES*, June 2018, pp. 1–10.

[43] K. Sharma and D. Jain, "Consensus algorithms in blockchain technology: A survey," in *ICCCNT*, July 2019, pp. 1–7.

[44] H. Saini, B. Bhushan, A. Arora, and A. Kaur, "Security vulnerabilities in information communication technology: Blockchain to the rescue (a survey on blockchain technology)," in *ICICICT*, vol. 1, July 2019, pp. 1680–1684.

[45] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22 328–22 370, 2019.

[46] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117 134–117 151, 2019.

[47] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 7, pp. 1366–1385, July 2018.

[48] S. Pahlajani, A. Kshirsagar, and V. Pachghare, "Survey on private blockchain consensus algorithms," in *ICIICT*, April 2019, pp. 1–6.

[49] G. Epiphaniou, M. Bottarelli, H. Al-Khateeb, N. Ersotelos, J. Kanyaru, and V. Nahar, *Smart Distributed Ledger Technologies in Industry 4.0: Challenges and Opportunities in Supply Chain Management*, Apr 2020, pp. 319–345.

[50] S. Kim, Y. Kwon, and S. Cho, "A survey of scalability solutions on blockchain," in *ICTC*, Oct 2018, pp. 1204–1207.

[51] K. Zhang and H. Jacobsen, "Towards dependable, scalable, and pervasive distributed ledgers with blockchains," in *IEEE ICDCS*, 2018, pp. 1337–1346.

[52] S. Barron, Y. M. Cho, A. Hua, W. Norcross, J. Voigt, and Y. Haimes, "Systems-based cyber security in the supply chain," in *2016 IEEE Systems and Information Engineering Design Symposium (SIEDS)*, April 2016, pp. 20–25.

[53] G. Lu, X. Koufteros, and L. Lucianetti, "Supply chain security: A classification of practices and an empirical study of differential effects and complementarity," *IEEE Transactions on Engineering Management*, vol. 64, no. 2, pp. 234–248, May 2017.

[54] M. J. M. Chowdhury, A. Colman, M. A. Kabir, J. Han, and P. Sarda, "Blockchain versus database: A critical analysis," in *IEEE TrustCom/BigDataSE*, Aug 2018, pp. 1348–1353.

[55] A. Ensor, S. Schefer-Wenzl, and I. Miladinovic, "Blockchains for iot payments: A survey," in *IEEE Globecom Workshops (GC Wkshps)*, Dec 2018, pp. 1–6.

[56] F. Golatowski, B. Butzin, T. Brockmann, T. Schulz, M. Kasparick, Y. Li, R. Rahmani, A. Haber, M. Sakalsız, and O. Aydemir, "Challenges and research directions for blockchains in the internet of things," in *IEEE ICPS*, 2019, pp. 712–717.

[57] A. F. Zorzo, H. C. Nunes, R. C. Lunardi, R. A. Michelin, and S. S. Kanhere, "Dependable iot using blockchain-based technology," in *LADC*, 2018, pp. 1–9.

[58] Y. Murray and D. A. Anisi, "Survey of formal verification methods for smart contracts on blockchain," in *IFIP NTMS*, June 2019, pp. 1–6.

[59] N. Al-Zaben, M. M. Hassan Onik, J. Yang, N. Lee, and C. Kim, "General data protection regulation complied blockchain architecture for personally identifiable information management," in *iCCECE*, Aug 2018, pp. 77–82.

[60] J. Bernal Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. Torres Moreno, and A. Skarmeta, "Privacy-preserving solutions for blockchain: Review and challenges," *IEEE Access*, vol. 7, pp. 164 908–164 940, 2019.

[61] M. Belotti, N. Božić, G. Pujolle, and S. Secci, "A vademecum on blockchain technologies: When, which, and how," *IEEE Communications Surveys Tutorials*, vol. 21, no. 4, pp. 3796–3838, Fourthquarter 2019.

[62] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 21, no. 2, pp. 1676–1717, Secondquarter 2019.

[63] M. C. Kus Khalilov and A. Levi, "A survey on anonymity and privacy in bitcoin-like digital cash systems," *IEEE Communications Surveys Tutorials*, vol. 20, no. 3, pp. 2543–2585, thirdquarter 2018.

[64] S. Park, S. Im, Y. Seol, and J. Paek, "Nodes in the bitcoin network: Comparative measurement study and survey," *IEEE Access*, vol. 7, pp. 57 009–57 022, 2019.

[65] C. Deng, J. Fan, Z. Wang, Y. Luo, Y. Zheng, Y. Li, and J. Ding, "A survey on range proof and its applications on blockchain," in *CyberC*, Oct 2019, pp. 1–8.

[66] A. Mushtaq and I. U. Haq, "Implications of blockchain in industry 4.o," in *ICEET*, 2019, pp. 1–5.

[67] H. Juma, K. Shaalan, and I. Kamel, "A survey on using blockchain in trade supply chain solutions," *IEEE Access*, vol. 7, pp. 184 115–184 132, 2019.

[68] N. V. Vafiadis and T. T. Taefi, "Differentiating blockchain technology to optimize the processes quality in industry 4.0," in *IEEE WF-IoT*, 2019, pp. 864–869.

[69] J. Al-Jaroodi and N. Mohamed, "Blockchain in industries: A survey," *IEEE Access*, vol. 7, pp. 36 500–36 515, 2019.

[70] ——, "Industrial applications of blockchain," in *IEEE CCWC*, 2019, pp. 0550–0555.

[71] M. AlTaei, N. B. A. Barghuthi, Q. H. Mahmoud, S. A. Barghuthi, and H. Said, "Blockchain for uae organizations: Insights from cios with opportunities and challenges," in *IIT*, Nov 2018, pp. 157–162.

[72] M. Demir, A. A. Mashatan, O. Turetken, and A. Ferworn, "Utility blockchain for transparent disaster recovery," in *IEEE EPEC*, Oct 2018, pp. 1–6.

[73] P. Siano, G. De Marco, A. Rolán, and V. Loia, "A survey and evaluation of the potentials of distributed ledger technology for peer-to-peer transactive energy exchanges in local energy markets," *IEEE Systems Journal*, vol. 13, no. 3, pp. 3454–3466, Sep. 2019.

[74] S. Madumidha, P. S. Ranjani, U. Vandhana, and B. Venmuhilan, "A theoretical implementation: Agriculture-food supply chain management using blockchain technology," in *TEQIP IMICPW*, 2019, pp. 174–178.

[75] M. Nakasumi, "Information sharing for supply chain management based on block chain technology," in *2017 IEEE 19th Conference on Business Informatics (CBI)*, vol. 01, July 2017, pp. 140–149.

[76] P. Dunphy, L. Garratt, and F. Petitcolas, "Decentralizing digital identity: Open challenges for distributed ledgers," in *IEEE EuroS PW*, April 2018, pp. 75–78.

[77] M. B. H. Weiss, K. Werbach, D. C. Sicker, and C. E. C. Bastidas, "On the application of blockchains to spectrum management," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 2, pp. 193–205, June 2019.

[78] E. N. Lallas, A. Xenakis, and G. Stamoulis, "A generic framework for a peer to peer blockchain based fog architecture in industrial automation," in *SEEDA-CECNSM*, Sep. 2019, pp. 1–5.

[79] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. M. Leung, "Blockchain and machine learning for communications and networking systems," *IEEE Communications Surveys Tutorials*, pp. 1–1, 2020.

[80] J. Moyne, S. Mashiro, and D. Gross, "Determining a security roadmap for the microelectronics industry," in *ASMC*, April 2018, pp. 291–294.

[81] M. S. Asif, "Survey for the applications in distributed iot," in *(ITC-CSCC)*, June 2019, pp. 1–4.

[82] M. Hammoudeh, G. Epiphaniou, S. Belguith, D. Unal, B. Adebisi, T. Baker, A. S. M. Kayes, and P. Watters, "A service-oriented approach for sensing in the internet of things: Intelligent transportation systems and privacy use cases," *IEEE Sensors Journal*, pp. 1–1, 2020.

[83] A. Sudhan and M. J. Nene, "Employability of blockchain technology in defence applications," in *2017 International Conference on Intelligent Sustainable Systems (ICISS)*, Dec 2017, pp. 630–637.

[84] M. Shen, J. Duan, L. Zhu, J. Zhang, X. Du, and M. Guizani, "Blockchain-based incentives for secure and collaborative data sharing in multiple clouds," *IEEE Journal on Selected Areas in Communications*, pp. 1–1, 2020.

[85] Q. Ding, S. Gao, J. Zhu, and C. Yuan, "Permissioned blockchain-based double-layer framework for product traceability system," *IEEE Access*, vol. 8, pp. 6209–6225, 2020.

[86] W. Xie, W. Zhou, L. Kong, X. Zhang, X. Min, Z. Xiao, and Q. Li, "Ettf: A trusted trading framework using blockchain in e-commerce," in *IEEE CSCWD*, May 2018, pp. 612–617.
[87] M. Demir, O. Turetken, and A. Ferwom, "Blockchain and iot for delivery assurance on supply chain (bidas)," in *IEEE Big Data*, 2019, pp. 5213–5222.
[88] J. P. Mohanty and K. K. Mahapatra, "Security vulnerabilities in applying decentralized ledger systems for obfuscating hardwares," in *2019 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS)*, Dec 2019, pp. 272–275.
[89] J. Zou, B. Ye, L. Qu, Y. Wang, M. A. Orgun, and L. Li, "A proof-of-trust consensus protocol for enhancing accountability in crowdsourcing services," *IEEE Transactions on Services Computing*, vol. 12, no. 3, pp. 429–445, 2019.
[90] U. Bodkhe, P. Bhattacharya, S. Tanwar, S. Tyagi, N. Kumar, and M. S. Obaidat, "Blohost: Blockchain enabled smart tourism and hospitality management," in *CITS*, 2019, pp. 1–5.
[91] H. Wu, J. Cao, Y. Yang, C. L. Tung, S. Jiang, B. Tang, Y. Liu, X. Wang, and Y. Deng, "Data management in supply chain using blockchain: Challenges and a case study," in *ICCCN*, July 2019, pp. 1–8.
[92] M. Sidorov, M. T. Ong, R. V. Sridharan, J. Nakamura, R. Ohmura, and J. H. Khor, "Ultralightweight mutual authentication rfid protocol for blockchain enabled supply chains," *IEEE Access*, vol. 7, pp. 7273–7285, 2019.
[93] P. Gonczol, P. Katsikouli, L. Herskind, and N. Dragoni, "Blockchain implementations and use cases for supply chains-a survey," *IEEE Access*, vol. 8, pp. 11 856–11 871, 2020.
[94] S. Wang, D. Li, Y. Zhang, and J. Chen, "Smart contract-based product traceability system in the supply chain scenario," *IEEE Access*, vol. 7, pp. 115 122–115 133, 2019.
[95] S. J. Divey, M. Hakan Hekimoğlu, and T. Ravichandran, "Blockchains in supply chains: Potential research directions," in *IEEE TEMSCON*, June 2019, pp. 1–6.
[96] S. Bose, M. Raikwar, D. Mukhopadhyay, A. Chattopadhyay, and K. Lam, "Blic: A blockchain protocol for manufacturing and supply chain management of ics," in *IEEE Things and IEEE GreenCom and IEEE CPSCom and IEEE SmartData*, 2018, pp. 1326–1335.
[97] S. Li, H. Xiao, H. Wang, T. Wang, J. Qiao, and S. Liu, "Blockchain dividing based on node community clustering in intelligent manufacturing cps," in *IEEE International Conference on Blockchain (Blockchain)*, July 2019, pp. 124–131.
[98] M. Kuperberg, "Blockchain-based identity management: A survey from the enterprise and ecosystem perspective," *IEEE Transactions on Engineering Management*, pp. 1–20, 2019.
[99] H. R. Hasan, K. Salah, R. Jayaraman, M. Omar, I. Yaqoob, S. Pesic, T. Taylor, and D. Boscovic, "A blockchain-based approach for the creation of digital twins," *IEEE Access*, vol. 8, pp. 34 113–34 126, 2020.
[100] A. Jaiswal, S. Chandel, A. Muzumdar, M. G M, C. Modi, and C. Vyjayanthi, "A conceptual framework for trustworthy and incentivized trading of food grains using distributed ledger and smart contracts," in *IEEE INDICON*, Dec 2019, pp. 1–4.
[101] S. Zhang, E. Zhou, B. Pi, J. Sun, K. Yamashita, and Y. Nomura, "A solution for the risk of non-deterministic transactions in hyperledger fabric," in *IEEE ICBC*, May 2019, pp. 253–261.
[102] A. N. Shwetha and C. P. Prabodh, "Blockchain - bringing accountability in the public distribution system," in *RTEICT*, May 2019, pp. 330–335.
[103] A. Ramalingaiah and T. Sulthana, "Study of blockchain with bitcoin based fund raise use case using laravel framework," in *CSITSS*, 2018, pp. 254–258.
[104] A. S. Omar and O. Basir, "Smart phone anti-counterfeiting system using a decentralized identity management framework," in *IEEE CCECE*, 2019, pp. 1–5.
[105] C. Li and B. Palanisamy, "Decentralized privacy-preserving timed execution in blockchain-based smart contract platforms," in *IEEE HiPC*, Dec 2018, pp. 265–274.
[106] L. P. I. Ledwaba, G. P. Hancke, S. J. Isaac, and H. S. Venter, "Developing a secure, smart microgrid energy market using distributed ledger technologies," in *IEEE INDIN*, vol. 1, July 2019, pp. 1725–1728.
[107] A. Seitz, D. Henze, D. Miehle, B. Bruegge, J. Nickles, and M. Sauer, "Fog computing as enabler for blockchain-based iiot app marketplaces - a case study," in *International Conference on Internet of Things: Systems, Management and Security*, 2018, pp. 182–188.
[108] K. Abdellatif and C. Abdelmouttalib, "Graph-based computing resource allocation for mobile blockchain," in *WINCOM*, Oct 2018, pp. 1–4.
[109] J. Stodt, E. Jastremskoj, C. Reich, D. Welte, and A. Sikora, "Formal description of use cases for industry 4.0 maintenance processes using blockchain technology," in *IEEE IDAACS*, vol. 2, Sep. 2019, pp. 1136–1141.
[110] M. S. Devi, R. Suguna, and P. M. Abhinaya, "Integration of blockchain and iot in satellite monitoring process," in *IEEE ICECCT*, Feb 2019, pp. 1–6.
[111] R. Matzutt, M. Henze, J. H. Ziegeldorf, J. Hiller, and K. Wehrle, "Thwarting unwanted blockchain content insertion," in *IEEE IC2E*, April 2018, pp. 364–370.

Mary Asante is currently pursuing a PhD degree in Cyber Security at WMG's Cyber Security Centre (CSC) at the University of Warwick. She received a Master's degree in Human Resources Management at University of Surrey, UK and a Bachelor's degree in Biological Sciences from KNUST, Ghana. She is a Certified Information Security Manager (CISM). She is a consultant and a trainer with over 10 years management experience and has provided information security governance and support for critical business systems in a variety of environments including Defence Industry, government and private sectors. She is a member of ISACA and a chartered fellow of CIPD. Her research interests are in the area of distributed ledger technologies, supply chain security management, industry 4.0, data sharing, cyber resilience and trustworthiness and related areas.

Gregory Epiphaniou Currently holds a position as an Associate Professor of security engineering in WMG's Cyber Security Centre (CSC) at the University of Warwick. His role involves bid support, applied research and publications. He led and contributed to several research projects funded by EPSRC, IUK and local authorities totalling over £3M. He is also the main inventor of a patented-pending technology on a distributed ledger system (GB2576160A/US200042497A1). He was previously holding a position as a Reader in Cybersecurity and acted as deputy director of the Wolverhampton Cybersecurity Research Institute (WCRI). He has taught in many universities both nationally and internationally a variety of areas related to proactive network defence with over 80 international publications in journals, conference proceedings and author in several books and chapters. He holds several industry certifications around Information Security and worked with several government agencies including the UK MoD in Cybersecurity related projects. He currently holds a subject matter expert panel position in the Chartered Institute for Securities and Investments. He acts as a technical committee member for several scientific conferences in Information and network security and serves as a key member in the development of WS5 for the formation of the UK Cybersecurity Council.

Carsten Maple is Professor of Cyber Systems Engineering at WMG's Cyber Security Centre (CSC). He is the director of research in Cyber Security working with organisations in key sectors such as manufacturing, healthcare, financial services and the broader public sector to address the challenges presented by today's global cyber environment. He has an international research reputation and extensive experience of institutional strategy development and interacting with external agencies. He has published over 200 peer reviewed papers and is co-author of the UK Security Breach Investigations Report 2010, supported by the Serious Organised Crime Agency and the Police Central e-crime Unit. Professor Maple is a Fellow of the British Computer Society and Vice chair of the Council of Professors and Heads of Computing, UK.

Haider Al-Khateeb specialises in Cybersecurity, Digital Forensics and Incident Response (DFIR), he is a Fellow of the Higher Education Academy (FHEA) and holds a PhD in Cybersecurity. Haider is a Senior Lecturer and conducts his research at the Wolverhampton Cyber Research Institute (WCRI), University of Wolverhampton. Within his area of expertise, he has published numerous professional and peer-reviewed articles, participated in a broad range of funded projects, worked with SMEs to launch new products, and delivered a range of hands-on technical training and executive Master's degrees through leading IT training providers in the UK such as QA Ltd.

Mirko Bottarelli was born in 1980 in Milan, Italy. He received his Bachelor and Master's degrees in Computer Science from Università degli Studi di Milano Bicocca, Milan, Italy in 2004 and 2006, respectively. He is a lecturer in Cybersecurity in the faculty of Mathematics & Computer Science at the University of Wolverhampton. Being a member of the Order of Engineers in Italy and a software architect and engineer, he is currently pursuing a PhD degree in the Faculty of Science and Engineering at the University of Wolverhampton, UK. His research interests are in the area of wireless communication, information theory and physical layer security. He is also interested in blockchain technologies and other related areas.

Kayhan Zrar Ghafoor is currently working as an associate professor at the Salahaddin University-Erbil and visiting scholar at the University of Wolverhampton. Before that, he was a postdoctoral research fellow at Shanghai Jiao Tong University, where he contributed to two research projects funded by National Natural Science Foundation of China and National Key Research and Development Program. He is also served as a visiting researcher at University Technology Malaysia. He received the B.Sc. degree in electrical engineering, the M.Sc. degree in remote weather monitoring and the Ph.D. degree in wireless networks in 2003, 2006, and 2011, respectively. He is the author of 2 technical books, 7 book chapters, 65 technical papers indexed in ISI/ Scopus. He is the recipient of the UTM Chancellor Award at the 48^{th} UTM convocation in 2012.