IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier xx.xxxx/ACCESS.xxxx.DOI

Blockchain for Industry 5.0: Vision, Opportunities, Key Enablers, and Future Directions

ASHWIN VERMA[1], PRONAYA BHATTACHARYA [1], NIRAV MADHANI[1], CHANDAN TRIVEDI[1], BHARAT BHUSHAN[2], SUDEEP TANWAR[1], (SENIOR MEMBER, IEEE), GULSHAN SHARMA[3], PITSHOU N BOKORO[3], RAVI SHARMA[4]

[1]Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat-382481, India (e-mails: ashwin.verma@nirmauni.ac.in, pronoya.bhattacharya@nirmauni.ac.in, 18bce135@nirmauni.ac.in, chandan.trivedi@nirmauni.ac.in, sudeep.tanwar@nirmauni.ac.in)
[2]School of Engineering and Technology, Sharada University, Greater Noida, 201310, India(e-mail: bharat_bhushan1989@yahoo.com)
[3]Department of Electrical Engineering Technology, University of Johannesburg, Johannesburg 2006, South Africa. (e-mails: gulshans@uj.ac.za, pitshoub@uj.ac.za)
[4]Centre for Inter-Disciplinary Research and Innovation, University of Petroleum and Energy Studies, Dehradun, 248001, India. (e-mail: ravisharmacidri@gmail.com)

Corresponding author(s): (Sudeep Tanwar (sudeep.tanwar@nirmauni.ac.in) and Gulshan Sharma (e-mail: gulshans@uj.ac.za)

ABSTRACT Industry 4.0 have witnessed a paradigm shift from cyber-physical systems (CPS) that aims at massive automation, towards a more customer-driven approach. The shift has been attributed to the design of hyper-cognitive systems, integration of virtual and extended reality, digital machinery prototyping and twin designs, trusted machine boundaries, collaborative robots, and artificial intelligence (AI)-based supply chains. This new wave, termed Industry 5.0, is expected to leverage massive production with user-centric customization outside the scope of Industry 4.0 ecosystems. Industry 5.0 is expected to assist diverse industrial verticals like healthcare, smart farming, drones, smart grids, and supply chain production ecosystems. However, data is shared among multiple heterogeneous networks, spanning different authoritative domains. Thus, trusted and secured data transfer is crucial to synergize and secure the industrial perimeters. Blockchain (BC) is a preferred choice as a security enabler to Industry 5.0 ecosystems owing to its inherent property of immutability, chronology, and auditability in industrial systems. Limited works are proposed that present the vision and holistic view of BC-assisted Industry 5.0 applications. The article presents a first-of-its-kind survey on BC as a security enabler in Industry 5.0. Based on a descriptive survey methodology and research questions, we presented the key drivers, and potential applications, and propose an architectural vision of BC-based Industry 5.0 in diverse applicative verticals. The survey intends to present solutions that would assist industry practitioners, academicians, and researchers to drive novel BC-assisted solutions in Industry 5.0 verticals.

INDEX TERMS Blockchain, Industry 5.0, Internet-of-Things, Security, Privacy

I. INTRODUCTION

We are presently in the midst of the fourth industrial revolution, or Industry 4.0, that invoked automation in industrial processes and integrated key technologies like Internet-of-Things (IoT), artificial intelligence (AI), cloud and edge computing to leverage the vision of smart factories, and increase in production. Industry 4.0 has revolutionized the previous versions, where the sole aim is to boost productivity and accomplish mass production. Industry 1.0, which started in the 1970, is mechanical, and water and steam energy generation are the major driving components. Industry 2.0 saw the emergence of assembly line production, where Henry Ford, in 1870, pioneered the concept of assembly lines and electricity production into a mass production unit at low costs. Industry 3.0 saw the shift from mechanical production towards digitization, and partial automation became part of the industrial processes. In this generation, memory-programmable controller logic and large-sized computers are included in industrial plans, which reduces human efforts. In 2011, the world saw a drastic shift towards Industry 4.0.

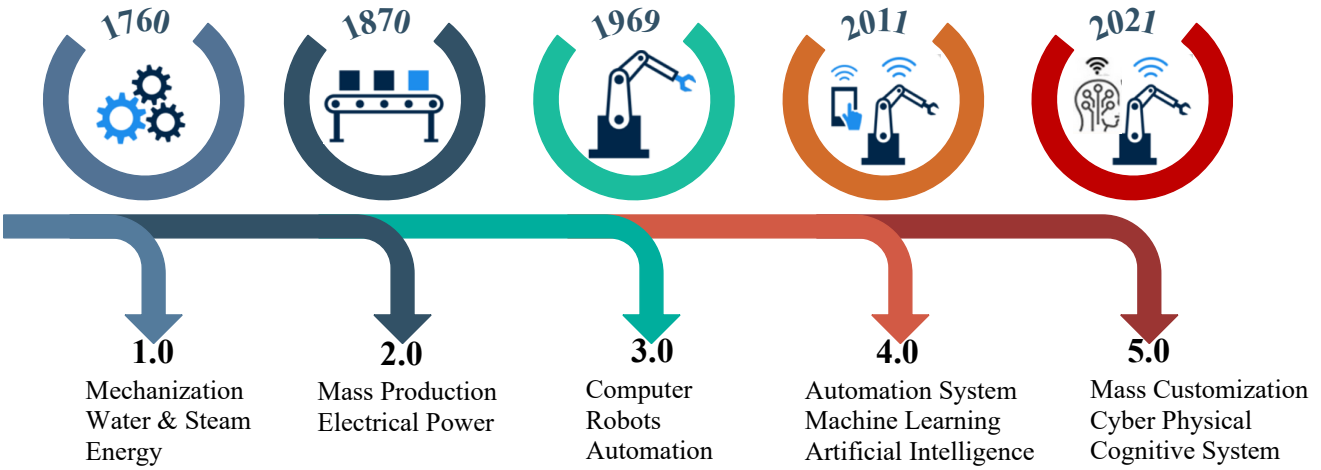


FIGURE 1: A prospective shift towards Industry 5.0 ecosystem

TABLE 1: Key definitions of Industry 5.0 by experts

Proposed By	Key Definition
Rada *et al.* [1]	Industrial 5.0 is the first human-led industrial evolution, based on the 6R principles of industrial upcycling such as Recognize, Reconsider, Realize, Reduce, Reuse, and Recycle. It is a method of systematic waste prevention and logistics efficiency design used to assess life standards, and inventive ideas and manufactures high-quality custom items.
Nahavandi *et al.* [2]	To enhance the process efficiency, Industry 5.0 combines human brainpower and ingenuity with intelligent systems. It combines the capabilities of the cyber-physical production system (CPPS) and human intelligence to cater to the labour shortfall problem present in Industry 4.0. Industries, in collaboration with researchers, develop creative and human-centred design solutions.
Longo *et al.* [3]	According to the European Economic and Social Committee, Industry 5.0 combines the strengths of human intelligence and CPPS to build cooperative factories. Authorities are trying to develop ethical and innovative solutions to overcome the labour shortage problem in Industry 4.0.
Friedman *et al.* [4]	Industry 5.0 necessitates industry practitioners and information technologists to prioritise human factors consideration in industrial system technology.
Koch *et al.* [5]	Industry 5.0 is society of smart factories where robots intended for direct communication with human interacts. The smart factories use the social and corporate networks to connect human and cyber-physical systems
Show *et al.* [6]	Industry 5.0 is a congruous innovation and next generation of governance and it attempts to isolate hyperconnected manufacturing and industrial automation systems.
Maddikunta *et al.* [7]	Industry 5.0 is a human-centred design approach where humans and cobots collaborative work for multiple resources to customise autonomous production. Cobots are not programmable but can detect and understand human presence. This enables cobots for repetitive activities and labour-intensive work, while humans will be in charge of overall management.

This generation involves information and communication technologies to assist remote production lines orchestrated through assisted networks. Industry 4.0 also witnessed the rise of IoT-driven cyber-physical systems (CPS), which initiated the smart factory vision and triggered autonomous monitoring, self-organized productions, and connected logistics to maximize business profits [8]. FIGURE 1 presents a brief dive into the industrial generations and their associated specifics. Industry 4.0 is oriented towards smart manufacturing, where automation is the main driving force. The next revolution is Industry 5.0 which presents the cognitive control process from Industry 4.0, with greater engagement in human-machine interactions. As a result, rather than being process-driven, it would be value-driven.

In Industry 5.0, AI would be a driving force to combine human expertise to design precise control and cognitive abilities. Experts have defined the Industry 5.0 vision based on manufacturing principles, control, and intelligent behaviour. TABLE 1 presents the key definitions by different researchers. The manufacturing processes would be tailored to meet the customized requirements of the end-user. Industry 5.0 is envisioned as a way to increase production quality by allowing robots to handle repetitive and boring tasks while people handle critical thinking and intelligent tasks. This would create a niche market for skilled labourers. Humans will guide robots in Industry 5.0, focusing on mass customization. Industry 5.0 has a strong connection with CPS, where a process relationship would be collaboratively visioned between humans and robots. The new term, collaborative robots (cobots), would form the basic foundation in process management. It would also be greener, where the focus would be on sustainable production and development [9], [10].

Automation is a prime requirement, and AI-driven pipelines would be supported through effective machine learning (ML), deep learning (DL), and reinforcement learning (RL) models. However, to manage the processes effectively, the inclusion of the human element is vital. The processes in CPS-driven Industry 5.0 would exchange massive data over the web through assisted wireless networking channels. Thus, the process data must be protected against malicious attacks that could jeopardize the security and privacy of sensitive data. Moreover, with tailored requirements, the client information must be preserved among communicating

TABLE 2: Acronyms and their meanings

Acronym	Meaning	Acronym	Meaning	Acronym	Meaning
3D	Three Dimensional	DT	Digital Twin	MEC	Multi-access Edge Computing
5G	Fifth Generation	DVM	Dew Virtual Machine	MHR	Medical Health Records
6G	Sixth Generation	EHD	Electronic Healthcare Data	ML	Machine Learning
AAA	American Automobile Association	EHR	Electronic Health Record	mMTC	massive Machine Type Communications
AI	Artificial Intelligence	EHRs	Electronic Health Record	P2P	Peer-to-Peer
API	Application Programming Interface	eMBB	enhanced Mobile Broadband	PHRD	Personal Healthcare Record
AR/VR	Augmented Reality and Virtual Reality	EMR	Electronic Medical Records	PoA	Proof-of-Authority
ASC	Agriculture Supply Chain	EOS	Electro-Optical System	PoS	Proof-of-Stake
BC	Blockchain	ESSs	Energy Storage Systems	PoW	Proof-of-Work
BFT	Byzantine Fault Tolerance	Ex-AI	Explainable Artificial Intelligence	PSNs	Pervasive Social Networks
BPM	Business Process Management	FeMBB	Further eMBB	RL	Reinforcement Learning
CAPEX	Capital Expenditure	HACCAP	Hazard Analysis and Critical Control Points	RPC	Remote Procedure Call
Cobots	Collaborative Robots	HDG	Healthcare Data Gateway	SCM	Supply Chain management
COVID-19	novel Coronavirus	HIPPA	Health Insurance Portability and Accountability Act	SCs	Smart Contracts
CP	Control Process	ICT	Information and Communication Technologies	SDN	Software-Defined Networking
CPPS	Cyber Physical Production Systems	IoT	Internet of Things	SPM	Supplier Performance Management
CPS	Cyber Physical Systems	IoV	Internet-of-Vehicles	UAV	Unmanned Aerial Vehicles
DApp	Decentralized Applications	IPFS	Interplanetary File Systems	UBI	Usage Based Insurance
DDoS	Distributed Denial of Service	JSON	Javascript Object Notation	uRLLC	ultra Reliable Low Latency Communications
DES	Distributed Energy System	LED	Logic Efficiency Design	V2I	Vehicle-to-Infrastructure
DL	Deep Learning	LSTM	Long Short Term Memory	V2V	Vehicle-to-Vehicle

nodes. Fair information practices and user-defined norms to access the data, with authorization is a baseline strategy to address privacy issues [11].

Privacy-preservation techniques require less data sharing, and thus AI models would not be able to customize themselves properly as explicit information fields would be hidden. Thus, an optimal mix of personalization privacy tradeoffs is required. However, the privacy and security-based solutions are not sufficient, as the anomalous behaviour of sensor nodes is not taken into account. Trust in data sharing and control is vital as heterogeneous and autonomous networks collaborate in Industry 5.0. Due to this, blockchain (BC) is a potential solution that can form transparent ledgers, where industrial process data is easily controlled and managed. BC is a shared, distributed and immutable ledger that facilitates the process of recording transactions and tracking assets in a Peer-to-Peer (P2P) network. It forms trusted review platforms that help in auditing and compliance purposes [12]. In a nutshell, BC is a digital data ledger that regularly accumulates information in chronological sequence. In BC, a block header is issued a hash, which is linked to the previous block hash. Thus, the data is immutable once it is added to the chain. If any of the transactions in the block are modified, the Hash of the block is modified.

In Industry 5.0 supply chains, smart contracts (SCs) also play a vital role in ensuring security enforcement, access control, authentication, and automated service-oriented behaviours. SC-assisted digital identities are used to manage assets, goods, items, and services [13]. SCs interact with the underlying BC network through the contract low-level interface, which automates the stakeholder agreements. To manage the BC network effectively, consensus protocols play an important role and control the scalability of the BC network, node throughput, and mining latency. Proof-of-Work (PoW) and Proof-of-Stake (PoS) consensus are resource-intensive and thus unsuitable for responsive data sharing in industrial processes. To manage and orchestrate real-time data, a permissioned BC is a preferred approach for Industry 5.0 ecosystems, where low powered consensus approaches like RAFT, Tangle, IOTA, and Omniledger are mostly deployed [14]. Another important aspect of BC's fourth generation is to form verifiable models to thrawt attacks like Sybil, distributed denial-of-service (DDoS), and 51% attacks. SC is often flawed with different attack sets like code injection, reentrancy, out-of-order, and gas attacks, which should be thwarted by secure BC design. In Industry 5.0, different business-related applications and Hashgraph technology assure that the proposed consensus is fair and scalable in approach. TABLE 2 presents the list of acronyms and associated meanings used in the article.

A. MOTIVATION

Industry 5.0 is envisioned to integrate human influence in the automation processes, which leverages precise and accurate control and modelling systems. The data exchange is over open wireless networks, and thus security becomes a key principle to safeguard the industrial systems. Thus, BC is a primer solution of Industry 5.0 to leverage trusted control with auditable, chronological, and timestamped ledgers. The recent studies on Industry 5.0 are preliminary and discuss the vision, key technologies, and process-driven measures. However, the security viewpoint of Industry 5.0 is equally important. To the best of our knowledge, this is the first article that discusses the requirement of BC as a key enabler in Industry 5.0. The motivation of the article is trivial. We present the key technicalities of BC-assisted Industry 5.0 in diverse verticals of Industry 5.0, namely, smart manufacturing, sensor-driven control, healthcare, robotics, and value-driven business applications. The article presents the use-cases, architectures, security challenges, and case study that systematically unfolds the BC-leveraged Industry 5.0 vision in the associated verticals.

B. ORGANIZATION AND READING MAP

FIGURE 2 presents the organization of the article and the reading map. Section II discusses the background of Industry 5.0, with a comparative analysis to its predecessor Industry 4.0, and we highlight the potential of BC in Industry 5.0

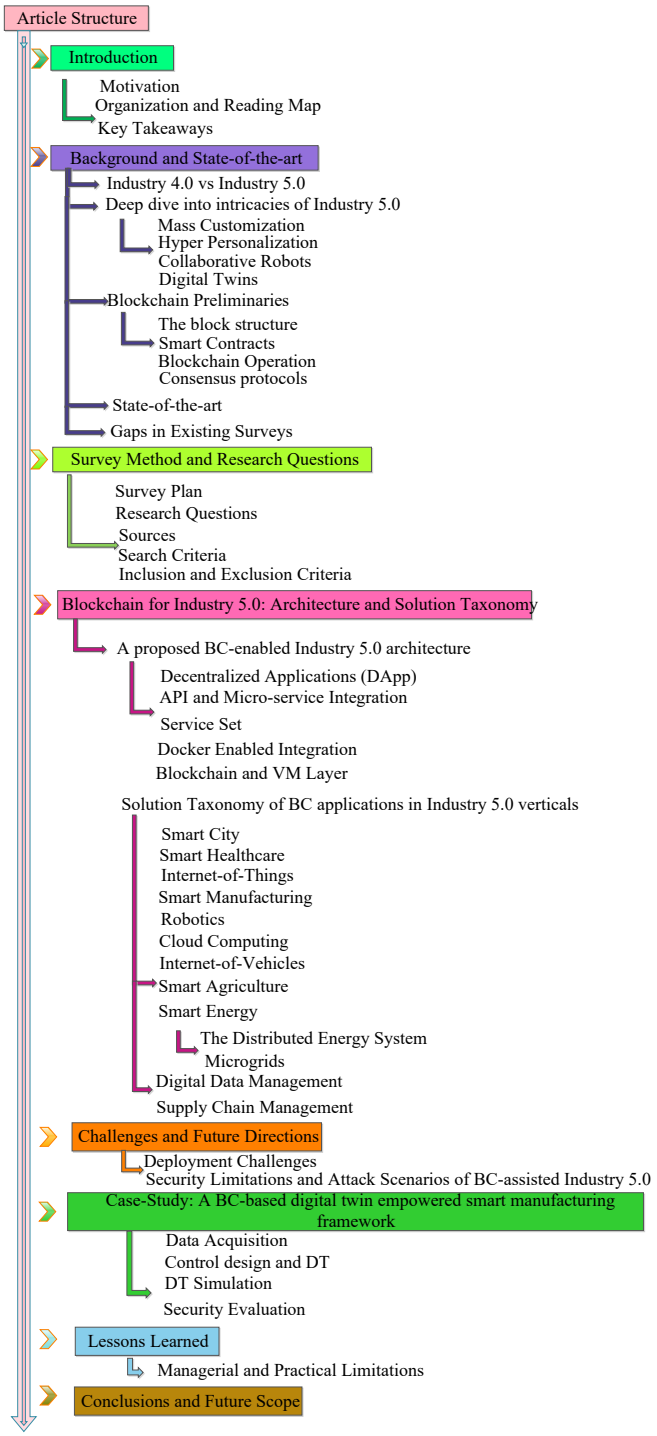


FIGURE 2: Organization and Reading Map

to secure the process boundaries. A discussion on existing state-of-the-art schemes is presented, which is followed by section III that presents the survey methodology and the research questions. Based on the proposed research questions, section IV presents a proposed BC-based Industry 5.0 architecture that meets the requirements of different industry verticals. A solution taxonomy is presented, and a comprehensive discussion is presented. Section V presents the research challenges and future directions to conceptualize the vision of BC-envisioned Industry 5.0. However, BC is not the panacea of all security implements, thus we highlight the security limitations and attack scenarios which are possible even with the integration of BC in Industry 5.0 ecosystems. Next, section VI presents a unique case study on Industry 5.0 production plant is presented, that integrates digital twin (DT) simulation, AI-driven analytics, and BC to assure optimal performance with minimized bias. We analysed the security analysis on the proposed case study, which justifies the proposed case-study deployment in real scenarios. Next, section VII presents the key lessons learned from the survey, and section VIII presents the concluding remarks.

C. KEY TAKEAWAYS

The key takeaways of the article as enumerated as follows.

- The foundations and basics of Industry 5.0 are presented, along with the assisted technologies. We present the integration of BC in Industry 5.0 verticals and discuss the potential use-cases.
- The article presents a proposed reference architecture of BC-assisted Industry 5.0 in different verticals. The modules and assisted components of related applications with BC integration are discussed.
- Based on research questions, a solution taxonomy of BC in Industry 5.0 is presented.
- Research challenges and future directions are discussed, and a case study of Industry 5.0 for smart manufacturing is discussed. The data is maintained in BC ledgers, and reference architecture with different layers and functionalities is discussed. Finally, the key lessons of the survey are outlined.

II. BACKGROUND AND STATE OF THE ART

The section discusses the basics of Industry 4.0, the potential limitations, and the emergence of Industry 5.0. Next, we present the key technicalities of Industry 5.0 and explore the integration of BC with Industry 5.0. We conceptualize the vision, enablers, and consensus protocols to realize the full potential of industrial processes. Finally, we present related surveys on the topic, and their pros and cons of them are highlighted. The details are presented as follows.

A. INDUSTRY 4.0 VERSUS INDUSTRY 5.0

Industry 4.0 is focused on sensor-driven connections, whereas Industry 5.0 is focused on human-centric solutions. Industry 5.0 integrates human ingenuity with robotic accuracy to create a one-of-a-kind solution that will be in high demand in the coming decade. A close interaction between human-to-machine is justified with cobots, which link communication between the factory, transportation, supply chain, and the end-user. TABLE 3 represents the key differences between Industry 4.0 and Industry 5.0, and the potential security solutions provided by BC.

TABLE 3: A comparative analysis of Industry 4.0 vs Industry 5.0 primers and its convergence with BC

Industry 4.0	**Industry 5.0**	**Limitation in Industry 4.0**	**Solutions with BC in Industry 5.0**
Intelligent Supply Chain	Distributed Supply Chain	Administrative access is limited to a single party, which increases data tampering, and misplaced control	Only insertion is allowed which prevents tampering and ensures transparency.
Mass automation	Collaborative AI	Replaces barriers in networked locations with an increase in cobot communication to yield more productivity	Increased access control is guaranteed with SCs
Smart Products	Experience Activated Products	Not customized as per user personal needs	Allow hyper-customization at large scales by ensuring data privacy using BC
Focus on Connecting Machines	Focus on delivering customer experience	End goal (customer experience) often ignored.	Trusted and auditable customer-oriented solutions
Mass Customization	Hyper-Personalization	Leaves all the work to the user to generate the best experience for themselves	Immutable ledgers of networked data and control processes to streamline the industrial processes

Industry 5.0 focuses on three increasingly crucial aspects, namely- the quality of life, inclusivity, and sustainability, with people at the core of processes. The goal of Industry 5.0 is to make workers' lives better and more pleasant while also guaranteeing that they have access to technology that allows for automated processes and higher productivity. Industry 5.0 teaches individuals about environmental stewardship, ecosystem protection, and the most efficient use of accessible resources for upcoming generations.

Industry 5.0 provides user-based customization, penalisation, integration of cognitive domain to human intelligence, and most importantly transition is back to a real environment. The motivation for Industry 4.0 is mass production while Industry 5.0 revolve around making smart societies. Industry 4.0 has the involvement of technologies such as IoT, cloud computing big data, robotics and AI while in Industry 5.0 the human-robot collaboration using renewable energy is the key technology. In terms of application and research areas, Industry 4.0 is inclined toward operational research, business administration and improvement in the innovation of processes. On the other side, Industry 5.0 additionally applies to a smart environment including agriculture, biology, waste prevention, and economy.

B. DEEP DIVE INTO INTRICACIES OF INDUSTRY 5.0

Industry 5.0 aims to combine human intervention with automated processes, making industrial workflows more explainable. In Industry 5.0, the autonomous workforce knows human desires and intentions. Thus humans would work closely with robotic coworkers without fear, as the former understands and interacts with them. Consequently, the process would exhibit synergism and be aligned to business models, which would lead to less resource wastage and reduce capital and operational expenditures. Moreover, Industry 5.0 would be self-sustainable and self-healing, supporting the green production movement.

In Industry 5.0, the autonomy of robots would decrease, in a sense, that robots would be employed only to perform tedious and repetitive tasks. It would be programmed to understand instructions from humans and process human instructions via ML and DL algorithms to produce correct outputs. Thus, this next generation of robots would minimize the production risk, specifically cobots. Cobots would be able to detect, comprehend, and feel not just the humans around them but also the associated aspirations and expectations. Furthermore, cobots would be able to learn from their associated environment using deep RL algorithms, and they would work on a reward-penalty-driven model where they would eventually train and learn. As instructed by human operators, cobots that learn as they go would be able to perform tasks with minimal errors or bias.

Despite its complexity, Industry 5.0 is based on basic yet effective methods, such as the 6R (Recognize, Reconsider, Realize, Reduce, Reuse and Recycle) methodology and the logic efficiency design (LED) principle. 6R methodology is a superstructure of the 3R (Reduce, Reuse, and Recycle) methods and aims at including the non-functional approach in waste management design. However, 6R methods are applied in waste management, but the principle itself is generic and applies to other manufacturing processes. The LED principle aims to design logic blueprints for industrial processes to maximize operational efficiency. The LED principle is mainly designed to boost supply chain profits. Specific rule sets are designed for operational transparency in supply-chain pipelines, profit-sharing among stakeholders, and design efficiency.

Despite the technical revolutions like 6R and LED in Industry 5.0, there have been disputes and challenges associated with the overall industrial workforce. These challenges mainly arise due to geographical and networked locations, workplace conditions, and societal impacts. In any industry workforce, the human workforce is ageing slowly, which means there are mostly middle-aged skilled persons who take the managerial decisions. This does not allow openness in discussions with the young workforce, and accountability is not properly documented. Moreover, many industrial workplaces are still based on legacy setups and use outdated tools and machinery for production. Thus, such workplaces are not connected via CPS to other production units, and the overall output suffers. Many industrial stakeholders are resistant to change and believe in old-school processes and thus are reluctant to adopt the Industry 4.0 automation processes.

The challenges mentioned above impact the business models, AI-driven profit predictions, and annual turnovers and

eventually lead to many prospective projects' closure. Thus, Industry 5.0 caters explicitly to these challenges. It allows key training of stakeholders, where the project vision, profitability, reliability, and the development blueprint are discussed before the commencement of the project. The role of technology and automation is also discussed, with specific guidelines. This maximizes the value chain and instils belief in the overall system. We next discuss the key design technologies that support the Industry 5.0 visions.

1) Mass Customization

The Industry 5.0 processes would be centred on the digital user experience in mass customization. First, we create a market segment-based approach, where a particular product is designed according to the custom inputs of the specific audience only. The input parameters are the suggestions taken from users through specific interviews, which reflect the unique selling proposition they would like to see in the designed product. Thus, by interviewing a large group (or mass) of users, the stakeholders form the desired set of mandatory functionalities for the design product. The parameter selection depends on user suggestions, demographics, and design features of competitive products. Via intelligent AI systems, the commonalities and striking differences are observed for the target audiences, and tailored products are designed to satisfy the end-user needs. Thus, mass personalization helps firms better engage with customers and target decision-makers across industries.

2) Hyper Personalization

Hyper-Personalization is the notion of acquiring real-time consumer behavioural data to personalize products, services, and experiences according to user preferences. The industrial process requires a deep understanding of the designed goods, their user base, and the associated technology cost to achieve hyper-personalization. Based on the acquired knowledge, a personalized marketing strategy is set up, where digital technologies support the cause, mainly computer vision, AI and ML pipelines, and hyper-cognitive systems, which allow industrial processes to select a specific product for every user. Human inputs and robots work in close collaboration for bulk production to customize the product. The functional behaviour of the product is of prime importance, with cost minimization. A transition from prototype design to agile manufacturing is done in the supply chain to scale the manufacturing processes. For example, a designed e-commerce website can evaluate previous client interactions to recommend the best choice for the new user based on the user clickstreams. This requires a clickstream recommender algorithm to set up a comparative analysis of the best market products for instant comparison.

3) Collaborative Robots

Collaborative robots, or cobots, are designed to work in close interaction with humans, and the collaboration helps them add the human element to the production. Cobots were initially designed by Northwestern University professors in 1996 [15]. First-generation cobots were mechanical and usually involved in mechanical processes, but modern cobots are sensor-driven and can form actuation based on human signals. In Industry 5.0, the personalization of cobots is done to create a full personalization engine for a product. For example, in healthcare 5.0, surgical cobots assist surgeons in performing surgery, which involves 3D-vision and tomography. A similar use case is a telesurgery, where a cobot takes instructions from a remote surgeon to operate through a responsive networking channel, such as tactile internet [16]. Cobots do improve not only production growth but also have the potential to automate mundane tasks and are an essential workforce in modern industries.

4) Digital Twins

DT are virtual representations of real industrial processes, or setups, which are created to specifically emulate the behaviour of a physical object [17]. For example, the physical object under investigation, a turbine motor, is equipped with different sensors that measure different kinematics of its motion, operations, and power control. These sensors generate data regarding the performance of the physical object or process in a variety of ways, including energy output, temperature, and weather conditions. This information is subsequently transmitted to a processing system, and incorporated to simulate a digital copy of the system. Once such information is collected, a virtual model is created, which is used to emulate the real-time physical object. The created DT can evaluate and analyze the performance with specified error bounds. These inputs are iterated multiple times on the system's software version, and the best inputs are collected to be given to the actual object in the real world.

Simulators of real objects are similar in operation, but the main difference between a DT and a simulator is the level of scaling of the industrial process. DT can run multiple simulations to explore different processes, whereas a simulator might work with limited inputs only. Real-time data is rarely useful in simulations, whereas DTs are built on a two-way information flow, where sensors provide data to the system. That data is analyzed with ML/DL model with specific input sets, and feedback is sent back to the controller with error estimation. As DTs have better and more up-to-date data than normal simulations, they can better investigate complex issues and related dependencies.

C. BC PRELIMINARIES

This section presents the background of BC, the block structure, SCs, and the associated operations. This section addresses the RQ1 of the proposed survey, as it presents the basics of BC and its potential in Industry 5.0 ecosystems [18]. In simple words, a BC is a collection of interconnected blocks that store data in a distributed, transparent, and tamper-proof manner [19]. BC-governed Industry 5.0 solutions are decentralized, and it mitigates the challenges of central-controlled industrial processes. TABLE 4 presents the research chal-

TABLE 4: Potential solutions of BC to central-authoritative Industry 5.0 ecosystems

Aspect	**Challenges**	**Implications**	**Solutions with BC**
Centralization	Systems are fragmented and data storage issues	Network latency, Requirements high computing capacity	Decentralized access, increased transparency, and cheap processing power are all advantages.
Establishing Trust	Specific safety requirements for manufacturers	Added redundancy, Dependence on the platform	The ledger's immutability prevents tampering.
Security	Unauthorized access to and alteration of data	Data breaches, data loss, centralized server, single point of failure	Database is not a centralized, immutable ledger of records.
Cost	Middlemen, mediators, and a centralized system are required.	Costly and time-consuming, high risk of fraud, product duplication	Decentralized database, bitcoin payment processing.
Transparency	Policies, standards, rules, and monitoring systems that are unique to each business	Unsatisfactory customer relationship, less visibility	Distributed ledger technology that incorporates a consensus method for verifying transactions.

lenges, the potential implications of central-controlled and authoritative industrial projects, and the potential solutions that BC provides [20]. Whenever a new transaction is added to BC, it is added to the new block, which is mined by entities called miner nodes. With more added blocks, the blocks in the chain increase. Still, any change by a malicious entity to any transaction would invalidate the hash of the associated block, which would further invalidate the linked hash.

1) The block structure

In BC, a corresponding block contains a block header and block body, simply the list of appended transactions. The header includes the version, current block's hash, timestamp, nonce value, and the Merkle root hash value. The Merkle hash is the genesis block information with no associated previous block. The Merkle tree structure assures that subsequent blocks have not been tampered with [21]. The Merkle root is the hashed value of child node hashes, with an associated timestamp of each node. In a bitcoin BC, the block header typically contains three sets of meta-information. The header is an 80-byte long string, where 4 byte represents the bitcoin version number, 32 bytes represents the previous block hash value, 4 bytes are for the difficulty target, 4 bytes for block timestamp, 4 bytes are the nonce value, which is used by miner entities. Moreover, 32 bytes are for the Merkle root information. The difficulty target is for miner nodes, where a Proof-of-Work (PoW) consensus is applied. A hash target is said with leading zeros (0x00 ...), which signifies the difficult problem for all miners [22] [23]. Next, the miner hashes the transactions and the current nonce value. The process is repeated, where the nonce is incremented until the computed hash is lower than the target. The miner node that completes the operation first gets the incentive and the chance to mine the block and subsequent nodes are informed that the target is solved.

2) Smart Contracts

SC plays a vital role in industrial supply-chain ecosystems as multiple stakeholders and transactions are involved between the manufacturer, retailer, warehouse, logistics, and the market sellers. Thus, there is a lack of transparency, ownership, and trust in the entire supply chain. In such cases, SCs can automate the agreements between peer entities on the supply chain, and the transfer of funds occurs when all the agreement cases are met. In short, SCs are programmable codes that are self-executable when the specified conditions of agreement suffice. SCs are deployed either on public, private, or permissioned BC, depending on the application and the data access. The deployment of the contract takes place from the owner's wallet address, and the native code is compiled, where the transaction includes the contract code, and the recipient wallet address [24]. Once the contract is successfully deployed, no change is possible to the transaction. SCs make low-level calls to the underlying BC network to store the arbitrary state and computation information. Ethereum is considered a popular BC network for SCs, and the contracts can be written in languages such as Solidity, Serpent, Go, and others. The contract is executed on the ethereum virtual machine, where the low-level bytecode is generated. Ethereum contracts are Turing-complete, as it involves branching and looping statements to represent programming conditions that can implement any programming problem [25]. In permissioned networks, SCs are often called chain codes and are executed on Hyperledger frameworks using services of orderers and channels.

3) Blockchain Operations

To verify a transaction, the BC network uses cryptographic hash algorithms, such as MD-5, SHA-256, or SHA-512, to generate a unique hash. The list of transactions and nonce value is hashed, and each block's hash is used to generate the hash of the next block. Due to this, BC forms an impenetrable network of transactions. Network nodes or SCs must validate and reach a consensus on any new transactions before adding them. The existing BC is extended due to the insertion of the new block, which is not alterable. As a result of this immutable ledger, a decentralized system is created that is secure and reliable. Consensus methods are used to verify and validate user status and transactions.

4) Consensus protocols

In this subsection, we discuss the consensus protocols of BC. Normally, a consensus protocol assures agreement between all nodes, where they agree on a common commit operation. In BC, once a block is proposed, it can be added to the chain once most nodes validate the proposal. PoW and Proof-of-Stake (PoS) consensus are known, and widely used consensus protocols but are not suitable for industrial operations due to the high-end resource, power, and electricity requirement to run the consensus process. As Industry

5.0 is sensor-driven, low-powered consensus approaches are suitable. Some of the scalable and low-powered consensuses are listed as follows.

1) *IOTA*: IOTA is a distributed ledger and cryptocurrency which is open-source and is optimized for the Internet-of-Things (IoT) ecosystems. IOTA stores transactions on its ledger via a directed acyclic graph (DAG), which provides a possible advantage over BC-based distributed ledgers in terms of scalability. IOTA does not need miners to validate transactions. Instead, nodes are required to approve two prior transactions before issuing a new transaction on the network. As a result, transactions are added without fees, and small transaction sets are also added to blocks. Such transactions are termed micro-transactions. In the IOTA network, the consensus is achieved via a coordinator node which the IOTA Foundation manages. The network is currently centralized due to the coordinator. The potential drawback is the single point of operation, which an adversary might manipulate due to the single-attack point. Thus, IOTA networks are vulnerable to DDoS attacks, where the IOTA server is bombarded with fake bot requests. Despite its centralised constraint, its monetary-free vision and direct connectivity with the underlying sensor network make it beneficial for Industry 5.0 applications. The underlying BC is lightweight, responsive, and scalable since SCs may directly retrieve data from sensor nodes.
2) *Tangle and DAG*: Tangle is also based on the DAG principle, where it is not under the control of any external authority, similar to a cryptocurrency transaction. Tangle is heavily deployed in IoT applications to share and store information in distributed ledgers. It supports massive transaction calls between sensors seamlessly. In tangle, we do not have the miner nodes, and thus the network does not have the incentive mechanism for miners [26]. It is highly scalable and supports microtransactions, just like IOTA. The limitations of the Tangle network over BC are that the consensus is still in developmental phases, and the security of transactions is a prime concern. Moreover, Tangle networks are not suitable for fully decentralized systems.
3) *Tendermint*: Tendermint is a consensus protocol that is a member of the byzantine fault tolerance (BFT) family of protocols and is mostly used in permissioned BC setups. Tendermint, unlike practical BFT (PBFT), aligns every node with different voting capabilities according to the ownership stake. In Tendermint, voting is done in two phases: the pre-vote and the pre-commit phase. The block would be proposed when more than $2/3$ of validators execute pre-commit on the transaction on the same round. Tendermint is suitable for IoT networks but requires alterations to the monetary incentives of the consensus protocol. Nevertheless, it would be one of the widely used protocols in IoT with monetary inclusions due to its low latency and high scalability.
4) *Omniledger*: Omniledger is a distributed ledger technology that ensures long-term security while operating anonymously. It ensures security and accuracy by sharding policy with a heuristic public-randomness technique. It selects statistical representative shards to execute transactions, as well as a fast cross-shard commit protocol for handling transactions that involve multiple shards [39]. Omniledger additionally improves speed by processing intra-shard transactions in parallel, pruning the ledger via collectively-signed state blocks. It performs low-latency "trust-but-verify" validation on low-value transactions. This use of Omniledger in Industry 5.0 is mainly for automation tasks, where the captured data from sensor nodes would be stored in decentralized Omniledger.

D. STATE OF THE ART

This subsection presents the existing state-of-the-art surveys on Industry 4.0, Industry 5.0, and their applicative use-cases with BC. TABLE 5 represents the comparison based on the parameters considered for this survey. In the healthcare domain, Zhang *et al.* [27] discussed the various healthcare-related matrices with the use of BC. A reference architecture is proposed. However, security techniques for healthcare are discussed, but no information or guidance related to privacy and security compliance are discussed. Liu *et al.* [29] proposed a computational logic-based healthcare architecture. Still, the physical design concept was not covered, and the regulations use-cases with BC integration are not discussed.

In the education sector, authors in [28] proposed the concept of tokenization in BC for the evaluation of student performance based on test and grade reports. The survey proposes a reference architecture limited to specific fields, but the open issues and challenges are not properly discussed. Radonav *et al.* [30] proposed a BC-based healthcare solution with access control mechanism. The security standards and validation protocols are not discussed in detail. They discussed the taxonomy that helps identify open issues in the medical domain. Nallapaneni *et al.* [32] presents the convergence of IoT with BC in Industrial processes, and the survey focuses on describing security issues and challenges in IoT in detail. However, the scalable consensus mechanism details to support the IoT networks are not discussed. Konstantinidis *et al.* [31] discussed the business aspect of industry applications, and a sector-wise bifurcation of BC use-cases in business logics. The authors have not proposed any reference framework and have not discussed the open issues in the survey. Dave *et al.* [33] discuss the integration of BC in industry 4.0, and presents the IoT related business aspects. The authors have concluded that scalability and interoperability are key principles considered in this domain study. However, the security aspects and challenges of adopting BC are not the focus of their survey.

Monrat *et al.* [34] discussed adoption of BC in different Industry 4.0 applications and the various roles and issues

TABLE 5: A comparative analysis of existing surveys with the proposed survey

Author	Year	Objective	Pros	Cons	1	2	3	4	5	6	7	8
[27]	2017	Provided evaluation metric for BC-based decentralized application in healthcare.	Evaluation of metric in terms of feasibility, compliance and capability in healthcare domain.	Security of patients data is not discussed.	✓	✓	X	✓	✓	X	X	X
[28]	2017	BC-based learning assessment system in education field.	BC-based learning outcome policy for education institutions to support continuous evaluation	Analysis with different application in the dame domain is not considered	✓	X	✓	✓	X	X	X	X
[29]	2017	Presented the advanced architecture for healthcare system.	Secure and efficient way to exchange medical records among different stakeholders.	Regulations of use either public or private are not mentioned as well as implementation cost is high.	✓	✓	X	✓	✓	X	✓	✓
[30]	2018	Discussed the opportunities of integrating BC in the field of medicine.	BC system provides personalized and secured way to store health record.	Scalability issues with access control.	X	✓	✓	X	✓	X	✓	X
[31]	2018	Discussed BC scenarios for business applications.	Pointed out areas where BC provides solutions to business problems.	Results of the survey does not caters the implementation challenges.	X	✓	X	X	✓	X	X	X
[32]	2018	Discussed issues and challenges in energy distribution in IoT system.	Discussed issues and security in the IoT ecosystem.	Does not consider the scalability issues of implementations of IoT.	✓	X	✓	X	✓	X	X	✓
[33]	2019	Discussed BC as key solution in diverse society verticals	Explored the implementation guidelines for developers	Result of the study does not discussed interoperability and scalability	✓	X	✓	✓	X	✓	✓	X
[34]	2019	Detailed study of BC in different smart city verticals	Benefits and tradeoff of integrating BC is discussed.	Survey does not include security, privacy and scalability	✓	X	✓	✓	✓	X	✓	✓
[35]	2020	Discussed the applications of BC in industry 4.0 in different verticals.	Focused on the security solution that are applicable in business applications.	Survey does not discussed IoV, robotics and edge computing verticals.	✓	✓	✓	✓	✓	X	✓	✓
[36]	2020	Discussed security and privacy issues in healthcare domain	Focused in Privacy and security issues	conclusion of the survey is not mentioned clearly	X	✓	X	X	✓	✓	X	X
[37]	2021	Conduct survey of BC in information system analysis and security	Extensive comparison, clustering, and classification have been carried out	Fault tolerance and compatibility is not mentioned	X	✓	X	X	✓	✓	✓	✓
[7]	2021	Survey of enabling technologies in Industry 5.0	Complete overview of all the enabling technologies in Industry 5.0	Focusing on overview, it provides very little information on role of BC	✓	✓	✓	X	✓	✓	✓	✓
[38]	2021	Authors have explored the link between these enablers by utilising the total interpretative structural modeling technique (TISM) approach.	Very structured bifurcation	A black-box approch, and details on how to perform the operations are not discussed	✓	X	✓	X	X	X	✓	X
[17]	2022	To explore state of art in development of industry 5.0 and its use case with future applications.	Discusses ethical issue and designs to solve the problem with Industry 5.0 with verticals	Limited reviews are taken into consideration and bifurcation of challenges is not discussed	✓	X	✓	X	X	X	✓	X
Proposed	2022	An extensive survey on the potential integration of BC in Industry 5.0 verticals	Discusses the requirements of BC in Industry 5.0 with effective use-cases and solution taxonomy	Role of BC-driven AI verticals is not discussed	✓	✓	✓	✓	✓	✓	✓	✓

1. Architecture, 2. Healthcare, 3. BC, 4. Simulation tool/Framework, 5. Security, 6. Hardware and Physical design, 7. Taxonomy, 8. Open issues and challenges, ✓-shows the parameter is considered, *X*- shows that the parameter is not considered.

in the adoption of BC. However, the challenges and tradeoffs between BC and industrial processes are not clearly explained to justify adoption. Bodkhe *et al.* [40] proposed a BC-based smart tourism and hospitality framework that employed time-series analysis of tourism data from BC ledgers and presented the same as inputs to long short term memory (LSTM) framework. The work provided predictions on travel costs and presented a recommender model that could provide prospective travellers with options for visits to different places. Authors in [36] present an exhaustive survey on BC with industrial applications like healthcare, with a specific focus on security and privacy issues. Bodhke *et al.* [35] proposed a detailed survey of BC in Industry 4.0, with the discussion of possible use-cases like healthcare, smart grid, tourism management, manufacturing, IoT, and others. Various merits and demerits of security solutions are discussed, but the emerging applications that integrate AI like robotics, digital twins, and Internet-of-Vehicles (IoV) are not discussed.

Berdik *et al.* [37] presented their view on BC technology in information systems through a comparative study. A solution taxonomy is presented in the survey for information systems, and potential challenges are discussed. Reddy *et al.* [7] proposed an exhaustive survey on the visions of Industry 5.0, and the key enables that build up the Industry 5.0 in different realms. They have covered many interesting applications and discussed potential use0cases. However, they have not proposed a unified and generic integration framework in the study. Kumar *et al.* [38] explored the linkage of various enablers in Industry 5.0 through the TISM approach and have explained the bifurcation of processes in a structured way. However, the details in their covered subtopics are limited to an overview of applications.

Recently, Dev *et al.* [17] proposed a survey on Industry 5.0 field with in-depth analysis of different verticals. They have considered ethical issues to solve the problem in Industry 5.0, but limited reviews have been considered for their study. However, the survey lacks a discussion of the security principles.

TABLE 6: Research questions to support the survey

Questions	Research Questions	Objective
RQ1	How would BC impact industry 5.0 and its applications?	To analyze the use of BC to provide transparency and traceability in the business processes.
RQ2	What characteristics of BC help to integrate different business processes?	To identify BC and its feature to improve secure communication among processes
RQ3	What are the verticals in industry 5.0 that require security integration?	To explore different industries where BC provides enterprise solutions
RQ4	What are the key challenges in adopting BC for industrial processes?	To delve into the various issues and challenges of adopting BC as an enterprise solution and propose future directions.

E. SURVEY GAPS

Most of the surveys are oriented toward discussing the underlying Industrial principles, key architectures of Industry 4.0 and beyond vision, or BC-based security design in a single industry vertical like healthcare, manufacturing, or others. However, in the future, Industry 5.0 would be a confluence of emerging technologies like IoT, AI, and big-data management, where a large amount of data would be monitored, processed, and exchanged. Thus, the industrial perimeters must have strong security and privacy in place. Furthermore, as BC technology has matured, it would form a trusted perimeter where the internal applications can have authentication and authorization in place [41]. Thus, the integration of BC in Industry 5.0 verticals is required to be discussed. To the best of our knowledge, this is the first survey that discusses the reference architecture of BC-assisted Industry 5.0, presents the solution taxonomy for different industry use-cases, and discusses the open issues and research challenges, with the inclusion of a case study of manufacturing and digital twin technology as an application of industry 5.0.

III. SURVEY METHOD AND RESEARCH QUESTIONS

The section presents the survey methodology as outlined in Kitchenham *et al.* [42], which outlines the logical process of designing a survey. First, we propose a survey plan, and after brainstorming among all authors, formulate the research questions we want to address in the article. The survey includes articles from academic databases filtered using the inclusion-exclusion principle. The details of the same are presented as follows.

A. SURVEY PLAN

The suggested survey is laid out methodically. For literature collection, the following procedures are followed. In the first phase, we determine the research objectives of the article and propose the research questions that we particularly want the article to address. The research questions are proposed based on available research on academic databases and what is not included as of yet. Then, based on set keywords, the articles are collected. After that, we finally outline the rigorous process of inclusion-exclusion to filter out the articles we included in the survey. This literature study includes a variety of publications in related domains such as Industry 4.0, IoT, healthcare, agriculture, and BC. In addition, it includes journal conferences, book chapters, short technical reviews, and blogs on the respective topics. Next, the collected data is inspected for quality, and afterwards, the survey relevant information is extracted. Systematic execution of surveys can assist researchers and scholars in producing fair results without any bias.

B. RESEARCH QUESTIONS

We have outlined the research questions for the article based on available literature on Industry 5.0 and BC. TABLE 6 presents the research questions with the selected objectives, which are addressed in the survey. In a nutshell, the research questions conceptualize the inclusion of BC in different verticals of Industry 5.0.

C. SOURCES

To prepare the survey, we have taken articles from academic databases like ACM, Wiley, Elsevier, ScienceDirect, IEEE *Xplore*, and Springer, which are the most commonly used libraries. These libraries have a broad and diversified collection of literature.

D. SEARCH CRITERIA

The survey included publications that use BC as the fundamental principle and its deployment and integration in industrial applications. We began by searching scholarly repositories for works based on the search term "Blockchain and Industry 4.0/5.0." Then, using the keywords IoT, manufacturing, agriculture, and other applications, we chose papers. The OR keywords are then used to expand our academic database. Papers based on the keywords "healthcare," "supply chain, "digital twin," "digital assets," and others were also gathered. Then we eliminated the publications that were not relevant to our survey study. FIGURE 4 presents the list of keywords and search strings used to search articles. Finally, we continued our search by looking at electronic publications and references to the retrieved documents.

E. INCLUSION AND EXCLUSION CRITERIA

We began by sorting papers into categories based on their relevance to the topic. FIGURE 3 illustrates the proposed survey's inclusion and exclusion criteria. We have included 320 research articles based on selected topics, out of which 70 are excluded as the titles are not relevant. Now, we studied the abstract and conclusion of the article, and further 59 articles are excluded. At this point, we included 30 more articles on digital twins and the manufacturing industry, and AI-based industrial processes. Out of 221 articles, we excluded 36 articles based on the article text on a preliminary

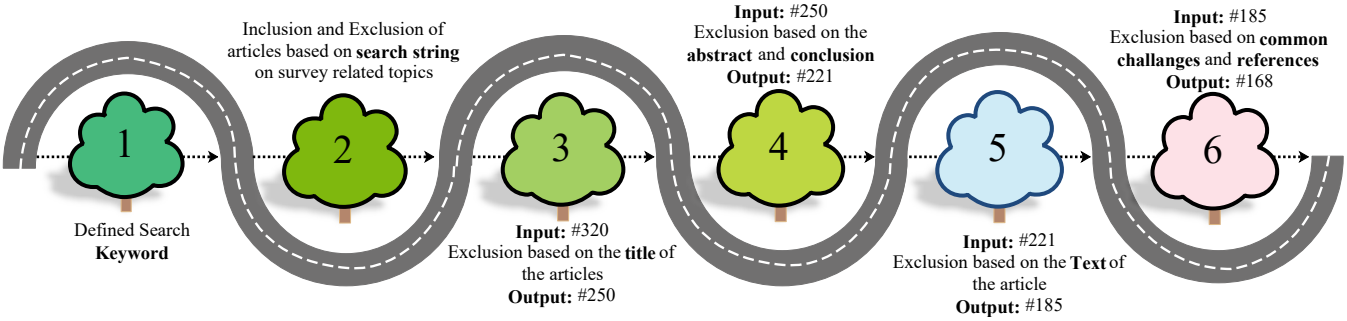


FIGURE 3: Inclusion and exclusion criteria

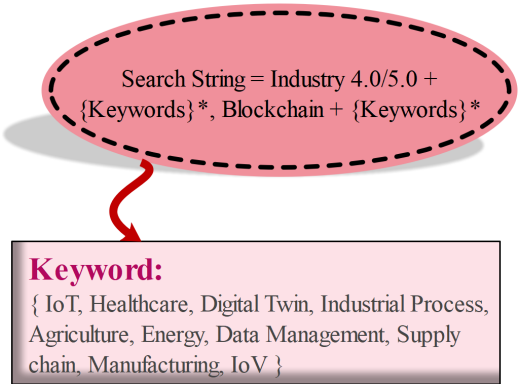


FIGURE 4: Search criteria strings

scan. Based on commonality, we narrowed it down to the final 168 articles, which are included as a part of the study.

IV. BLOCKCHAIN FOR INDUSTRY 5.0: ARCHITECTURE AND SOLUTION TAXONOMY

This section presents a proposed reference architecture of BC-assisted Industry 5.0. Based on the reference architecture, we propose the assisted solution taxonomy of BC-based Industry 5.0. Thus, the section addresses the RQ2 and RQ3, which are presented in TABLE 6. RQ2 is addressed as we discuss a holistic reference architecture of BC-enabled Industry 5.0, which is used to assure secured communication among different processes. The proposed solution taxonomy addresses RQ3 as we comprehensively discuss the applicative use-cases of BC in Industry 5.0. The details are presented as follows.

A. A PROPOSED BC-ENABLED INDUSTRY 5.0 ARCHITECTURE

In this subsection, we present the underlying technicalities of the proposed reference architecture. FIGURE 5 depicts the same. The proposed architecture considers Industry 5.0 applications like supply-chain management, personalized healthcare, smart education, manufacturing production plants, unmanned aerial vehicles (UAVs), connection with cloud, edge, and fog systems for resource management and control, and interfacing with emerging Web 3.0 architecture. We consider reliable network services at the backdrop of fifth-generation (5G) and beyond networks to assist the reference architecture. The services include enhanced mobile broadband (eMBB), ultra-reliable low latency communications (uRLLC), and massive machine-type communications (mMTC). mMTC is required for sensor-based massive control in Industry 5.0, where the collected sensor data is distributed among different decentralized applications. The stakeholders transact through decentralized applications (DApps), which can be interfaced seamlessly with SCs to automate conditions and payments via SCs. The edge services authorize the data exchanged between the user and the enterprise application. The components of the reference architecture are discussed as follows.

1) Decentralized Applications

DApps are digital applications or program that runs on a P2P BC network. A cryptographically empowered database facilitates the exchange of information. A standard application runs on a computer server owned and operated by a single organization such as Uber and Twitter, whereas DApps are autonomous and are free from the control of a central authority. It ensures users' privacy and provides flexibility to the developer. DApp can store financial transactions, personal identity, SCs, and other healthcare data. Healthcare-based DApps allow updates in the patient medical health records (MHRs), which can be updated by different healthcare stakeholders like hospitals, doctors, and drug labs, on the authorization by the patient entity. The medical practitioner makes informed decisions based on what was examined and administered before with precise accuracy.

Similarly, DApps are extremely useful in cloud, edge, and fog environments, where services can be instantiated for resource requirements. Recently, the dew computing paradigm allows for the setup of a dew virtual machine (DVM) on local computers (mobiles and laptops), which can communicate with the dew server for analytics. The dew server can periodically synchronize the local file contents with the cloud through the DApp integration. DApps are set up for specific UAV operation types in UAV-based networks, where the UAV flight parameters are communicated to the ground station through DApp. DApps can support the in-

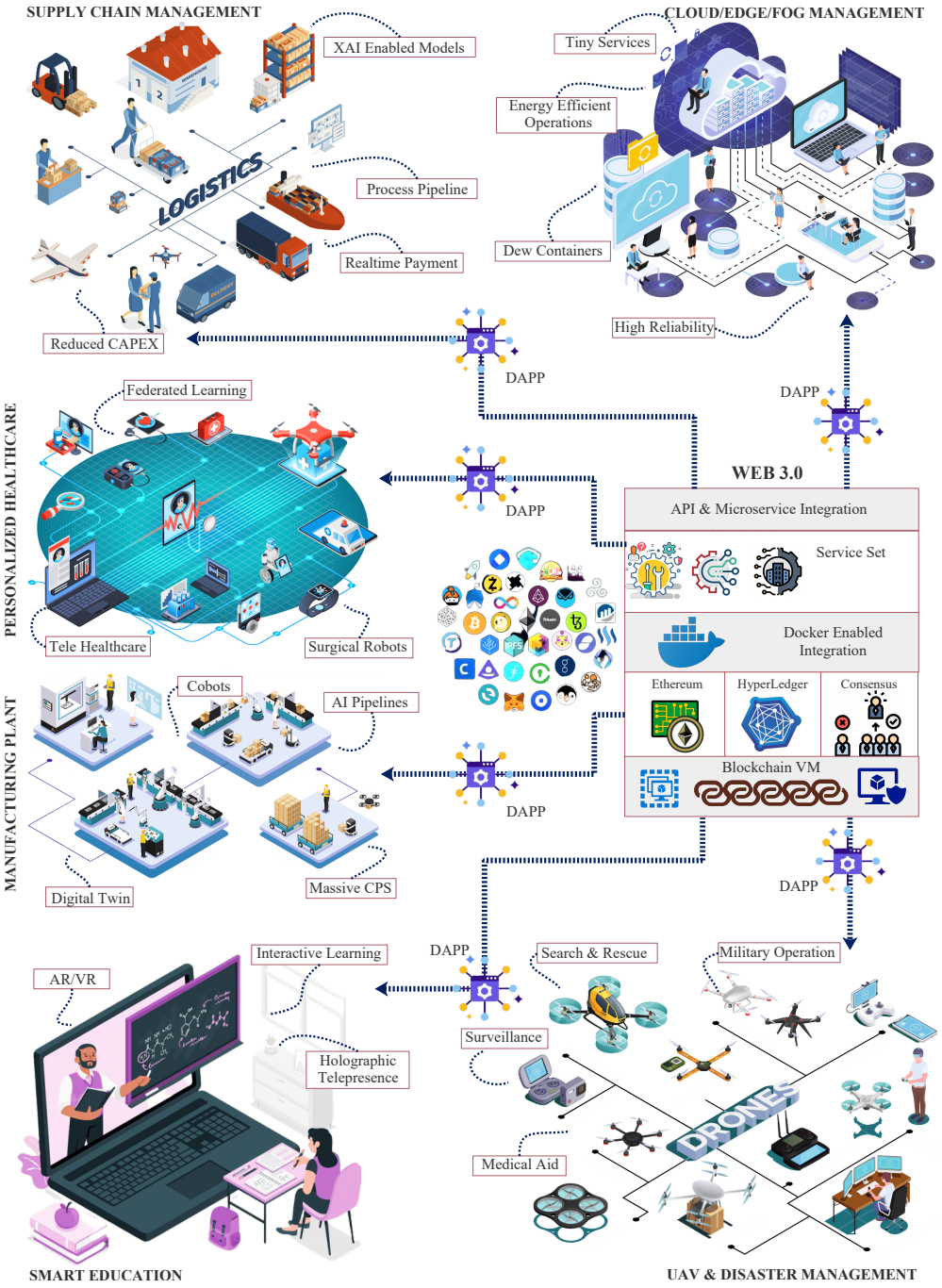


FIGURE 5: Proposed reference architecture of BC-assisted Industry 5.0 ecosystem

teractive smart Edutech sector through interactive learning and holographic telepresence of teachers via augmented and virtual reality (AR/VR), which pushes beyond the physical boundaries. DApps communicate with SCs to automate payments between different stakeholders in the process pipelines in supply-chain management. The emerging Web 3.0 architecture has close interfacing to support functionality-based DApps, based on defined service sets.

2) API and Micro-service Integration

In Industry 5.0 applications, sensors are embedded with tiny embedded controller devices with limited computing capability and power supply. Thus, effective network communication protocols are required to relay data between different nodes. Thus, the sensor nodes require a loosely coupled, independent, deployable service in heterogeneous and specifically targeted toward defined tasks. Thus, the micro-service paradigm is an integral component of Industry

5.0 that extends the communication boundaries. Microservices are tiny, lightweight, and extensible. Microservices are easily executable on small isolated Docker containers, making them ideal for edge computing. An authentication and access method is necessary to protect the microservice's confidentiality and integrity for that only authorised user has access to the service. To deliver a secure authentication stream to the organisation, a micro-service security agent is integrated with an application programming interface (API) gateway.

3) Service Sets

Based on the type of BC network, service sets are specifically created for the user requirements. Thus, it matches the vision of Industry 5.0 hyper-personalization and mass customization. Popular DApp provides services to enable secure APIs for sending continuous data streams, which can be read and interpreted via SCs. For example, a BC-based advertising service provides control and privacy of end-user data and provides service tokens to different users based on recommendation clicks, generating revenue. Decentralized credit services open the debt position against the locked stable coin such as ethereum. In banking, the know your customer (KYC) service verifies the customer's identity and streamlines the account opening process. In supply chains, services track the raw material requests, their movement to the warehouse, and the logistics control till the product reaches the marketplace.

4) Docker Enabled Integration

To run the application quickly and reliably in a decentralized computing environment, there is a need to provide a standard set of software services and their code and dependencies. Docker is a standalone and lightweight package that includes everything a software requires to run, such as system tools, settings, and environment variables. In addition, the applications running in containers are safe, as docker provides complete isolation to the services made available to organizations.

5) Blockchain and VM Layer

The collected data from different verticals are stored as transactional ledgers in the BC. In industrial setups, a permissioned BC is a preferred choice that stores the records in the form of transactions. A virtual machine (VM) is a preferred choice to deploy transactions on BC, as it makes the data independent of the intricacies of the operating system as well as acts as a decentralized computer. The BC nodes can be referred to through API calls, and to scale the transactions, the main BC is connected with different chains which are custom and application-specific. This allows high transactional throughput, and the consensus mechanism varies according to the underlying application and the network support. For example, healthcare applications can store patient medical records at local nodes, where a global model is downloaded and trained on local data. This paradigm is termed federated learning, and it allows data privacy and sanctity as local data is not shared [43]. For the COVID-19 vaccination, we can set up user identification and purchase details via SCs, and analyze the entire cold-chain process through automated service level agreements between stakeholders. Similar use-cases of BC can be related to cloud computing and manufacturing processes that employ DT control. In smart education, the online meeting meta information and the AR/VR-enabled connection status information can be stored on BC ledgers. In UAV networks, we can store the status and initial coordinates of UAV swarms in the BC, which is entered through the ground station controller. This assures that in-flight operational data has not been tampered with, and UAV swarms could safely carry out the delivery, search, and rescue operations for disaster management control [44]. Normally, developers create their DApps and test them on VM to trace the possible bugs. Once the code is tested, it can be deployed on the test network or the mainnet, which requires real cryptocurrency for executing the SCs.

6) Web 3.0-The key principles

Web 3.0 is decentralized and is mainly categorized into a three-layer architecture- the frontend application layer, the data layer, and the backend layer.

1) *The Frontend Layer*- The frontend layer is to leverage communication between the DApps and the SCs. The data of SCs is carried to the BC state ledger. The frontend is supported by third-party node providers, like Alchemy, Infura, and Quicknode. We use a lightweight exchange model via Javascript object notation (JSON) through a remote procedure call (RPC) specification. The JSON-RPC is required to communicate the front end to the BC network. It allows the frontend DApp to run from the client space but executes the functionalities on the remote machine through a driver stud on the client. The communication is normally supported through HTTP or Web socket connections. Once the DApp providers are connected to BC, the client can trace the BC state and write transactions to the BC network. The transactions are signed through the client's private key and are executed through a gas fee. Providers, such as Metamask, present the runtime environment to execute the transactions, where the low-level calls are made to the ethereum VM.
2) *The Data Layer*- As BC has limited storage capabilities, storing the entire transactional data on the main BC network is not feasible, as it would drastically reduce the network throughput. Moreover, the stored transactions incur a gas fee, and thus it is a costly affair. Thus, a viable solution is to store the data on a P2P storage network such as interplanetary file systems (IPFS) or a swarm network. IPFS is a P2P system protocol that enables users to store content that can be connected and fetched through browsers. The stored content is encrypted and can be retrieved through the IPFS key. The content metahash is stored in BC as transactions. Swarm is similar to IPFS and is accessible through the

ethereum SC. Once the data is stored on P2P storage networks, queries can be fired through the GraphQL language through the SC event handler, requiring P2P gateways for socket connection transfer.

3) *The backend layer*- At the backend, the BC network acts as a representative state machine that maintains the program state and validates the contract rules. Once the contract is executed, the consensus protocol of the BC network is called, and the validation is done through the miners or validator nodes. The backend logic supports the interaction of the SC data through different databases such as NoSQL through a server-side application. In cloud applications, a serverless approach is also used. The connectivity to the database is managed through API calls made by popular backend languages like NodeJS, C#, GO, Python, and Ruby. For big-data analytics, the frontend can connect to MongoDB, Cassandra, FlockDB, and Neo4J.

7) Industry 5.0 verticals

This subsection discusses the different Industry 5.0 verticals and associated components that interact with the BC network with the Web 3.0 service. The details are presented as follows.

1) *Supply-Chain Management*- In a supply-chain ecosystem, Industry 5.0 defines AI-driven pipelines, where the genuineness, quality and expiration of the manufactured product are monitored. Through a DApp, any supply-chain stakeholder can place custom orders. The orders and delivery conditions between two transacting peers are executed through SCs, the system wallet blocks the currency before the final trade, and once the product is delivered, SC is executed to facilitate the real-time payments. Thus, it reduces capital expenditure (CAPEX) and simplifies the logistics cycle. In healthcare-based supply chains, prediction models are critical, where the model results should be interpretable. With the rise of Explainable AI (XAI), an explainable module has been added to the supply-chain ecosystem that explains the model results.
2) *Personalized Healthcare*- In Industry 5.0, the healthcare sector is on the rise. Recent use-cases include telehealth and telesurgery, where remote surgery is performed through specialized cobots. The cobot and the surgeon are connected through a responsive network, such as tactile internet, with a low latency of < 1 ms. Healthcare informatics with the use of AI and ML has evolved much in the same line, federated learning is an emerging paradigm that allows global cloud models trained with local data without exchanging any sensitive information. The local system only shares gradients and weights of the parameter.
3) *Manufacturing Plant*- In manufacturing systems, cobots would assist humans in repetitive tasks. Automation would be a critical component in manufacturing plants, combining industrial processes, control, and systems to form a massive CPS. The pipelines would become more intelligent and AI-driven, where the raw product packaging and control data would be monitored. To ensure the safety of plant operations, the machinery inputs would be first simulated on a DT control, which would be an emulation of the real physical process. The DT outputs would be sent as feedback to the AI models, and the manufacturing processes would become intelligent. Once sufficient iterations are completed and errors are minimized, the inputs will be fed to the real processes. This would assure safety and high precision in manufacturing.
4) *Smart Education*- At present, real-time BC-enabled use-cases in the education industry include the storage of student credentials, mark sheets, and credit transfers between different universities [45]. However, with the rising wave of the COVID-19 pandemic, online teaching-learning is supported through online meeting platforms such as Zoom, Cisco Webex, and Microsoft Teams. In industry 5.0, smart education would be more innovative, where there would be a blended mix of teaching through an assisted environment. For example, AR/VR-enabled remote labs would be set up to allow students to feel the real experiment from a remote location. However, it would require high networking bandwidth and low latency in communications. Recently, 6G networks are proposed which envision holographic telepresence that can portray real-time, three-dimensional (3D) images of a remote person in the student living room environment, where the virtual image would interact and interplay with physical objects in its nearby environment. The images would be captured and rendered with nearby objects, compressed, and transmitted over a responsive service, such as FeMBB in 6G. Then, they would be decompressed and projected using laser beams in the living environment. However, as the confidential data is shared over open channels, BC ledgers would maintain the hologram state so that the environment sequence has not been tampered with.
5) *UAV and Disaster Management*- At the UAV front in Industry 5.0, services like medical aid [46], search and rescue, military operations through sensor-driven battlefield networks, and surveillance operations would be supported. BC would assist that UAV swarm networks are not intercepted and malicious UAVs are not able to disrupt the communication in the entire network [47]. A similar use case also exists in the Internet-of-Vehicles (IoV) scenario, where the confidential data of the vehicular nodes are stored on BC ledgers [48]. For example, electric vehicles (EVs) can communicate with peer EVs to share energy in a P2P manner [49], or the charging stations, and the transactional data is maintained in BC ledgers as immutable and chronological records. Zuhair *et al.* [50] proposed a UAV-based BC-assisted scheme, named as *BloCoV6*, that proposed a massive surveillance and contact tracing framework for the COVID-

19 pandemic. The scheme is proposed on 6G services that allow low latency in surveillance operations of UAV swarms, where a real-time object detection process in densely populated regions is constructed, and the contract tracing ledgers are updated for persons in close proximity of infected persons. The architecture used UAVs to orchestrate mass-level surveillance operations. However, the authors failed to discuss the consensus process that manages the COVID-19 BC ledger, as the contact tracing data is humongous. Thus the BC scalability is limited for the practical use case.

6) *Cloud/Edge/Fog Computing*- In Industry 5.0, massive data would be exchanged, and thus enterprises would rely on cloud, fog, and edge computing infrastructures to provide resources, storage, and network to host their applications. On a pay-per-usage policy, cloud computing models mainly provide software, infrastructure, and platforms as service models. Recently, industrial IoT applications require low latency and stable connection bandwidth and thus resource management and processing should be supported at multiple and distributed work nodes. Thus, the edge computing paradigm allows processing at local edges, where complex tasks are broken down into tiny subtasks and are assigned to local nodes. These local nodes assist tiny service operations, which reduces communication latency. Edge computing assures high reliability in industrial systems. A close technique, fog computing extends the cloud computing model and services at the network edge and provides service to end-users with high mobility. The services are normally hosted on access points in the fog network. This reduces the overall servicing latency of applications and is suitable for real-time embedded control systems. Another approach, termed dew computing, allows an on-demand premise setup of associated software, services, and hardware on a local device itself. Thus, it allows the devices to work offline without connecting to the cloud server. An instance of the dew server runs on the local device, which connects to the cloud server, and synchronizes its contents once it is online. A popular example of dew computing is Dropbox, which stores a local dew machine on the system that synchronizes the file contents when the system is online and connected to the cloud dropbox server. To support the operations of dew computing, tiny microcontainers are set up which are isolated and independent of other application services. ML-based container orchestration has recently been set up for distributed applications for autoscaling system infrastructures and managing diverse workflows. In such cases, ML-based prediction models are applied that improve the resource provisioning of containers, and improve the end-user quality-of-experience [51].

B. SOLUTION TAXONOMY OF BC APPLICATIONS IN INDUSTRY 5.0 VERTICALS

Based on the proposed architecture, this subsection outlines the solution taxonomy of BC-assisted Industry 5.0 in different applications. FIGURE 6 presents the solution taxonomy. We now follow an in-depth discussion on the same.

1) Smart City

Smart cities strive to promote a sustainable lifestyle by creating a greener, safer urban environment and therefore realize the sustainable vision of Industry 5.0. The futurists have already begun exploring Industry 5.0 to incorporate a human feel or personalization through co-working and between robots and humans. Various smart gadgets deploy heterogeneous sensors to collect data in smart cities. Data from these sensors are analyzed and used to improve the functioning of traffic and transportation systems and schools and libraries. Due to greater usage of IoT devices, the notion of a smart city has gained prominence, and it integrates big data, AI, and assisted networking technologies. The confluence has resulted in advanced IoT paradigms, termed as Internet-of-Everything (IoE). We need effective procedures to create further smart cities to solve the existing energy, transportation, environmental, governance, and concerns. To successfully and efficiently deploy smart city projects, some unresolved challenges such as inadequate security in IoT, difficulty maintaining and upgrading equipment, preserving user confidence, optimizing data centre costs, damage resistance, security, and privacy must be addressed. BC technology [52] can solve all of these issues, making it ideal for constructing smart city solutions.

In smart cities, energy management is a critical concern. Moreover, an adversary can tamper with energy data from smart grids. BC alleviates the challenges of big data control and energy management in the grid, and IoT environment [53], [54]. This study examined concerns such as user credibility, data accountability in the central database, and data privacy protection. BC mitigates the entry of malicious nodes and rogue access points in the ecosystem. Authors in [55] proposed a BC-based decentralized database with boosted storage and computation capability with assisted data privacy in IoT. The proposed technique effectively avoided numerous assaults on network infrastructure. Sharma *et al.* [56] examined the potential challenges on smart city network architecture. Due to the exponential growth in data volume and linked IoT devices, existing smart city frameworks face bandwidth, security, latency, and scalability difficulties. To solve these difficulties, they developed a hybrid smart city architecture. The hybrid architectural scheme divides it into two parts, namely, the core and the edge. This architecture was designed to combine the best of both worlds, i.e., the distributed and centralized designs. The authors of this study proposed the PoW strategy to increase privacy and simulated the suggested model to assess its viability and performance in terms of latency and throughput. An integration of BC and software-defined networking (SDN) based network architecture was

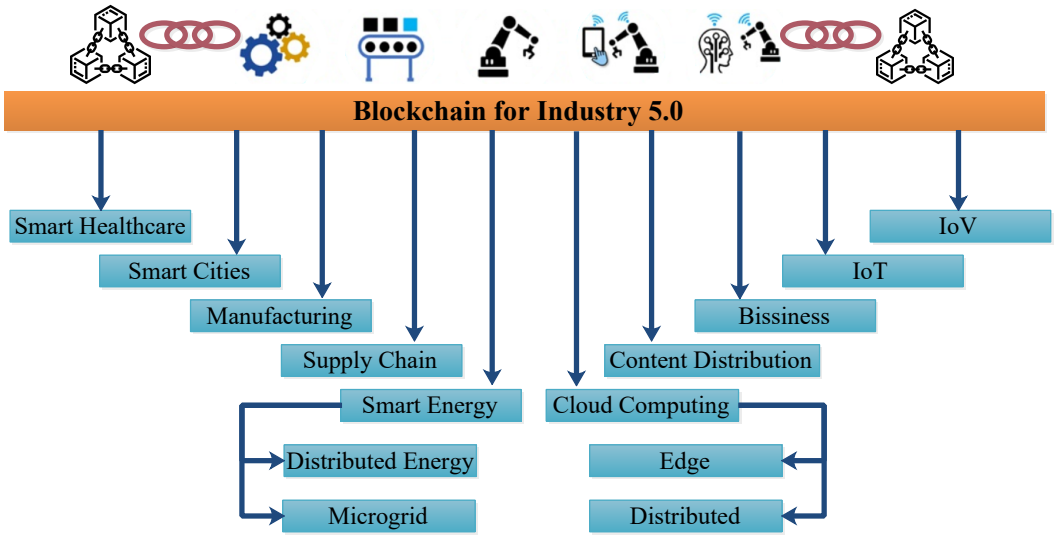


FIGURE 6: Taxonomy of BC Applications in Industry 5.0

proposed, but critical aspects like how to deploy edge nodes and allow caching at edge nodes were ignored. This research gap opens up a lot of potential future work in this area.

Biswas *et al.* [57] presented a four-layer decentralized BC security approach, with the four layers as physical, database, communication, and interface. They integrated smart devices and created a secure and reliable communication mechanism for smart cities. Multiple smart device standards were created for the physical layer to share and integrate data. The communication layer utilizes BC protocols to offer anonymity and security of sent data. Many real-time applications such as smart parking, house cleaning, and road traffic management systems could benefit from widespread usage of the private ledger [58]. This framework scalability is also nice for real setups, and the suggested model has high degrees of fault tolerance, capability, reliability, and speed. The limitation of the paper is that they have not focused on the scalability and the interoperability issues.

Rivera *et al.* [59] described smart city architecture as a digital hub that connects government, schools, universities, and the economy [60]. The paper focused on modern corporate and smart city scenarios, where the user identity is paramount. The authors established that user identity and security are paramount for Industry 5.0, which aligns with human-centric development. Digital identification is key in securing networked devices in a smart city. However, important topics that include architecture, smart energy, and SDN-based security were not addressed. Liao *et al.* [61] concentrated on the interoperability and transparency of services in the smart city. The authors presented a fair and transparent ecosystem with limited openness toward data transfer. The authors proposed a lottery-based incentive system and a BC-based smart city lottery system. The scheme is named *FairLotto*, a three-layered BC-based lottery system with four lightweight protocols. The suggested system included four stages, namely, close-time, purchase, initialization, and validating winning numbers. This four-layered architecture ensured that every player had an equal chance of winning. No financial transactions were stored in the BC in the *FairLotto* system. This ensured transactional privacy and fairness in the lottery system. The authors did not discuss the networking aspects of the scheme, and the paper lacked connectivity and service integration. Also, the experimental parameters for designing the scheme are not discussed.

2) Smart Healthcare

Industry 4.0 facilitated mass customization, but personalization and human feel are required in the healthcare industry. Thus, a paradigm shift is required from mass customization to mass personalization to cater to the specific requirements of the patients through the healthcare providers. FIGURE 7 presented the key visions of BC-assisted healthcare applications. As we shift towards Healthcare 5.0, the interaction between doctors, hospitals, and associated stakeholders would improve, which would enable quality of experience for the patient. In healthcare 4.0, the focus is on analytics-driven from patient records, but the analytics is mostly centralized on healthcare clouds. With rising decentralization, the analytics would shift towards local edge models, and thus, patient data privacy and security must be protected as it is exposed to various threats [62].

Thus, smart healthcare is oriented towards sensor-assisted body area networks, where the local nodes would monitor the patient's health and collect the data. Doctors, patients, and medics should have secure and authorized access to healthcare records. Secure data transfer is critical for decisions such as designing new hospital services, recommending doctors, studying symptoms of various diseases, and enhancing the overall model.

TABLE 7 compares the latest healthcare security standards

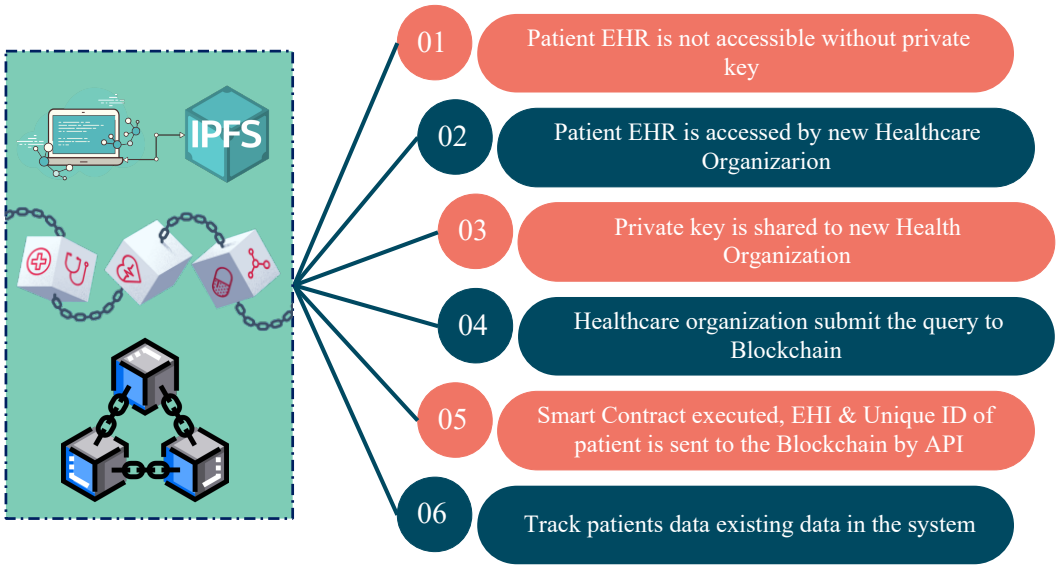


FIGURE 7: BC-assisted Healthcare ecosystems

utilized in smart healthcare. These standards are compared based on access control, security maturity, cost and complexity reduction, and healthcare compliance. Patient data must be supplied frequently for medical research, treatment decisions, and disease symptom analysis. Traditional access control policies do not safeguard the transfer of extremely sensitive healthcare documents. Moreover, patients rarely communicate their medical histories with clinicians [63]. In an emergency, the patients' medical records are required but are often unavailable due to inadequate record-keeping. Smart healthcare is based on the massive collection and distribution of electronic health records (EHRs), and the EHRs are stored as transaction ledgers in the BC network on healthcare clouds, or edge nodes, with proper authorization policies. The fundamental challenge in the health industry is enabling privacy and confidentiality on patient-sensitive attributes, which should not be disclosed, and maintaining the data availability for supervised analytics. BC can facilitate smart healthcare for patients, doctors, hospitals, and insurance companies.

In recent studies, authors in [64] proposed a healthcare data gateway (HDG) on a BC-based intelligent application framework. HDG is a secure data gateway that allows patients to share and control their data. It processes and manages patient data anonymously. HDG has three layers, namely, the utilization, management, and storage layers. The data utilization layer includes physicians, businesses, governments, and researchers. HDGs are connected to the data management layer. This layer also controls patient data, indices, and schema. The storage layer provides secure and scalable storage, ensuring confidentiality and integrity to the healthcare system. Azaria *et al.* [65] created a decentralized healthcare scheme termed as *MedRec* for large-scale EHR data management. This scheme used a BC-based transaction model which guarantees the confidentiality, accountability, and authentication of health records. The authors in [78] created a dependable healthcare system based on pervasive social networks (PSNs) and a variety of protocols. The protocol mentioned first is an upgraded version of IEEE *02.15.6* protocol that shows authentic associations. It was used to establish secure connections between mobile devices and resource-constrained sensor nodes by imposing uneven computational requirements on mobile devices and sensor nodes. The second protocol is designed on BC and is used to exchange verified data through the PSN nodes. The authors evaluated the performance by examining the recommended procedures and other parameters. The suggested solution exemplified the utility of BC technology, particularly for PSN-based applications. However, the suggested system's performance was not evaluated on a large-scale PSN-based system. Furthermore, as highlighted by the authors, the proposed system performance might be enhanced in terms of transport and environmental monitoring [79]. The authors of [80] debated a point of view about a BC-based healthcare database management for selecting and inserting items. Additionally, they provided a structure for sharing and maintaining electronic medical records (EMRs), particularly for cancer patients. The suggested architecture featured both a front-end and a back-end. The back-end was composed of membership services, a certification authority, node clusters, a load balancer, and different cloud storage for patient certificates and data. This reduces the turn-around time for sharing medical records and empowers the decision-making skill of the involved authority for better medical treatment. Additionally, the suggested system ensured the availability, privacy, security, and access management of EMR data. Author in [81] created a BC-based framework *MeDShare*, which is designed to manage large amounts of medical data in the cloud using big data,

TABLE 7: Existing research on BC-assisted Healthcare vertical of Industry 5.0 ecosystem

Author	Year	Objective	1	2	3	4	5	6	7	8	Pros	Cons
[66]	2018	An attribute-based BC system to protect the EHRs.	X	✓	✓	✓	✓	✓	✓	✓	Identity-based encryption assures traceability and integrity of the data in the database	Does not provide the implementation and deployment.
[30]	2018	To investigate the potential applications of BC technology in the medical network	X	✓	✓	✓	✓	✓	X	X	Database encryption based on user identity, and ensures the integrity and traceability ensured	Data accessibility and scalability is not addressed.
[67]	2018	Proposed a attribute based secure signature scheme for the use of EHRs for different authorities.	X	✓	✓	✓	✓	X	✓	✓	Immutability of the information ledger	Interoperability and privacy are not discussed.
[68]	2018	To investigate the usability of BC in heterogeneous healthcare data stored in the cloud.	✓	✓	✓	✓	✓	✓	✓	X	P2P network, database decentralization, and cryptographic security	Traditional data storage in data warehouse.
[69]	2018	To create a smart contract based healthcare system with the purpose of enabling safe automated remote patient monitoring.	X	✓	✓	✓	✓	✓	✓	X	A ledger based on hashes, a P2P network	Delay in the response due to large scale key management.
[70]	2018	To investigate the possibility of continuous patient monitoring using patient-centric agents.	✓	X	✓	✓	✓	✓	✓	X	Encryption and authentication that are both lightweight and tamper-proof, as well as protection against single points of failure	High and variable end-to-end delay.
[71]	2018	To investigate the feasibility of decentralizing attribute-based signatures in healthcare through BC.	X	✓	✓	✓	✓	✓	✓	✓	Secure exchange of large-scale and dispersed EHRs, and provide anonymity	Scalability and robustness of the scheme.
[72]	2019	Examines current BC technology in healthcare sectors and evaluates their advantages and disadvantages.	✓	✓	✓	X	✓	✓	✓	✓	Analyzed the potentials of BC in healthcare domain	Does not discussed privacy issues in storage of health records.
[73]	2019	Integrating BC technology and deep learning to protect EHRs	✓	✓	X	✓	✓	✓	✓	✓	Signature based schemes to protect collusion attacks.	Higher communication cost due to lattice cryptosystem.
[74]	2020	To explore the applications in health sector and framework of future implementation of architecture with security compliance	✓	X	✓	✓	✓	X	✓	✓	Evaluated the gaps and implications of BC to improvise healthcare industry.	Issues with data integrity and encryption is minimal
[75]	2021	Evaluation of existing model and its implementation of healthcare based on PRISMA framework	✓	✓	✓	X	✓	✓	X	✓	Security, privacy, cost and performance are discussed in a comparative way	Simulation related information and data sharing mechanism
[76]	2021	EHR system based on off chain medical data storage with implementation of SC	✓	✓	✓	X	✓	X	✓	X	Decentralized architecture and robust system for medical data	automation of health diagnostic and decision-making system
[77]	2022	SC-based patient health management having modified Merkle tree and immutable log	✓	✓	✓	✓	✓	X	✓	X	Security and integrity through hash functions	process of real-time implementation

1. Architecture, 2. Data integrity, 3. Medical data sharing, 4. Access control, 5. Distributed electronic health records, 6. The patient encryption key, 7. Simulation tool/ Framework, 8. The algorithm, ✓ - shows the parameter is considered, *X*- shows the parameter is not considered.

information transfer and shared stored securely. The authors concluded that cloud service providers might achieve auditing and data provenance using the *MeDShare* by comparing its performance to conventional data sharing methods. The proposed solution also decreased privacy risks. However, data interoperability, scalability, and key management were not addressed. Rifi *et al.* [82] explored crucial issues like interoperability and scalability and the benefits of using BC technology for medical data transmission.

Liang *et al.* [83] addressed privacy and identity management through a BC channel construction and membership service. They also presented a mobile-controlled hyperledger fabric architecture with permissioned BCs. The suggested effort focused on validating network nodes and preserving healthcare data. Magyar *et al.* [84] developed a BC-based information paradigm. This model incorporated complex electronic health data (EHD). Using cryptographic techniques and BC, they enabled the creation of a decentralized and disposable network. The model was created based on the American health insurance portability and accountability act (HIPAA) regulations. The authors did not present any methodology or method to manage EHD-related concerns such as security, integrity, and portable user ownership of data. Individuals and hospitals produce vast amounts of healthcare-related data every day, and Jiang *et al.* [13] exploited the features to assure data confidentiality, privacy, and integrity of health records. The authors designed a BC-based model to exchange health-related information. This system considered personal healthcare data and computerized medical records. They studied several methods and requirements for sharing and storing healthcare data. The framework used two loosely coupled BCs, one for electronic medical records (EMR), and the other for data.

Various chain verification and storage approaches were incorporated to ensure authenticity and privacy. Also, the authors created two transaction packaging algorithms, *TP&FAIR* and *FAIR-FIRST*, for *PHRD-Chain* and *EMR-Chain*. The *BlocHIE* framework was used to compare the two packing algorithms, throughput, and fairness. The author in [85] suggested that health data can be utilized for further research and innovation in healthcare. The authors of [85] proposed a new architecture on BC to secure permission for

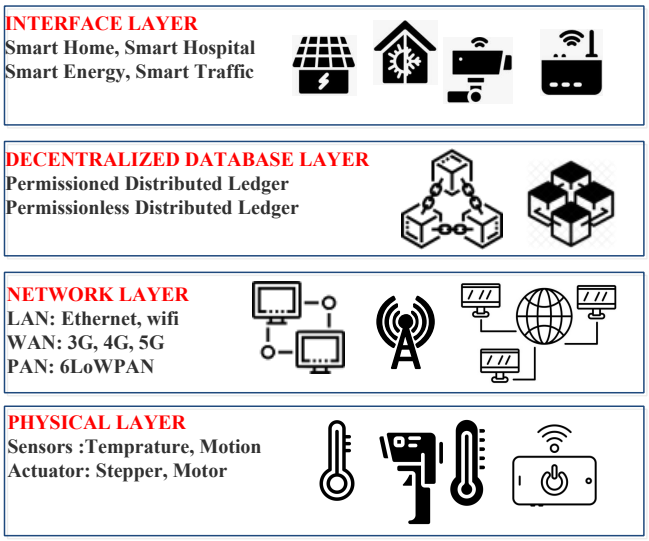


FIGURE 8: A layered IoT reference architecture for Industry 5.0

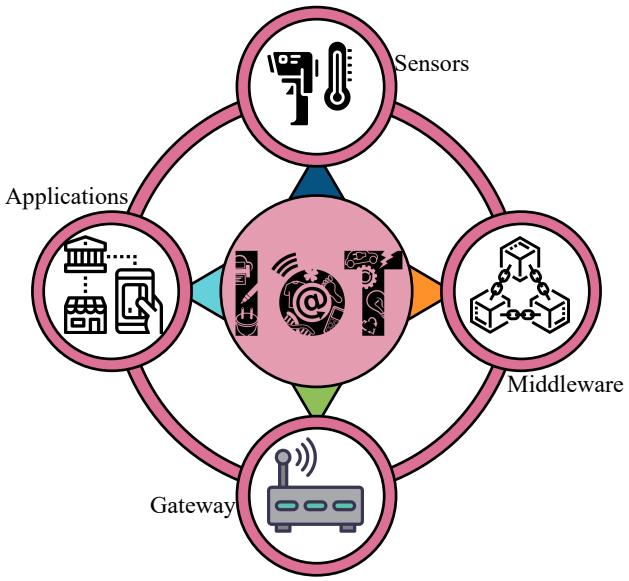


FIGURE 9: Components of IoT architecture

data management sharing in the healthcare business. Three layers were devised- a web platform, a cloud middleware platform, and a BC network. As demonstrated in work, this design has the potential to enhance security and integrity significantly. The *KONFIDO* project used this model to test parameters, including interoperability and data exchange. The authors claim the proposed methodology improved patient anonymity, process automation, auditing, data integrity, and accountability.

3) Internet-of-Things

In Industry 4.0, there is a deep interconnection between IoT nodes and AI to train the data collected from the sensor nodes. With the shift towards Industry 5.0, the sensors would be intelligent and learn from nearby environments. FIGURE 8 presents a layered reference architecture of IoT in Industry 5.0 ecosystem. The physical layer would be sensor-enabled communication, which would communicate through IoT network protocols like 6lowPAN, Zigbee, HART, and other protocols over the WiFi, Bluetooth, and cellular networks like 5G or beyond networks. There is a decentralized layer to store the sensor data as BC transaction ledgers for security. A permissioned or permissionless consensus approach is presented based on application requirements. Finally, we connect to applications at the interface layer.

Industry 5.0 is based on accessibility and communication between humans and machines. IoT technology would enable easier and more comprehensive machine access. Due to this, IoT would allow robotic systems to be useful human collaborators. When this type of cooperation is available, it makes facilities more efficient. Industry 5.0 combines human workers' flexibility with robotics speed and accuracy. This movement would be impossible without IoT connectivity. IoT connects various devices to the internet to share information and perform tasks such as measuring humidity, temperature, and moving shafts. Using IoT, correct information can be delivered to the targeted people at the right time.

Sensors continuously collect data that can be used to make effective decisions. The number of devices connected to the internet is expected to reach 50 billion shortly, which necessitates a new approach to the design and integration of these devices to provide a future-proof delivery network. IoT architecture is the backbone of any application. It should be carefully crafted to meet evolving functional, scalability, availability, and maintainability requirements. FIGURE 9 presents a layered reference architecture of IoT-driven Industry 5.0 system. Security would be a central driving force in the IoT ecosystems. Nowadays, most IoT sensor devices are insecure and easily hackable. The devices have limited computational memory, network, and storage capacity. These features make such devices more vulnerable to attacks than a traditional computer. Samaniego *et al.* [86] proposed that cloud-centric IoT systems caused network latency issues. They created virtual resources (VR) to solve these issues, presenting a software-defined IoT management construct. Decentralized, tamper-proof BCs solve the IoT security issues. One of the key challenges in integrating BC in IoT networks is service hosting. As edge devices have limited computational and bandwidth, they can be hosted by fog, or cloud [87]. Authors in [88] examined and categorized key IoT security obstacles and demands. Lesser-known solutions were tabularized and compared. To address the future research issues, the authors suggested integrating BC as a key solution to provide reliable, scalable, and efficient security solutions for the IoT.

Singh *et al.* [89] concluded that the existing security methods cannot protect IoT applications from business-related

cyber-attacks. They also proposed three different BC-based IoT security patterns. Numerous distributed ledger technologies, such as ethereum, hyperledger fabric, and IOTA, are appropriate for IoT deployment [90]. The article examined the performance of different protocols for developing IoT applications. Additionally, the authors provided three designs. As a result, the designs enhanced network security and decreased network traffic. The difficulty with these designs is that they are limited in monitoring IoT device transactions automatically. Using ethereum and a computing platform, Huh *et al.* [91] developed a novel method for managing IoT devices. They suggested three SCs that would track meter readings and preserve light bulb and air - conditioners values using public keys and signatures. The computer systems, air-conditioners, and light bulbs can identify and ignore harmful assaults on the network, monitored and detected via the proposed SCs. However, the paper did not address attack vectors such as denial of service and data synchronization. Additionally, the suggested technique addressed only a tiny proportion of IoT devices, preventing the implementation of a scalable multi-device IoT system. Liao *et al.* [61] investigated the design and architectural problems for IoT services based on BC technology. There were no detrimental consequences on architectural qualities such as robustness, efficiency, or security. Storage capacity and Scalability, anonymity and data privacy, and consensus methods are examined by Reyna *et al.* [92]. They recognized the advantages of BC technology for IoT and proposed several integration topologies. Additionally, the study explored how to leverage BC to boost the performance and practicality of IoT applications.

4) Smart Manufacturing

Industry 5.0, in general, focuses on reinstating the "human touch" into contemporary production processes and technologies. While the third industrial revolution was concerned with mass production, the fourth with mass customization and efficiency, and the fifth was concerned with personalized or creative production. It's the ideal fit for applications or services that benefit from a tailored and human touch. Fashion and clothing development is an excellent example of Industry 5.0 advancements. Human intelligence will collaborate with cognitive computing to create higher-value-added products and services. Industry 5.0 would enable customers to mass customize their orders. Consider the possibility of buyers customizing shoes or apparel — picking colours, styles, and materials — before production. This process encompasses asset management, operations management, intelligent manufacturing, planning and the human-machine interaction. According to Li *et al.*, [93], IoT has made conventional manufacturing operations turn into smart manufacturing processes, which are more efficient than cloud manufacturing. As a result, most manufacturing organizations have invested millions of dollars in IoT applications. By 2020, 40 Billion people would be using IoT in manufacturing and logistics [94]. These benefits include increased energy efficiency, predictive maintenance, improved product quality and reduced downtime. IoT has several use-cases in manufacturing operations [95]. As we all know, energy is one of the highest costs in production, so achieving energy efficiency through IoT-centered smart manufacturing is critical.

Authors in [96] proposed a prototype of a decentralized, trustworthy scheme *FabRec* that connected physical devices and computed nodes. Audit trails ensured transparency in this prototype. In the decentralized network, the authors created SCs to allow nodes to interact without human intervention. The suggested architecture enables smart manufacturing by linking nodes and physical devices. This centralized network faces security and availability issues. To solve these issues, authors of [93] created a prototype *BVmfg*, which is a distributed network architecture based on BC technology. This five-tier design fosters trust between users and service providers to facilitate secure service sharing. The authors evaluated *BVmfg* performance on 15 end-users and 5 service providers, with a particular emphasis on security and scalability. The authors then enhanced their prototype to also include data exchange from the shop floor and machines [97]. The authors used a BC network for service providers and retailers to capture essential data. The new prototype built a level 2 P2P network using a BC. It addressed cloud manufacturing security and centralization successfully.

Authors in [93] suggested an injection mould redesign information-sharing system based on a BC with four layers. This study established the rules and criteria for securing the system in a trusted setting. It also allowed owners to share data and assets among themselves securely. The search efficiency is improved with the help of k-nearest neighbour retrieval. The proposed paradigm was limited to some applications and incomplete to others. According to [98], the OMNeT++ simulator was used to assess industrial network needs such as scalability and flexibility. To evaluate existing BC-based manufacturing systems. TABLE 8 examines the usage of BC in smart industry verticals that include digital payments, business models, and smart manufacturing criteria, with a discussion on associated benefits and potential limitations.

5) Robotics

There are many other perspectives and important technologies of Industry 5.0, one of which is Swarm Robotics. Robotics is crucial for Industry 5.0 operations, as they would work cooperatively with each other in manufacturing industries or warehouses. Another application of swarm robotics is in self-driving cars. Keeping in mind the steep change in the trend of automatic driving, it won't be unrealistic to expect completely self-driving cars to be a new normal. Furthermore, it will be interesting to speculate how long it will take before computers are declared superior to humans in driving. Keeping this in mind, swarm robotics can help solve the problem of traffic jams and even eliminate the need for traffic signals [109]. Eduardo Castelló Ferrer explains how merging BC technology and other distributed systems, like a robotic swarm, improves the security, autonomy, flexibility,

TABLE 8: BC-assisted smart manufacturing business in Industry 5.0

Author	Year	Objective	1	2	3	4	5	6	7	Pros	Cons
[99]	2017	Analysed the cost of using BC in different business model	✓	✓	✓	✓	✓	✓	X	Computational cost model of ethereum	High transaction cost.
[100]	2017	Discussed adoption and development of BC for government sector.	✓	✓	✓	X	✓	✓	✓	Explored design aspects of domain-specific BC	Failed to detect fraud in incentive distribution.
[101]	2018	To develop an inter-bank payment system on BC for commercial purpose.	✓	✓	✓	✓	✓	✓	✓	Prototype support gridlock solution and gross settlement	Higher cost due to centralization
[102]	2018	To safeguard the execution of sensitive business processes on the BC	✓	✓	✓	✓	✓	✓	X	Trust, transparency, and accountability in business model	Not mentioned confidentiality and privacy.
[103]	2018	To manage organization processes with the use of BC technology	✓	✓	✓	X	✓	✓	✓	There is no point of failure of the system	Not mentioned Latency, throughput and bandwidth of the approach
[104]	2018	To improve the transparency of corporate processes using BC technology	✓	✓	✓	✓	X	✓	X	Distributed database, traceability and immutability	Transparency in food supplychain
[105]	2018	To implement a BC-based smart cooperation for business process	✓	✓	✓	✓	✓	✓	X	Smart contracts, collaborations and secure Authentication	High Latency Traffic
[31]	2018	To conduct an examination of the commercial uses of BC technology	✓	✓	✓	✓	✓	X	✓	Smart collaboration, authentication	Implimentation complexity
[106]	2019	To conduct an investigation into the commercial uses of BC technology	✓	✓	✓	✓	✓	✓	X	Transparency	Privacy of data is not considered.
[107]	2020	A secure biometric based authentication scheme for UAVs is presented	X	✓	✓	✓	X	✓	X	Identity registration of UAVs is based on random oracles, which ensures diffusion in registration functions	A lightweight security module is not discussed owing to computational UAV requirements.
[108]	2022	An integration of BC and federated learning for vehicular ecosystems to assure privacy of vehicle data	X	✓	✓	✓	✓	X	✓	Federated offloading model is proposed that sends the local updates to global server in a lightweight manner	Security cost analysis is not presented

1 : Business process service 2 : Trust management 3 : Security 4 : Architecture 5 : Consensus transaction mechanism 6 : Cost model 7 : Monetary policy

and profitability of robotic swarm operations [110]. The article highlights how BC technology is utilized to solve four emergent problems in swarm robotics research. The authors describe novel security, decision-making, behaviour distinction, and commercial models for swarm robotic systems through case studies and examples. Finally, the limits and potential future difficulties associated with combining these two approaches are explored.

Authors of [110] study a specific aspect of swarm robotics. They propose that while swarm robotics systems are typically touted as fault-tolerant, research has focused on controlled laboratory conditions, ignoring security challenges posed by Byzantine robots or robots that act arbitrarily defective or maliciously. With swarm coordination systems failing, one or more Byzantine robots may be sufficient in many situations. A BC-based security management solution for swarm robotics systems is demonstrated in their work. Their technique employs decentralized BC-based SCs to ensure swarm coordination and identify and exclude Byzantine swarm members. We contrasted the BC-based strategy's performance in a collective decision-making scenario with and without Byzantine robots and with an existing collective decision technique. When Byzantine robots are part of the swarm, the results reveal a clear advantage of BC.

6) Cloud Computing

This section brings the reader's attention to decentralized edge-computing models proposed by researchers globally. On the other hand, a parallel technology known as mobile edge computing (MEC) has emerged that has a variety of uses in distributed networks [111]. According to the authors, its primary benefit is that it accelerates pf processes over the networks. However, like with BC, edge computing has drawbacks[112].In addition, its security and management mechanisms have been deemed deficient. As a result, the concept was born to connect the two technologies and leverage their respective capabilities. Combining the two would result in powerful network servers, massive data storage, and enhanced transaction security. However, the integration would be more effective if certain precautions were taken. For instance, there is a requirement to address scalability, resource management, and system security in the proposed approaches. To address the integration issue, this article presents a decentralized BC-based MEC paradigm is proposed.

7) Internet of Vehicles

With technical advancements in the automobile sector, vehicles have shifted towards renewable sources of fuel consumption to reduce their carbon footprints. Businesses continue to place a higher premium on their automobiles than on the environment they run. Nonetheless, the advent of BC as a feasible means of data storage and communication is a positive development. Fostering settings that permit two-way communication between automobiles and their supporting infrastructure is crucial to guarantee the successful implementation of autonomous vehicles. Although the IoT and smart cities have aided in this progress, BC technology represents a huge step forward that has the potential to change the future of driving.

One of the biggest barriers to autonomous automobiles becoming more usable in real scenarios is their resilience and connectivity with the external entities. The autonomous vehicles are equipped with sensors and are network controlled, where they communicate through controller area networks (CAN), and local area interconnect (LIN) environ-

ments. However, in road scenarios, the network has to be responsive to support massive data exchange over vehicle-to-vehicle (V2V), vehicle-to-roadside units (V2R), and vehicle-to-infrastructure (V2I) links. Recently, with the advent of 5G and 6G services [113], the links are capable of supporting and processing massive amounts of data per second, but they must do it independently and in isolation. This functionality is substantially enhanced by utilizing IoT devices to gather and communicate crucial contextual data to automobiles to optimize their performance. This should include driving conditions, vehicle accidents, and other cars on the road, all of which may affect a vehicle's power to navigate. In reality, IoT devices continue to be restricted by the limitations of existing technology. Centralization exposes data to danger, and the difficulty of data to be swiftly transferred between locations diminishes its value in real-time circumstances. However, BC can transform the existing state of affairs considerably.

In Internet-of-Vehicles (IoV) scenarios, the key advantage of BC inclusion is trust among the communicating vehicles and authorization of owner identities. In IoV, both certificate and certificate-based registrations are considered for owner identity management. Automated vehicles must maintain a continual awareness of three important variables: the road driving conditions, vehicle position, and the location of roadside units and other vehicles. BC also facilitates energy trading among autonomous vehicles in a trusted manner, as the records are stored as immutable and chronological ledgers. Businesses have already implemented enhanced vehicle monitoring and communication to increase overall connectedness. Developing decentralized networks capable of more smoothly transferring data among nodes is the first step in developing a secure driverless environment. Around 14% of drivers would feel confident riding in a self-driving car, as per the American Automobile Association's (AAA) annual automated vehicle study for 2021 [114].

To streamline transactions among vehicles, microtransactions play an important role. They streamline transactional flow among vehicular entities and support the surrounding infrastructure. They increase the communication bandwidth as services are tiny and require low power consumption. In V2V links, the vehicle owners pay for specific prices through cryptocurrency tokens over DApp. Basic services might include weather forecasts, gas costs, lane congestion statistics, and route maps. Vehicles might also earn tokens by selling user data to other vehicles over peer links. Thus, BC creates a closed V2V loop that assures proper incentives and rewards for participation in the network. In V2I links, BC offers a substantially simpler payment environment for vehicles to simplify various driving elements. The payment is automated based on underlying SCs. For example, consider SCs are executed between vehicle owners and infrastructure providers like government, cloud services, and others for a diverse range of applications like toll payments, insurance registration, and automated cloud service pricing.

Another use-case of vehicular networks includes the BC-based ride-sharing industry. While ride-hailing apps like Uber and Lyft presently dominate the market, popular ride-sharing services like Google's Waze are gaining momentum by prioritizing carpooling over taxis. The Toyota research institute (TRI) has already made considerable strides in researching and preparing for BC integration in the automobile industry. TRI has partnered with many businesses to create BC-based solutions that improve ride-sharing, including car-sharing for vacant seats, capacity management, and other service sets. Thus, BC-based vehicular networks have great potential as they leverage automobile stakeholders and infrastructure companies to form a seamless payment and trusted exchange solution.

8) Smart Agriculture

The Agri-food system requires critical data and available natural resource information to increase the production capacity. This information assists the farmers in acting against natural calamities. As depicted in FIGURE 10, BC assures data and information flow from inputs to outputs via several phases of value addition, while goods and cash flows from output to input. IoT networks play a vital role in smart agriculture as it allows sensor-driven networks to control the agriculture processes. It allows precise measurements of inputs to agriculture fields like water measure, proper temperature control, humidity, and fertilizer intakes on the crops. However, as the sensor networks communicate data over wireless channels, there are possibilities of attacks [115]. Any malicious sensor node might trigger incorrect measurements over the network, which would result in incorrect measurements being propagated over the network. Hence, the data communicated between sensors must be trusted, and a consensus-driven approach is viable. Thus, BC in smart agriculture paves the way for mitigation of sensor attacks, which can then be customized for different agriculture use cases depending on scenarios, capabilities, and the farmer requirements.

In BC-driven smart agriculture, once the data from sensor nodes are captured, they can be sent to cloud servers for analytics. This allows for effective decision-making about crop health and gives an accurate prediction about crop quality, which fetches higher prices in the markets. Also, via BC, there is assured transparency among the farmers, crop markets, sellers, logistics, and consumers, as it instils trust in the entire food supply chain. It eliminates the middlemen from the supply cycle and mitigates the black-marketing and illegal hoarding of crops that increase the prices. Recent studies have integrated unique solutions that involve UAV-driven field management for better surveillance and control of crops. UAVs trigger alarms in case of possible trespassing in the crop fields. For example, weather and environmental data are also captured by UAV nodes which can be sent to cloud or edge servers to form accurate predictions on crop management. Thus, BC technology secures the data in the agri-chain businesses and guarantees that information and data are accessible to all parties and that all data collected is unalterable. The type of BC deployment (permissioned or permissionless) and the underlying consensus algorithm

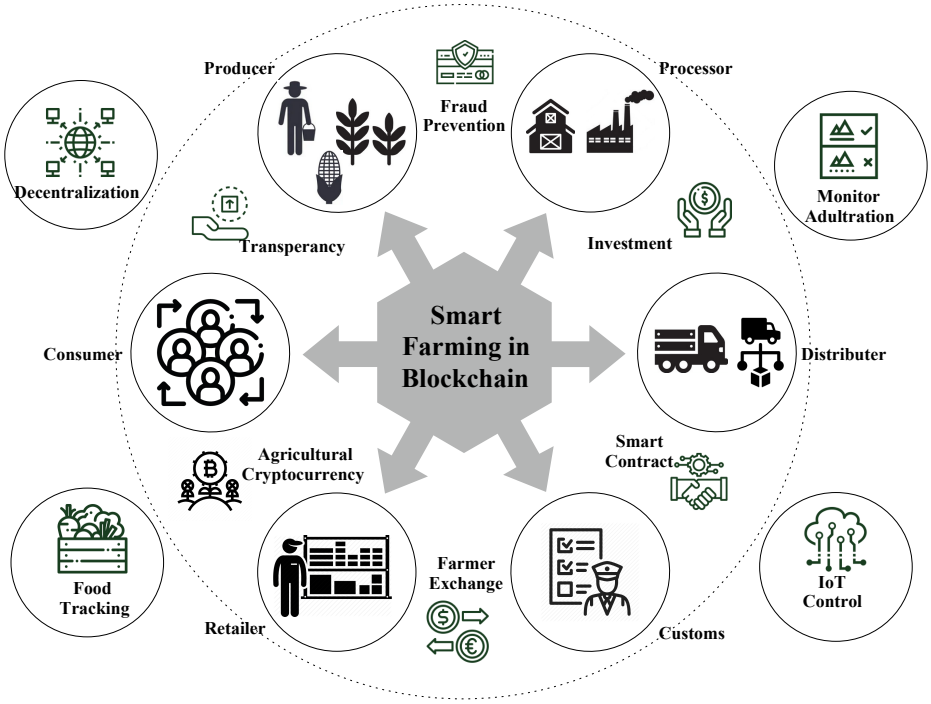


FIGURE 10: BC in Smart Agriculture

determine the stored ledger transaction rate. FIGURE 11 presents the data and information flow in the agri-supply chain.

Numerous smart agriculture concepts are being developed and deployed in combination with IoT and BC technologies. Author in [116] proposed a BC-based architecture for intelligent greenhouse farms where IoT sensors send the data to private BC maintained by a single authority. Similar solutions are also proposed by Lin *et al.* [117] for general-purpose smart agriculture. The framework is a platform that enables parties to create trust using BC technology at its core. Agents engaged in manufacturing a product, from germination to sale, can use smart mobile phones to access the data recorded in the BC. Authors in [118] proposed a BC-based e-agriculture paradigm for usage at the regional and local levels, in which each actor keeps real-time data on water quality in BC. Numerous firms are dedicated to the implementation of BC technology in smart agriculture. To cite a few, the firm Filament creates smart agricultural technology that enables physical things and networks to communicate with one another. It developed penny-sized technology that connects easily to current machines or devices through any accessible universal serial bus (USB) port and is used to secure BC transactions. Additionally, agricultural groups are embracing BC technology to enhance their farming operations. In Taiwan, rural irrigation groups utilize BC data storage and improve their contacts with the public [118]. Each public association provides irrigation management data to the public BC. Transparency engages the public in irrigation management and inspires them to work more diligently to improve water utilization. Over time, the long-term data produced using BC technology may be utilized to guide decisions on irrigation canal development and maintenance.

9) Smart Energy

This section presents the fundamentals of smart energy in terms of a distributed energy system framework, Microgrid, and the integration of BC in the allied fields. The details are presented as follows.

1) *The Distributed Energy System-* In the energy industry, the distributed energy system (DES) allows decentralized energy generator that enhances the system throughput by considering energy generation and economics with the environment. By increasing the utilization of renewable sources of energy for distributed energy generation, DES overcomes the various drawbacks of a centralized network of energy [119]. Integration of ML in IoT networks via DES has simplified the monitoring and management operations of data records. DES has substantially benefited the electric utility industry due to its broad adoption, opening the door for the growth of renewable services. Numerous developing technologies exist now that make it simple to transfer energy to digital. These technologies enable us to maintain a closer watch on a DES in a faraway place. Because the IoT is important for energy changes, DES has embraced it. Due to the availability of BC and IoT, a broad range of DES-enabled services ensures transparent and secure data exchange among different stakeholders. DES provides a measure of security and the capacity to make and

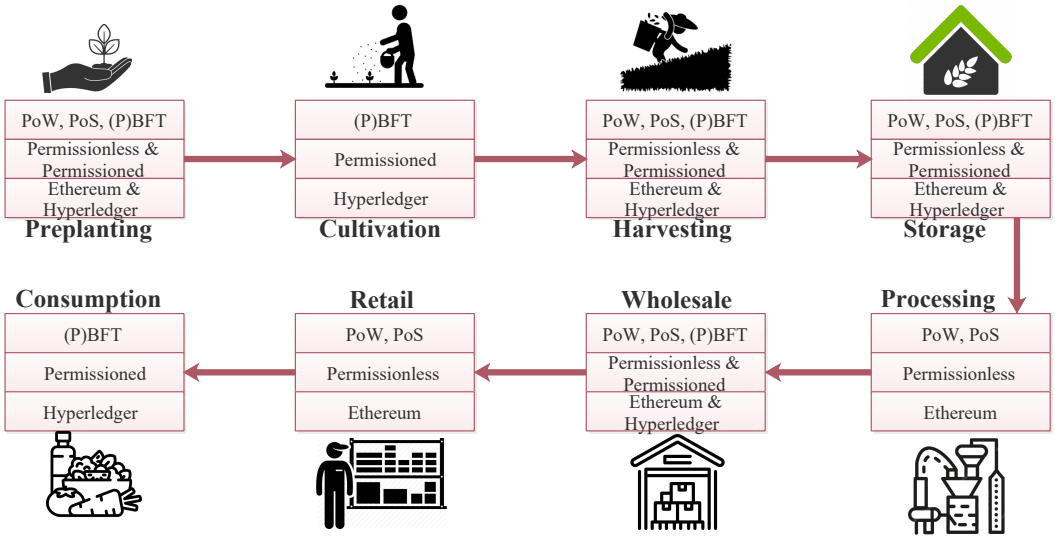


FIGURE 11: Data and information flow along the food value chain

process choices in response to real-world situations. Additionally, BC-based energy-generating offers are more beneficial than conventional DES approaches. As BC allows a decentralized energy trading network that stores the import and export of energy in BC with timestamp and usage[32]. DES is a highly sophisticated system that provides various services, including development, operation, energy trading metering, and energy trading. To cite some recent examples, authors in [32] did not consider problems like ageing grid infrastructure, dependability, energy loss, stability, old-fashioned design, and environmental concerns. They decreased generation, transmission, and supply efficiency. Truby *et al.* [120] suggested ways to improve the environmental sustainability of BC applications. BC also allows a trusted financial ecosystem that governs energy transactions through cryptocurrency exchange [121].

2) *Microgrid-* Microgrids are small-scale power plants with their own generating and storage capabilities. A microgrid has clear borders consisting of a tiny cluster of electrical consumers supplied by a local source of electricity. The clusters are connected to a self-sufficient national grid. A hybrid microgrid is linked to the power grid. To establish a microgrid and deliver power, decentralized energy resources are coupled with energy storage systems (ESSs) [122]. A microgrid strategy can quickly diminish the decentralized flexibility of renewable energy sources. Goranovic *et al.* [123] offered two ways to offer grid control. The first way is to monitor decentralized and centralized monitoring systems. In a centralized system, an operator is in charge of the overall operations. The deployment of central operating devices demands the construction of expensive infrastructure. Centralized systems gather and process data before determining the best course of action based on the conditions. Multiple places in the system are made available for data transmission and reception via communication channels and centralized devices. The major downside of this technique is that employing numerous locations in the centralized system raises the likelihood of system failure. Secondly, a decentralized system, in which each device operates autonomously, can overcome the centralized system's restrictions. Furthermore, the decentralized system enhances communication speed and fault tolerance. Through the inclusion of SCs, BC is perfect for executing business operations in microgrids [124]. The authors have provided numerous examples of BC solutions for microgrids with particular technical characteristics. When discussing sample microgrid projects, the researchers took into account the BC type, consensus method, and availability of components necessary for hardware development or open source [123]. Following are some real-deployment projects that include BC-based initiatives in microgrid applications.

- *TransActive grid-* It is a joint venture of LO3 energy and BC-based incubator consensus system that proposed a smart meter for solar panel owners. It monitors the energy requirements of solar owners and circulates excess energy back to the grid. The bills are generated at the end of the day, which can be transacted via SC. It also allows a direct trading approach with the grid and solar panel owners.
- *Solether-* It is an open software for solar plants for better management of energy and uses cryptocurrency for payment.
- *PowerLedger-* It is BC-based trading and clearing system in the market[35], and is community-driven. It

employs both a private ethereum network using PoW consensus and PoS.

- *BankyMoon*- It is a South Africa-based project startup that proposed a mechanism to connect smart meters in the BC network and allows users to use bitcoin for energy flow and provide a prepaid option with cryptocurrency.
- *NRGcoin*- It is a BC-based smart contract architecture on the 'energi' BC network. It was driven by gateways that computed electricity flow and interacted with one another using an SC. It uses the PoW consensus mechanism and is ethereum compatible with capabilities to support third-party DApp vendors.
- *Charge and share*- It is a network of electric charging stations based on a public ethereum chain that uses the PoW consensus algorithm. The stakeholders can register in the BC and fix their tariff charges. These networks work on sharing models with other charging stations. Using the Sharing module, any charging station may be connected and integrated into the Share and Charge network. [122].
- *SolarCoin*- It is aimed to help with the widespread generation of solar energy. Customers generally shun solar systems due to the long installation procedure. This initiative attempted to alleviate this problem by rewarding purchasers. Each megawatt-hour (MWh) generated resulted in the awarding of one solarCoin. It used the PoW consensus method and bitcoin as the currency.
- *GrunStromJeton*- This was a theoretical structure built on Ethereum, which was designed to validate the real usage of power. It uses Proof-of-Authority (PoA) consensus mechanism to validate the block. It incentives the user with the token that indicates the system's systematic behaviour.
- *GridSingularity*- A decentralized data interchange architecture created particularly for the energy sector, with a focus on water, electricity, gas, and heat. The consensus methods utilized on the above platform that uses public Ethereum were PoW, and PoA were used as consensus algorithms.
- *Slock*- It is a BC platform that allows users to sell or rent directly without any intermediary such as *BlockCharge* that provide a smart plug to charge an electric vehicle with the help of cryptocurrency, and *PriWatt* to manage energy transaction.

10) Digital data management

In recent years, technical innovation and similar studies on collaborative techniques for exchanging user data among organizations have accelerated [125]. There is a need for data sharing techniques to find a balance between user privacy and user experience that increases corporate profit [126]. The issues of *when what, and whom* of data sharing are simplified with BC [127]. BC also facilitates how the data owner should be rewarded as an incentive for sharing their data. The different organizations collect users' data is collected for business purposes by the different organizations from social media applications to enhance their business model and serve their clients more appropriately. However, the acquisition of user data raises significant privacy concerns, which either organization provides as part of the data privacy policy or based on the user's behaviour monitored by the internal audit [128]. The prevailing paradigm of data ownership, which is typically reflected in service license agreements, is presumed that the ownership is transferred to the organization that collects it and can share it with its enterprise network.

The storage of personal data raises privacy and security concerns; most well-known service organizations have suffered data breaches. When data is stored in a centralized storage system, then it becomes more vulnerable to attacks such as data modification, deletion, and the inability to send data to authorized entities. Sharing data across applications and organizations enables greater personalization, a key component of Industry 5.0. It results in a more positive user experience, but an added layer of security and privacy is required within organizational boundaries. Standard security measures, as well as experimental ways, have been used to solve sharing security, such as conducting all communication without trusting anyone and possibly replacing the centralized governing authority [125]. Numerous modern technologies have been used as computational backbones for collecting user data and how to share it with others, services such as cloud computing, radio-frequency identification, and security solutions to safeguard the user data against hackers [129]. Federated learning [130] enables the mining of data that is dispersed across multiple sites.

The great technological advancements in recent decades have enabled many businesses to communicate while making smart judgments better. Using technological resources to acquire data about people's daily lives from many autonomous data sources has become a major practical issue with legal ramifications. Enterprise data sharing models are networked information systems that allow users to build profiles, store data, and share it with others. This model includes a single, centralized, decentralized, and BC-based system. Giant tech data hoarders like Google, Microsoft, Twitter, and Facebook are single enterprise data sharing systems. They gather and exploit user profile data in their ecosystem. Other services can leverage these single systems' existing APIs and authorization methods to access data. Users may retrieve their complete data and switch to other services that ensure data privacy. With desktop publishing (DTP), customers may easily migrate their data between internet service providers using an open-source data portability platform. Interoperability is important to the project's contributors. Useful datasets may be discovered and accessed via amazon *OpenDataRegistry* web services as data suppliers back them. The amazon web services Open Data team reserves the right to delete data. Google's Dataset allows you to search 25 million in available public datasets. To explain their datasets' metadata, publishers must utilize the open standards of *schema. org*,

which Google does not manage or grant direct access, and it performs indexing and creates searchable metadata.

Authors in [131] detailed many tests illustrating Google's frightening collecting of user data to target them with paid advertising. If you use Google's platforms such as Chrome, Android, Maps, and YouTube, it gathers data, tracks your daily activity, uses it against your search, and makes your mind with related advertisements. In service-oriented, mobile, and ubiquitous computing settings, centralized architectures seldom acquire and exchange varied bits of user data from independent and autonomous entities (apps, agents, sensors, devices, services) [132]. Centralized design imposes a consistent logical structure (ontology) for the user model, removing contextual information from applications closer to the user data. Due to the popularity of efficient web-based client-server architectures. The user data can be saved in various storage locations, while the user modelling process can be centralized [133]. However, storing user data centrally does not need centralized user modelling if the alternative semantic schema is utilized that makes user modelling procedures independent [134].

Data sharing models such as Wikidata [135], Mypes [136] is an online P2P file-sharing and management system that evaluates the non-functional criteria including efficiency, scalability, and dependability [137], and materializing these data for better performance [138]. So most of the research on these design frameworks focuses on optimizing the framework qualities. In most situations, centralized architectures do not gather and distribute user data from independent and autonomous entities such as systems, agents, devices, sensors and services that provide service-oriented and ubiquitous computing environments [132]. Centralized user modelling often includes a set point of failure. To safeguard data, servers are mirrored, although this frequently results in high connection costs. Iyilade and Vassileva [139] proposed a networked architecture for exchanging multi-application life logs. Data from various systems, such as life logs, is collected by agents and sent back to the centralized broker for modelling. This includes request analysis and response processing. Systems like *MobiTribe* [140] provide a distributed yet conceptually centralized user paradigm that focuses on data sharing across multiple apps and mobile devices, with a centralized content management system that acts as a mediator. *PersonisAD* [141] is a mobile and ubiquitous computing paradigm, which collects data from users and their surroundings, and logically integrates it to deduce the preferences and alter user service functions to deliver a better experience. Authors in [142] proposed a distributed sharing model using single standalone agents that store each user's unique characteristic in a central vector model.

Moreover, accommodating competing user desires is inextricably linked to architectural design that optimizes certain system attributes at the expense of participant autonomy [133]. These studies employ decentralized user models owned by multiple agents and acquire information from them just temporarily, on-demand, for specific adaption purposes. Users' data sharing systems have developed from centralized to P2P. Centralized indexes can help P2P networks search faster, but we need decentralized and hashed data storage methods to ensure anonymity. In a structured P2P system like Chord [143], users are not allowed to keep their data with peers of their choosing but with random peers.

11) Supply chain management

Supply-chain management (SCM) is a crucial management input in agricultural applications. Traditional food and agricultural logistic systems store orders and deliver them to their destinations. These traditional systems lack traceability, auditability and transparency to their orders, inventory and transactions [144]. However, in today's digital era, these elements may increase food safety and quality, and hence customers seek high-quality food [145]. To monitor the food-supply chains from remote networked locations, research and development firms have shifted towards the use of smart sensors to monitor the supply chain conditions. The packages are packed and transported, embedded with radio frequency identification (RFID) chips, that monitor the item's conditions inside packages during transit operations. Caro *et al.* [146] claims that most centralized cloud infrastructures are utilised as contemporary SCM IoT solutions. The common challenges in such systems include single-point failure, data integrity, and lack of transparency. BCs can efficiently tackle these concerns. BC may be used to construct decentralized, trustworthy systems. *AgriBlockIoT*, a decentralized BC-based SPM solution, was proposed [146], which included IoT sensor devices that generated and consumed data. The scheme can access stored data and execute autonomous SC, delivering unprecedented transparency and inflexibility in a contemporary setting using mini-PCs and gateways. *AgriblockIoT* performance is measured in terms of computation and communication cost. According to Perboli *et al.*, [147], numerous IoT technologies are employed for food safety and SCM, but certain concerns remain unresolved. The main challenge is to assess whether the information or data supplied across supply chain partners is reliable. A method called hazard analysis and critical control points (HACCP) was presented in [145], which provides real-time tracking information to all the stakeholders involved in SCM at the same time maintaining dependability, openness, impartiality, transparency and security.

Weber *et al.* [148] presented a BC-based solution to verify the trustworthiness of information transmitted across supply chain parties. They addressed business notations and process models. The BC prototype concept was verified via business processes [35]. Guerreiro *et al.* [149] established a concept called business process management (BPM) to safeguard commercial interactions. The suggested paradigm reduces the risk of fraud by boosting trust, authenticity, resilience, and traceability. Leng *et al.* [150] proposed an agriculture supply chain (ASC) system based on the double chain design, which boosted the Scalability of ASC drastically. The authors proposed adaptive rent-seeking service platforms

such solutions assured data openness, privacy and security. The system's efficiency and utilization of the public service platform were also upgraded. The suggested solution faced performance and BC size issues. Mao *et al.* [151] presented a public BC-based credit assessment system. This method improved the administration and oversight of the food supply chain. The authors obtained credit rating text from traders through BC smart contracts and then assessed the text using the long short-term memory (LSTM) model. However, the authors did not examine the system's cost and advantages. Thus, a holistic framework to deploy the same common technique to design, build, and verify the whole BC system is impossible. Later, in [147], the authors focused on one of the most significant concerns, namely the application of the blockchain in the supply chain, including all parties. Moreover, sharing information throughout the BC might cause stagnation in solution adoption. So, to properly deploy BC based on the supply chain, first analyze the requirements and goals of all involved parties. The authors developed a business model that maximizes both economic and consumer happiness with this goal in mind.

A study by Kshetri *et al.* [152] found a correlation between the adoption of BC in supply-chain operations and increased accountability. Cost, quality, speed, risk reduction, reliability, sustainability, and adaptability were assessed. Kaijun *et al.* [150] suggested a public BC for the agricultural supply chain. A consensus algorithm and resource rent-seeking mechanism were the key points proposed in the system. The findings show that an architecture that follows the double chain model could protect transaction information while maintaining company privacy. It might also self-adapt rent-seeking and resource matching. Thus, the suggested design increased the platform's legitimacy and overall efficiency.

V. CHALLENGES AND FUTURE DIRECTIONS

The section discusses the challenges of BC-assisted Industry 5.0 verticals. We categorize our challenges in two parts. First we cover the potential challenges of Industry 5.0 applications in terms of deployments, and present BC as a viable solution to these challenges. Next, we discuss the potential loopholes (security limitations) of BC-assisted Industry 5.0 applications, and present BC is not a panacea for all security issues. We discuss the attacks on BC and SC assisted systems, and potential directions to mitigate the attacks.

A. DEPLOYMENT CHALLENGES

In Industry 5.0, BC plays a vital role in securing assets and information flow in different industrial processes and components. It forms a trusted and auditable trail to support the diverse nature of application end-points. Thus, from a security viewpoint, BC as an enabler for Industry 5.0 would depend on the internal specifics and underlying representation of major architecture, frameworks, and schemes that are supported by BC ledgers. FIGURE 12 shows the key research and implementation challenges in deploying BC solutions in Industry 5.0 architectures.

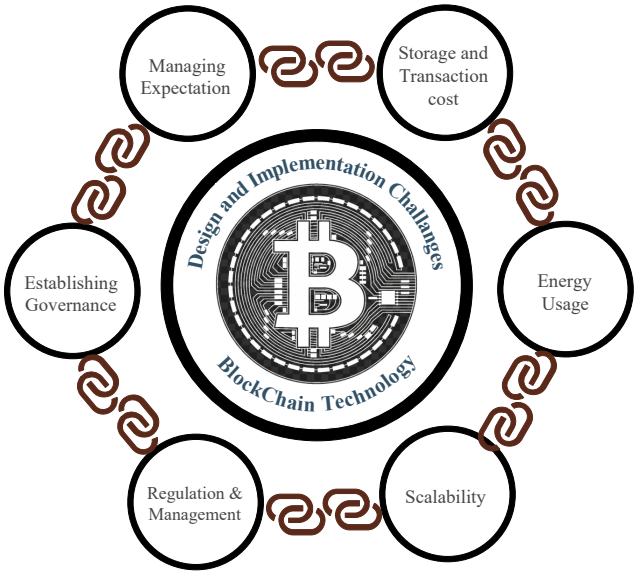


FIGURE 12: Design and Implementation Challenges of BC in Industry 5.0 applications

In the near future, BC technology will be shaped by security tokens, SCs, and a changing legal landscape by documenting legal data on blockchain [153]. A highly reliable, secure, and scalable BC deployment is necessary to accomplish these goals. The BC type, supported by the underlying consensus would be vital to leverage the full potential of advanced technologies like AI, IoT, CPS, and big data. This section discusses the design and implementation difficulties inherent in conventional systems and the possible benefits of BC technology. Thus, the section is focused on addressing the RQ4 in the proposed survey, where we discuss the key challenges and pitfalls in adopting BC as the mainstream technology in Industry 5.0 applications. The research challenges and the possible future directions are presented as follows.

1) *Regulations and Management*: The centralized procedure of the current industrial control systems is a major obstacle. These systems are bigger, complex to scale for business processes. If the central system is compromised, all the data need to be re-routed, which results in higher network latency and computing power. In a centralized system, authorities have all the rights to verify the user's transaction. In a decentralized system peer to peer connected system set verifies the transaction. However, the communication standards for P2P communication should be uniformly regulated for overall applications. A possible solution is to form a unified web framework, where data is exchanged via APIs to assure greater control between applications and service end-points.
2) *Scalability*: Nowadays, all transactions are stored and validated on the BC network. Consequently, the ledger size of the BC network becomes massive, and it takes

more time to traverse all blocks in the chain. Each block size is fixed, which can handle a limited number of transactional data. The BC varies in block size and block addition time, depending on the consensus mechanism used to verify the newly created block. For example, some public BC ledgers can handle only 7 to 8 transactions per second. In contrast, millions of transactions happen in real-time industrial situations, making it difficult to deploy BC, and presenting a scaling issue. A potential solution to address the problem is to form sidechain ledgers that can switch transactional data from one chain to another, depending on the application use case. Another approach is to support sharding in BC, which forms mini BC ledgers which are controlled by a sharded authority [154]. The only concern is to ensure a fair consensus principle on sharded BC so that transactions are fairly ordered in the main chain and selective applications are not prioritized.

3) *Managing Expectation*: Establishing trust is critical in the business environment as an attacker may disrupt an ongoing situation of a data leak that makes it difficult to trust anyone in the network. In these instances, BC may be utilized to prevent tampering and build trust since it generates blocks using cryptographic hashes and the ledger is permanent. The challenge is trust measurement, which becomes critical in real-time system management, where a statistical analysis of trust computation is required if the nodes behave maliciously. Recent studies have suggested a reputation-based BC design that presents a reputation score to added transactions and forms a consensus based on the miner's reputation.
4) *Establishing Governance*: The protection of vital data is the main priority of any business organization and security requirements vary from application to application. For example, authorization and authentication are major requirements in cloud monitoring, where we evaluate the signature patterns of attackers and determine the vulnerabilities. This prevents the attackers from gaining unauthorized access and manipulating data. Certificate generation is a critical issue in vehicular systems, and BC allows trusted certificate generation. In healthcare, privacy is the prime requirement, as sensitive patient attributes must not be disclosed to unauthorized entities. Thus, a single unified BC architecture is not sufficient to address all the requirements of Industry 5.0. A possible direction is to form custom BC networks that can cater to and address the specific requirements of different verticals.
5) *Storage and Transaction Cost*: Although BC assures trust and chronology in Industrial processes, the cost of deploying BC in terms of resources is high. Moreover, the communication cost increases when sensor nodes establish communication with other nodes. To date, no general set of standards is formed for cost addressal, and most solutions focus on optimizing the cost factor only. Possible research directions thus include forming a unified standard set of protocols for the BC network that can reduce the communication cost. However, this would highly contradict with application and its specific requirements. Another direction is to form low-cost SCs, that can reside in the memory of the sensor node itself, where once the sensor node gathers data, the contract is self-deployable. By this, a high degree of automation and cost reduction in industrial applications is achieved
6) *Energy Usage*: As industrial processes are sensor-driven, they are constrained by energy usage. Recently, permissioned and private BC networks are considered a potential solution to this challenge. Still, the private network employs their tailormade consensus approach, which might reduce their security to address the energy consumption of sensor operation. Such consensus networks again shift towards the centralized or semi-distributed approach, where there is a main validator node to address the mining requirements. In such cases, the overall trust measurement becomes a vital use case. Thus, recently, researchers have shifted their views towards the proposal of verifiable trusted BC solutions in permissioned and private networks, so an optimal mix of energy cost vs. security trade-off is achieved in deployed applications.

B. SECURITY LIMITATIONS AND ATTACK SCENARIOS ON BC-ASSISTED INDUSTRY 5.0

BC allows transactions to be digitized and distributed across the network, which eliminates the validation by a central authority. BC strength lies in immutability through cryptographic hashes, and identity and access control through SCs. However, despite its security features, it has some inherent limitations. The major security loopholes in BC arise from social engineering attacks, where a naive user might accidentally share its wallet security phrase on some link, in response to some coins. Such sites are built to lure users as honeypots and contain viruses, and Trojans to trap user information. Other attacks are related to mining pools, privacy thefts, and SC related attacks. As per a recent study by Chen *et al.* [155], the authors have presented a systematic review on attacks on BC-assisted ecosystems. The authors focused on three critical aspects, namely, the mining pool attacks, the communication-based attacks, and the SC-based attacks. The implementation challenges and future directions are presented. Thus, it is critical to address the vulnerabilities raised in the BC-based Industry 5.0 ecosystem. We present some of the key attacks on BC classified in [155][156]. The details are presented as follows.

1) Mining Attack:

We start the discussion with the mining-based BC attacks. Such attacks are targeted to gain control of the mining network, where an attacker tries to manipulate the hash rate of the network, keeps a block secret from other miners in

some private (alternate chain), or tries to manipulate the BC by making its alternate chain as the largest chain. The attacks are sub-classified as follows.

(a) *Block Withholding Attack*: An attacker (miner) submits a partial PoW that lowers the overall pool profitability. The attacks delays submitting the block captured from the victim mempool address to the mining pool admin, thus, in the long run, it decreases the pay per share of the pool, and consequently, the incentives of miners decrease. Potential solutions include a random mining strategy that selects a random miner to submit PoW, or game theory between miners, which allows miners to watch-guard other miner activities, or optimization strategies to increase the pay-per share among miners (swarm-based optimization). These solutions leverage a fair ecosystem for all miners in terms of incentive and control.

(b) *51% Attack*: The attack targets the hash rate of the mining pool, where a group of miners collude to have a combined hash rate of more than 51% of the entire network and thus form a majority. With this attack, the colluding miners can reverse a transaction validation, which would be supported by 51% of nodes in the system, or might create a side-chain which is invalid, but would deem as legitimate as it would get the majority consensus [157]. Different solutions exist to thrawt the 51% attack. The first solution is to not use the standard PoW consensus, as it allows the miner to succeed with a high hash rate. The second solution is to create checkpoints after a fixed number of blocks are added to the chain. This makes the chain irreversible from the created checkpoint, or when a block successfully mined in the network chooses an alternate miner [158]. Authors in [159] proposed a history weighted information of miners that calculates the total hashing power of any mining pool. The proposed method allows honest miners to resolve the conflict between two branches in the same main chain. The honest miner calculates the historical weighed difficulty to both the branch and side-chain and considers the chain with high historical weighted difficulty.

(c) *Selfish Mining*: In this strategy, a malicious miner mines a block, but keeps the block secret from other miners. The secret block is published in a side-chain, which is not known in the main network. At the same time, an honest miner mines the same block and publishes it to all miners. The attacker keeps on mining blocks and adding them to the side-chain structure, and honest miners add the same blocks on the main chain. The instant the side-chain length becomes longer than the main chain, the attacker publishes its side-chain to be visible to all nodes. As per the longest chain rule, the side-chain is considered as correct, and honest miners are pruned of incentives. More blocks are then added to the side-chain, instead of getting added to the main network. A possible solution to the attack is to identify the block confirmation via sequence numbers, and also publish the block height (number of added blocks in the chain) apriori. This allows the nodes to detect selfish mining activity in the main network [160]. Another possible solution is to include unforgeable timestamps at the time of block validation in the main network. Any block with a lower timestamp value can be treated for further examination by other nodes in the main network [161].

(d) *Cryptojacking:* This is a type of cybercrime where cryptojackers try to get unauthorised access to the user device for mining purposes, where the user is unaware of the mining process. With the malicious program, crypto mining code is installed in the target machine and runs as a background process and contributes to the mining pool by computing hash. The way hash power is generated is the same way incentive is distributed but the actual beneficiary of that incentive is never materialized. Solutions to such problems are to use proper security mechanisms in machines as well as report to law enforcement agencies.

2) Network Communication Attack:

BC application are decentralized and uses a P2P network for communicating between nodes in the network. The possible attack on the BC network, SCs, and the supported application are discussed as follows.

(a) *Eclipse:* In this attack, a specific user is isolated within a P2P network by a malicious intruder. The attacker redirects the inbound and outbound connections from legitimate neighbour nodes to the attacker's neighbour. By doing so, the attacker manipulates the node which leads to illegal transactions and disruption of block mining. The possible solution includes a deterministic random eviction that makes dynamic changes in the communication list. It also includes a random selection and test before eviction that ensures the number of a malicious node does not grow continuously [162]

(b) *Sybil:* Sybill is another P2P attack model, where a node is capable of operating in multiple identities. The main aim of the attack is to gain the network and carry out illegal instructions. In the consensus process, a malicious node sends a message to other P2P nodes to gain critical information about the connection pools in the BC network, and mislead the routing information. The attacker forms false identities to form legitimate and authorized information and spoofs the neighbour nodes. Authors in [163] proposed a credit-based block consensus mechanism, which ensures that only a block with the highest credit score is selected to join the group of block consensus. The other technique uses a network flow algorithm to select an agent node for block consensus by calculating the credibility of the node based on the transaction data.

(c) *Distributed denial of service:* In a DDoS attack, a group of controlled machines targets a node by gaining information about the attacked node network and then controls the devices that interact with the attacked node. The attack is launched through a botnet swarm, that injects a large amount of false information and makes the attacked node unable to complete the block mining. This type of attack involves sending cryptocurrency to a malicious node, where small quantity transactions are carried out in massive quantities. This creates a large number of micro-transactions (dust transactions) in the network, which requires unnecessary mining power in the network. Thus, the cost of executing these dust transactions becomes more than what is supported by the chain. One of the possible defence mechanisms against DDoS chain attacks includes building intrusion detection systems, that can monitor such illegal transactions through ML and DL anomaly algorithms. The required computational power for running the algorithms is supported in a cloud-based ecosystem [164]. A hybrid ensemble learning method to improve the performance of detecting such attack involve different ensemble learning for different BC [165]. Authors in [166] proposed a DL-based learning model which uses the principle component analysis to identify the feature of the attack and uses real-world data for training and testing.

(d) *Re-entrant:* This is an SC category attack and occurs when an SC function makes an external call to another untrusted contract placed by the attacker in the main chain. That untrusted contract makes a recursive call to the original function to drain the funds. The event occurs when the contract fails to update the state before sending funds. The attacker calls withdraw function and use the malicious address as the recipient's contract address. The attack happens due to the vulnerability in the SC, and to avoid it, small changes in the contract are required that update user's balance before transfer. Another solution is to combine static and dynamic analysis for application binary coding using SC to improve the detection efficiency [167].

(e) *Flash loan:* In decentralized finance (Defi) operations, instant loans are provided by execution of SCs, and wallets are debited without any security checks. SCs consist of three states in Defi, where the user first gets the approved loan amount, then the loan purpose is specified, with the equated monthly instalments fixed, and finally, the repayment cycles are provided. If any of the states in the SC fails the BC revert back to its previous state i.e. the loan never gets disbursed. To exploit this vulnerability, the borrower needs to act instantly and transfer the fund before finalizing the block in the chain. Possible solutions include carefully designing the SC.

(f) *Rug pulls:* In this attack, pulling the rug out by attracting the investor in a new project associated with a new cryptocurrency. The developer wallet is kept open and all the funds are transferred to some new wallet before making everything official and leaving the investor with worthless coin. These types of attacks involve malicious intention and intentionally designed SCs with multiple wallet addresses.

3) Privacy Attack:

BC is a public ledger that makes each transaction transparent, attackers track the transaction information in a public ledger. The common privacy attack is listed as follows.

(a) *Identity Privacy:* The attacker gains control of the private information using the communicating wallet address on the chain and the registration details with that address on the chain. The user monitors the transaction on a public ledger and analyzes the transaction between the entities. The common privacy attack includes key, replay and impersonation attacks, where the attacker illegally tries to get the key phrase of the user or intercepts the transaction data, thereby demanding the user authentication. The attacker also makes use of airdrop links to the vulnerable contract that shares your key phrase from your wallet. One solution to such a situation includes binding of IP address with the wallet address, where every transaction is completed with the IP and MAC address of the user and receiver.

(b) *Transaction Information:* The attacker uses the transaction to analyse the potential sensitive information. The attacker can download the transaction data of historical transactions for analysis [168]. This includes privacy tracking, false data, and information leakages. After obtaining the user's information, the attacker tracks the associated transaction and analyses it. If the users are registered on a private chain, then the registration information is secured. Another solution is the use of hardware-based digital wallets that uses a pseudo-random function so that nobody can identify the owner of that wallet.

VI. CASE-STUDY: A BC-BASED DIGITAL TWIN EMPOWERED SMART MANUFACTURING FRAMEWORK

This section presents a proposed case study of BC deployment in the smart manufacturing ecosystem, where we envision that the control process operations are simulated through a DT controller. A mathematical model is constructed that simulates the real-world feature of the system. Sensors receive data from the physical world, which is converted to a digital model. We employ IoT devices to connect the physical model with DT digital model that receives the input from the sensors. DT helps to measure the performance and identifies the potential problems in the physical model. It can be used in a simple and complex system where we need to minimize the system's downtime by careful simulation. The sensors data continuously update the DT to detect the early possibility of failure and identify the possible area of improvement for efficiency.

In Industry 5.0, the manufacturing industry must have

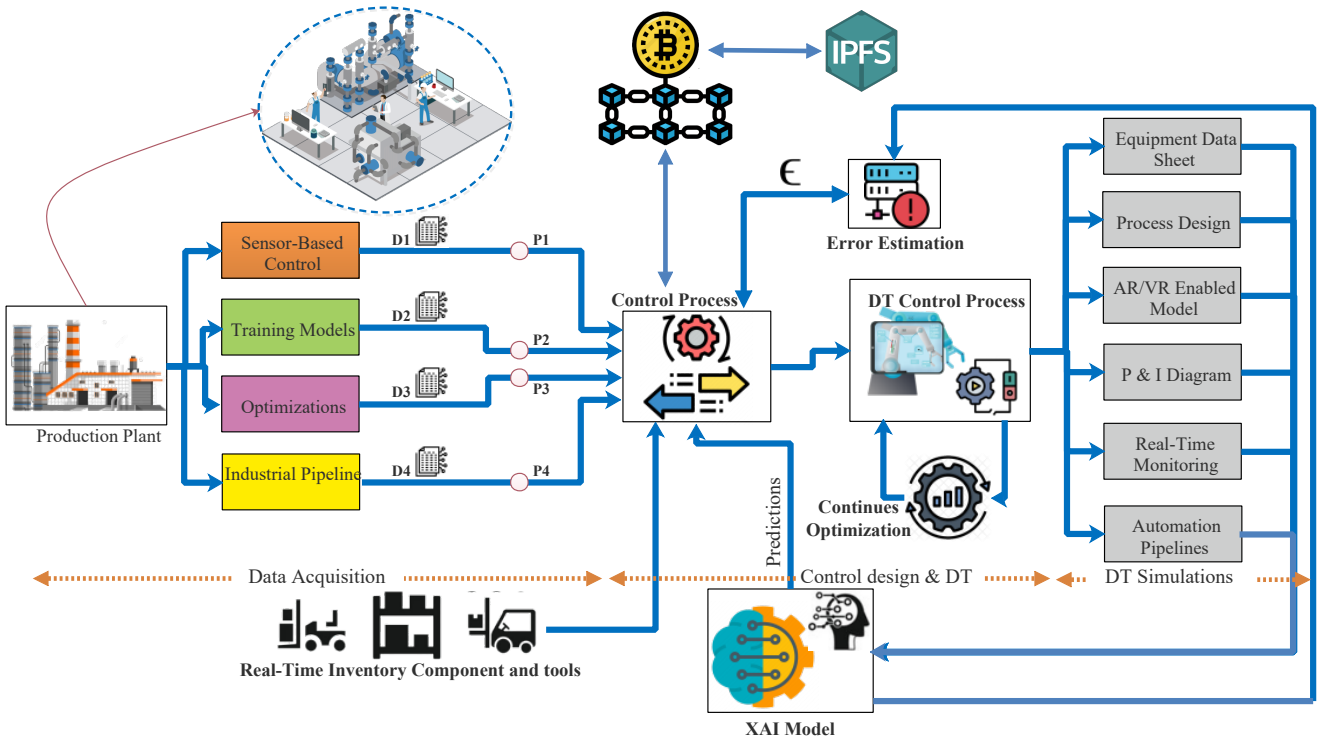


FIGURE 13: DT Enabled Process Plant in Industry 5.0 Ecosystem

predictive quality measurements and control, which requires that automated functions are initially monitored under DT. We measure the bias in the expected output and then pass the monitoring data to AI-driven pipelines for error estimation. Once the bias is minimized, we employ the inputs to real processes. The DT control data is stored in IPFS, which is connected to the permissioned BC network. FIGURE 13 present the design schematics of the proposed case-study. We have divided the case study into three functional phases: data acquisition, control design & DT, and DT simulation. The details are presented as follows.

A. DATA ACQUISITION PHASE

In this phase, we consider that the production plant generates d data streams $\{D_1, D_2, D_2, D_4, \ldots, D_d\}$, which is captured from d processes. Conventionally, a data stream is a collective summation of data which is acquired from k IoT sensors $\{s_1, s_2, \ldots, s_k\}$, l training models $\{m_1, m_2, \ldots, m_l\}$ that operate on the associated data, and m optimization rules which are applied to the l models. The optimization constraints are not necessarily applied to every model, but would specifically depend on specific input control only. We represent the optimization condition on l models as $\{o_1, o_2, \ldots o_m\}$, where $m < l$. To realize the Industry 5.0 vision, we assume a distributed data stream, where the collected data over d streams are from parallel industrial pipelines, which is represented as $\{ip_1, ip_2, \ldots ip_n\}$. In a nutshell, each data stream D_d is represented as follows,

$$\sum_{i=1}^{k} \sum_{j=1} ds_i \rightarrow D_j, \forall j \in \{1 \ldots d\} \tag{1}$$

Where s_k is the sensors data accumulated in D_d. The collected data D_d is mapped to q industrial processes, represented as $\{p_1, p_2, \ldots p_q\}$. These q processes are presented as inputs to the control process (CP), which is defined as follows.

$$p_q \leftarrow f(D_j) \tag{2}$$

where $q < d$. Any q^{th} process is allocated a priority value, denoted by $V(p_{q_d})$, where q is the process id, and d is the datastream identifier. We consider the priority computation as follows.

$$V(p_{q_d}) = \frac{1}{T_{q_d} + e} \tag{3}$$

where T_{p_d} is the time taken for the process q to complete the work. Thus, a process is assigned less priority if it has a large completion time. We sort the processes according to the priority values in a priority queue P_q. To prevent the priority values to overshoot, we keep a bound check through e in the priority equation. Based on P_q, the inputs are supplied as a steady-state simulation for preliminary process design. The reason for the inclusion of a dynamic simulation model is that we measure system responses as time-dependent source system for specified input sets.

B. CONTROL DESIGN AND DT

An initial model is created during the preliminary planning based on the initial information and nominal equipment datasheet. In this phase, CP receives p_d, real-time inventory components, and creates digital object DT of that physical production plant. To increase the accuracy of the DT, CP also receives prediction variables from an explainable artificial intelligent (Ex-AI) model, with error estimation ϵ to fine-tune the CP. DT process continues optimization based on the frequent inputs from the CP tuned by error estimation. It also combines real-time data from both ongoing and past historical data to compute all the jobs' expected processing time. Then, a scheduling algorithm is selected based on the rules and decided to take the most efficient action. To fine-tune the CP, ϵ is computed which is a difference between estimated parameter value v_e and actual parameter value v_a.

$$\epsilon \leftarrow |v_a - v_e| \tag{4}$$

To control the output value, certain corrections are required that we receive from the Ex-AI model as prediction output. The accuracy A_c of the DT can be defined as follows

$$A_c \leftarrow 1 - \frac{|v_a - v_e|}{v_a} * 100\% \tag{5}$$

C. DT SIMULATION

In this phase, we collect simulation results along with simulation parameters that can be utilized to generate predictions with the help of the Ex-AI model. During the operational maintenance process of process plant life cycle, generated simulation results, and DT is connected to automation system to monitor the execution. This enables continuous synchronization of the current process and simulation model. The DT is connected in a non-disruptive manner as the plant is under operation. The sensor data D_d is exchanged among stakeholders, the real system, and DT from the real physical system. The connection is made initially to DT while noting the finishing time of all the jobs. On scheduling the DT to physical systems, instructions are given to the physical object. The instructions are also known to the stakeholders in real-time, and they can track the system status, allocate resources, and DT stakeholders to forecast the current data. DT generates an equipment data sheet that captures specific equipment's electrical, mechanical, and control requirements. The process design captures the choice and sequencing of the units, the P & I diagram captures the piping and related components of the physical system, and real-time monitoring information is captured for specific inputs/outputs. In such designs, augmented reality and virtual reality (AR/VR) capture the physical object designs to be mapped to a given environment, which helps in the initial design and physical modelling. It also helps in rapid prototyping and pipelining solutions to improve safety, up-time and energy consumption.

BC is the next step to bridge the concept, redefining DT and providing full transparency to the data shared among different stakeholders. DT is built on traditional technologies that require a centralized server which makes it dependable in storing and analyzing data. BC is the most relevant solution to monitor the DT process that provides immutability and security to the data exchanged among stakeholders. To enhance the performance of the DT, BC provides data encryption and immutability to the data stored, and this allows DT to transit data security in all the components where IoT sensors receive the data to the DT model. BC is used to capture the intermediate update from CP, error estimation and accuracy to ensure the output from DT is secured. It prevents certain malicious input from changing the accuracy of the DT. BC stores the DT, its updates, owner, and virtual simulation results, making organizations track their product globally to count and maintain the inventory. To add the DT model in the BC, It will be published on the inter-planetary file system that stores the content in a distributed manner and generates a single fixed-length content key, defined as follows.

$$H_{key} \leftarrow \{DT_x, I_x, \epsilon\} \tag{6}$$

Where H_{key} is the content key, DT_x is the updated DT model with I_y, for the x^{th} input variable set, with ϵ error estimation. Now H_{key} is used as transaction data in the BC which greatly reduces the size of the block and results in lower transaction cost. The structure of the block and its content is defined as follows.

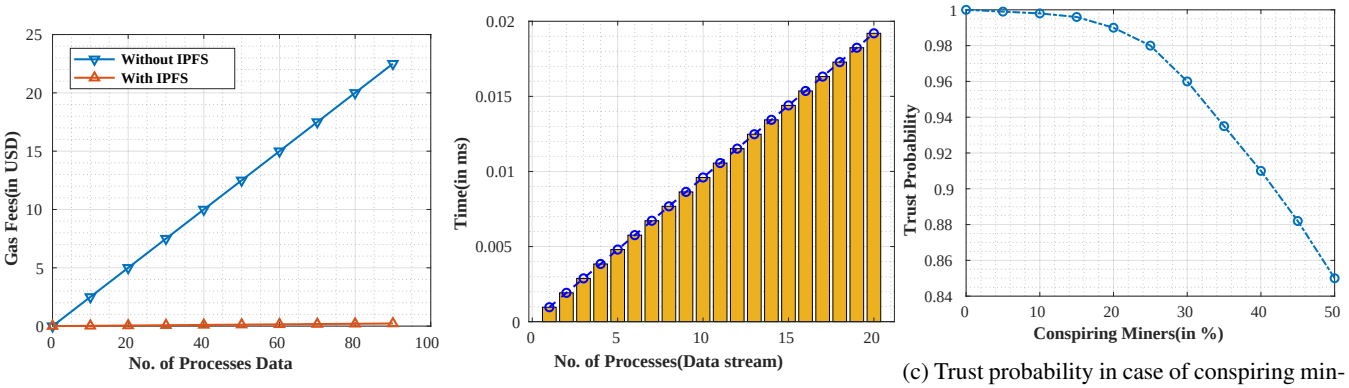
$$B \leftarrow \{H_{key}, T_s, N_s, H_{prev}, M_{root}\} \tag{7}$$

Where T_s is the timestamp of the transaction, N_s is the nonce value, H_{prev} is the hash of the previous block and M_{root} is the Merkle root of the Merkle tree. Thus, the data is secured over BC, and DT allows safe prototyping of the real manufacturing process.

D. SECURITY ANALYSIS OF THE PROPOSED CASE STUDY

In this subsection, we present the security analysis of the proposed case study in terms of storage cost, computation cost, and trust probability. The details are presented as follows. FIGURE 14a presents the cost of storing DT process data on on-chain and off-chain IPFS. The DT enabled process plant generates data from different processes. The system uses BC to store all such data from a different process. To store and execute one transaction on the standard chain, USD 12.51 gas fee is required during odd hours. Our case study employs IPFS to store data, where the 32 byte content address is required to refer to the IPFS stored file. A significant less gas fee of USD 0.124 is required to store the data on IPFS, which is $\approx 98\%$ less than the standard chain gas fees.

FIGURE 14b estimates the computation cost of storing the process data on BC via IPFS, every process data is first stored in the IPFS and hash is generated, that hashed value is stored in the BC that consist of the block header and block content. The header consists of Merkle root i.e. hash of the root of the Merkle tree, once the block content is identified a hash of overall content is computed. Overall 3 hash functions are required to store process data in the chain via IPFS. Each



(a) Cost of storing the data on chain and off-chain

(b) Computation cost of storing process Data

(c) Trust probability in case of conspiring miners

FIGURE 14: A security evaluation of the proposed BC-based DT-enabled Process Plant in Industry 5.0

hash function take $\approx$ 0.00032 ms [49]. We consider that 20 process data is stored, so $\approx$ 0.019200 ms is required as security computation cost. This cost excludes the block validation time.

FIGURE 14c shows the effect of conspiring (colluding) miner nodes on the overall trust of the network. When more than 51% from a group of miners in private or consortium BC form a collusion attack, more hash power is captured, and they force an alternate side-chain in the network. This decreases the trust probability of the system. Trust probability is computed as the percentage of legitimate (valid) block additions out of total blocks in the network. As more miners collude, the trust of the network drops. In the case of distributed databases to process the data, the trust drastically drops with a slight increase of colluding nodes, owing to the byzantine attack formation. In BC-assisted systems, the drop is not drastic, as evident from the figure. At 50% colluding nodes, the system maintains a trust probability of 0.85, which is better than traditional security in distributed systems.

VII. LESSONS LEARNED

These sections underline the key lesson learned from the survey and potential future directions. The authors discussed the limitations of current industry 4.0 standards in the present technical landscape and presented the requirements and visions of emerging Industry 5.0 specifications. BC is presented as a key enabler and viable solution to induce trusted control over industrial processes to secure the industrial boundaries. The author highlighted the privacy, security and trust management in BC-assisted smart manufacturing, where an organization uses BC technology to monitor its different processes and solutions to create trust among different business processes in the system that exchanges data over an unsecured channel. To support our claim, the authors proposed a reference architecture that integrates Industry 5.0 standard practices in business processes, which is supported through an assisted case study.

Going forward, the integration of BC, AI, and IoT customizes service sets to users, which supports the Industry 5.0 vision of mass personalization. As we move to the digitization and smart industries, the heterogeneous data move from one business process to another, which creates loopholes to exploit the privacy of the system, which makes the system vulnerable. Thus security and privacy are the main concerns before offering services. Privacy preservation is the potential issue during data accumulation, where the data is processed and shifted among different processes. The manpower in an organization needs to be trained in compliance with machine intelligence to gear up with cobots to scale the industry's manufacturing process.

AI, ML, and vast automation are an integral part of industry 5.0 and open a new threat vector. We require trusted datasets to train the model, which is protected and explainable to their decision during different data input points. To utilize the global data for better accurate decision, the system uses local data from all other local tenets and combines the data to train the original model, which is possible only through sharing sensitive data with another business competitor. This can be eliminated using federated learning, where an organization shares its model updates to help another organization model with a global training data set. This can be achieved with one centralized node that computes the global model by receiving the local updates from multiple organizations and ensuring the privacy of sensitive data. In the different business processes, they share their sensitive monitoring and control information that needs to be stored and shared through trusted cloud services. The ethical and societal impact of AI need to be elevated properly because the industry 5.0 revolution creates more the job opportunities for humans even with vast automation, which need to be addressed for better co-working of humans and cobots in the system.

A. MANAGERIAL AND PRACTICAL LIMITATIONS

Industry 5.0 is a conflux of smart technologies, which are IoT-connected. Thus, the attack boundaries are numerous. Thus, there is no perfect plan of security assessment, that can

TABLE 9: Attack analysis on BC-assisted Industry 5.0 ecosystems

Sr No	Name	Property of BC					
		Immutability	Decentralization	Anonymity	Privacy	Scalability	Smart Contract
1	Block Withholding Attack	*X*	✓	*X*	*X*	✓	*X*
2	51% Attack	✓	✓	*X*	*X*	✓	*X*
3	Selfish Mining	✓	✓	*X*	*X*	✓	*X*
4	Eclipse Attack	✓	✓	*X*	*X*	✓	*X*
5	Sybil Attack	*X*	✓	*X*	*X*	✓	*X*
6	Distributed denial of service	*X*	*X*	*X*	*X*	✓	*X*
7	Re-entrant Attack	*X*	*X*	*X*	*X*	*X*	✓
8	Identity Privacy	*X*	*X*	✓	✓	*X*	*X*
9	Transaction Information	*X*	*X*	✓	✓	*X*	*X*
10	Cryptojacking	*X*	✓	*X*	*X*	✓	*X*
11	Flash loan	*X*	*X*	*X*	*X*	*X*	✓
12	Rug pulls	*X*	*X*	*X*	*X*	*X*	✓

✓: Parameter affected by the attack, *X*: Parameter not affected by the attack

cover over a wide range of attack vectors. During the deployment phase, attacks on authentication, integrity, and availability are common. At the resource management front, massive machine-to-human (M2H) communication takes place over nodes. The IoT devices should be registered before communication in the network, so that trust management is present. Industry 5.0 should be scalable that connects billions of devices and be lightweight to be easy to deploy. The business organization shares and exchanges information in the different processes using third-party unsecured channels. Thus, the integrity of data exchanged and access control mechanisms to use such private and sensitive information must be maintained. The stakeholders access the data at different system points to evaluate the alignment of services and create a need to maintain strong auditability in the system that requires a logging functionality.

When system process interacts with other entity in open BC P2P network, there are chances that private information or the system become vulnerable. TABLE 9 presents the possible attacks in BC-assisted smart manufacturing, and how each attack affect the system property. Attacks are classified in three classes- mining, network communication and privacy, as outlined in section V. The table showcases which property of BC is effected by the attack, and thus effective analysis is required to mitigate the counter effects. For the same, AI models are an effective choice of integration in BC-assisted Industry 5.0 ecosystems.

At the practical front, the advancements in industry 5.0 have forced multiple organizations and working units to be connected. Thus, scaling manpower and organization processes is equally important. The problem is non-deterministic, as it is not known in advance about the required level of automation and human control to obtain optimal control on processes, as defined in the service level agreement. Scaling any organization requires skilled manpower, which makes it essential to provide systematic training to the manpower who will operate the machinery during uncertain situations and failure. The full adoption of industry 5.0 in the current situation follows the regulations and policies that are decided by the policymaker in general to avoid legal issues.

VIII. CONCLUSION

The proposed survey provides useful insights to the readers about the role of BC as a potential enabler to induce trust in Industry 5.0. We discussed the supportive technologies that built the Industry 5.0 vision and justified the integration of BC as a key security enabler in the Industry 5.0 processes. We aligned our discussion through a proposed BC-assisted reference architecture to support the Industry 5.0 verticals like smart healthcare, manufacturing, digital twins, cobots, and others. To summarize, BC-enabled Industry 5.0 would secure the CPS perimeters and improve end-user satisfaction through automation in transactional payments via SCs. We presented a solution taxonomy of assisted verticals of Industry 5.0 and presented the open issues and challenges in practical deployments. We also suggested that BC is not the universal solution, and presented open attacks on BC, with future directions to mitigate the attacks. Finally, a unified case study on BC-assisted digital twin production for Industry 5.0 is presented. We presented the security analysis of the proposed case study, that justifies its practicality in real setups. Finally, the lessons learned from the survey, and conclusions are presented.

As part of the future scope, we aim to design a BC-based trusted architecture for massive human-robot interaction, where the shared data sent to AI models is verifiable on distributed ledgers. The threat and network models would be discussed as part of the underlying architecture and trusted AI solutions would be presented.

REFERENCES

[1] M. Rada, "INDUSTRY 5.0 definition." https://michael-rada.medium.com/industry-5-0-definition-6a2f9922dc48, 2018.
[2] S. Nahavandi, "Industry 5.0—a human-centric solution," Sustainability, vol. 11, no. 16, p. 4371, 2019.
[3] F. Longo, A. Padovano, and S. Umbrello, "Value-oriented and ethical technology engineering in industry 5.0: a human-centric perspective for the design of the factory of the future," Applied Sciences, vol. 10, no. 12, p. 4182, 2020.
[4] B. Friedman and D. G. Hendry, Value sensitive design: Shaping technology with moral imagination. Mit Press, 2019.
[5] P. J. Koch, M. K. van Amstel, P. Dębska, M. A. Thormann, A. J. Tetzlaff, S. Bøgh, and D. Chrysostomou, "A skill-based robot co-worker for industrial maintenance tasks," Procedia Manufacturing, vol. 11, pp. 83–90, 2017.
[6] P. L. Show, K. W. Chew, and T. C. Ling, The Prospect of Industry 5.0 in Biomanufacturing. CRC Press, 2021.

[7] P. K. R. Maddikunta, Q.-V. Pham, B. Prabadevi, N. Deepa, K. Dev, T. R. Gadekallu, R. Ruby, and M. Liyanage, "Industry 5.0: a survey on enabling technologies and potential applications," Journal of Industrial Information Integration, p. 100257, 2021.

[8] Y. Lu, X. Xu, and L. Wang, "Smart manufacturing process and system automation – a critical review of the standards and envisioned scenarios," Journal of Manufacturing Systems, vol. 56, pp. 312–325, 2020.

[9] K. A. Demir, G. Döven, and B. Sezen, "Industry 5.0 and human-robot co-working," Procedia Computer Science, 2019.

[10] S. Tanwar, A. Popat, P. Bhattacharya, R. Gupta, and N. Kumar, "A taxonomy of energy optimization techniques for smart cities: Architecture and future directions," Expert Systems, vol. n/a, no. n/a, p. e12703.

[11] D.-J. Lee, J.-H. Ahn, and Y. Bang, "Managing consumer privacy concerns in personalization: A strategic analysis of privacy protection," MIS Quarterly, vol. 35, pp. 423–444, 06 2011.

[12] S. R. Singh, H. Mithaiwala, N. Chauhan, P. Shah, C. Trivedi, and U. P. Rao, "Decentralized blockchain-based framework for securing review system," in Security, Privacy and Data Analytics (U. P. Rao, S. J. Patel, P. Raj, and A. Visconti, eds.), (Singapore), pp. 239–255, Springer Singapore, 2022.

[13] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, "Blochie: A blockchain-based platform for healthcare information exchange," in 2018 IEEE International Conference on Smart Computing (SMARTCOMP), Taormina, Italy, pp. 49–56, 2018.

[14] P. Bhattacharya, D. Saraswat, A. Dave, M. Acharya, S. Tanwar, G. Sharma, and I. E. Davidson, "Coalition of 6g and blockchain in ar/vr space: Challenges and future directions," IEEE Access, vol. 9, pp. 168455–168484, 2021.

[15] J. Van and T. S. W. C. Tribune, "Mechanical advantage." https://www.chicagotribune.com/news/ct-xpm-1996-12-11-9612110101-story.html, 1996. [Online; accessed 03-04-2022].

[16] R. Gupta, S. Tanwar, M. S. Obaidat, S. Tyagi, and N. Kumar, "Capsule: All you need to know about tactile internet in a nutshell," in 2021 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI), pp. 1–5, 2021.

[17] K. Dev, K. F. Tsang, and J. M. Corchado, "The era of industry 5.0 - technologies from no recognizable h-m interface to hearty touch personal products," IEEE Transactions on Industrial Informatics, pp. 1–1, 2022.

[18] P. Zhang, Y. Hong, N. Kumar, M. Alazab, M. Alshehri, and C. Jiang, "Bc-edgefl: Defensive transmission model based on blockchain assisted reinforced federated learning in iiot environment," IEEE Transactions on Industrial Informatics, vol. PP, pp. 1–1, 09 2021.

[19] A. Srivastava, P. Bhattacharya, A. Singh, A. Mathur, U. Pradesh, and U. Pradesh, "A systematic review on evolution of blockchain generations," International Journal of Information Technology and Electrical Engineering, vol. 7, no. 6, pp. 1–8, 2018.

[20] R. Gupta, A. Kumari, and S. Tanwar, "Fusion of blockchain and ai for secure drone networking underlying 5g communications," Transactions on Emerging Telecommunications Technologies, vol. 32, 11 2020.

[21] V. Kebande, F. Awaysheh, I. Adeyemi, S. Alawadi, and M. Alshehri, "A blockchain-based multi-factor authentication model for cloud-enabled internet of vehicles," Sensors, 09 2021.

[22] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh, and W.-C. Hong, "A survey on decentralized consensus mechanisms for cyber physical systems," IEEE Access, vol. 8, pp. 54371–54401, 2020.

[23] M. Chen, T. Malook, A. Rehman, Y. Muhammad, M. Alshehri, A. Akbar, M. Bilal, and M. Khan, "Blockchain-enabled healthcare system for detection of diabetes," Journal of Information Security and Applications, vol. 58, p. 102771, 02 2021.

[24] A. Kumari, D. Vekaria, R. Gupta, and S. Tanwar, "Redills: Deep learning-based secure data analytic framework for smart grid systems," in 2020 IEEE International Conference on Communications Workshops (ICC Workshops), pp. 1–6, 2020.

[25] N. S. Patel, P. Bhattacharya, S. B. Patel, S. Tanwar, N. Kumar, and H. Song, "Blockchain-envisioned trusted random oracles for iot-enabled probabilistic smart contracts," IEEE Internet of Things Journal, vol. 8, no. 19, pp. 14797–14809, 2021.

[26] Y. Li, B. Cao, M. Peng, L. Zhang, L. Zhang, D. Feng, and J. Yu, "Direct acyclic graph-based ledger for internet of things: Performance and security analysis," IEEE/ACM Transactions on Networking, vol. 28, no. 4, pp. 1643–1656, 2020.

[27] P. Zhang, M. A. Walker, J. White, D. C. Schmidt, and G. Lenz, "Metrics for assessing blockchain-based healthcare decentralized apps," in 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), Dalian, China, pp. 1–4, IEEE, 2017.

[28] B. Duan, Y. Zhong, and D. Liu, "Education application of blockchain technology: Learning outcome and meta-diploma," in 2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS), Shenzhen, China, pp. 814–817, IEEE, 2017.

[29] W. Liu, S. Zhu, T. Mundie, and U. Krieger, "Advanced block-chain architecture for e-health systems," in 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), Dalian, China, pp. 1–6, IEEE, 2017.

[30] I. Radanović and R. Likić, "Opportunities for use of blockchain technology in medicine," Applied health economics and health policy, vol. 16, no. 5, pp. 583–590, 2018.

[31] I. Konstantinidis, G. Siaminos, C. Timplalexis, P. Zervas, V. Peristeras, and S. Decker, "Blockchain for business applications: A systematic literature review," in International Conference on Business Information Systems, Berlin, Germany, pp. 384–399, Springer, 2018.

[32] N. M. Kumar, "Blockchain: Enabling wide range of services in distributed energy system," Beni-Suef University journal of basic and applied sciences, vol. 7, no. 4, pp. 701–704, 2018.

[33] D. Dave, S. Parikh, R. Patel, and N. Doshi, "A survey on blockchain technology and its proposed solutions," Procedia Computer Science, vol. 160, pp. 740–745, 2019.

[34] 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. 117134–117151, 2019.

[35] U. Bodkhe, S. Tanwar, K. Parekh, P. Khanpara, S. Tyagi, N. Kumar, and M. Alazab, "Blockchain for industry 4.0: A comprehensive review," IEEE Access, vol. 8, pp. 79764–79800, 2020.

[36] J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in healthcare 4.0," Computer Communications, vol. 153, pp. 311–335, 2020.

[37] D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, "A survey on blockchain for information systems management and security," Information Processing & Management, vol. 58, no. 1, p. 102397, 2021.

[38] R. Kumar, P. Gupta, S. Singh, and D. Jain, "Human empowerment by industry 5.0 in digital era: Analysis of enablers," Advances in Industrial and Production Engineering: Select Proceedings of FLAME 2020, p. 401, 2021.

[39] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "Omniledger: A secure, scale-out, decentralized ledger via sharding," pp. 583–598, 05 2018.

[40] U. Bodkhe, P. Bhattacharya, S. Tanwar, S. Tyagi, N. Kumar, and M. S. Obaidat, "Blohost: Blockchain enabled smart tourism and hospitality management," in 2019 International Conference on Computer, Information and Telecommunication Systems (CITS), Beijing, China, pp. 1–5, 2019.

[41] P. Bhatttacharya, K. Patel, M. Zuhair, and C. Trivedi, "A lightweight authentication via unclonable functions for industrial internet-of-things," in 2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM), Gautam Buddha Nagar, India, vol. 2, pp. 657–662, 2022.

[42] B. A. Kitchenham and S. L. Pfleeger, "Principles of survey research part 2: Designing a survey," SIGSOFT Softw. Eng. Notes, vol. 27, p. 18–20, jan 2002.

[43] D. Saraswat, A. Verma, P. Bhattacharya, S. Tanwar, G. Sharma, P. N. Bokoro, and R. Sharma, "Blockchain-based federated learning in uavs beyond 5g networks: A solution taxonomy and future directions," IEEE Access, vol. 10, pp. 33154–33182, 2022.

[44] R. Gupta, P. Bhattacharya, S. Tanwar, N. Kumar, and S. Zeadally, "Garuda: A blockchain-based delivery scheme using drones for healthcare 5.0 applications," IEEE Internet of Things Magazine, vol. 4, no. 4, pp. 60–66, 2021.

[45] A. Srivastava, P. Bhattacharya, A. Singh, A. Mathur, O. Prakash, and R. Pradhan, "A distributed credit transfer educational framework based on blockchain," in 2018 Second International Conference on Advances in Computing, Control and Communication Technology (IAC3T), Allahabad, India, pp. 54–59, 2018.

[46] R. Gupta, S. Tanwar, and N. Kumar, "Blockchain and 5g integrated softwarized uav network management: Architecture, solutions, and challenges," Physical Communication, p. 101355, 2021.

[47] A. Verma, P. Bhattacharya, M. Zuhair, S. Tanwar, and N. Kumar, "Vacochain: Blockchain-based 5g-assisted uav vaccine distribution scheme

for future pandemics," IEEE Journal of Biomedical and Health Informatics, pp. 1–1, 2021.

[48] P. Bhattacharya, A. Shukla, S. Tanwar, N. Kumar, and R. Sharma, "6blocks: 6g-enabled trust management scheme for decentralized autonomous vehicles," Computer Communications, vol. 191, pp. 53–68, 2022.

[49] P. Bhattacharya, S. Tanwar, U. Bodkhe, A. Kumar, and N. Kumar, "Evblocks: A blockchain-based secure energy trading scheme for electric vehicles underlying 5g-v2x ecosystems," Wireless Personal Communications, pp. 1–41, 2021.

[50] M. Zuhair, F. Patel, D. Navapara, P. Bhattacharya, and D. Saraswat, "Blocov6: A blockchain-based 6g-assisted uav contact tracing scheme for covid-19 pandemic," in 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, pp. 271–276, 2021.

[51] Z. Zhong, M. Xu, M. A. Rodriguez, C. Xu, and R. Buyya, "Machine learning-based orchestration of containers: A taxonomy and future directions," ACM Comput. Surv., jan 2022. Just Accepted.

[52] A. Devulkar and M. Awwad, "Blockchain and the internet of things: A literature review," 12 2020.

[53] H. F. Atlam and G. B. Wills, "Technical aspects of blockchain and iot," in Advances in Computers, vol. 115, pp. 1–39, Elsevier, 2019.

[54] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, "Survey on blockchain for internet of things," Computer Communications, vol. 136, pp. 10–29, 2019.

[55] A. Kumari, S. Tanwar, S. Tyagi, N. Kumar, M. Maasberg, and K.-K. R. Choo, "Multimedia big data computing and internet of things applications: A taxonomy and process model," Journal of Network and Computer Applications, vol. 124, pp. 169–195, 2018.

[56] P. K. Sharma and J. H. Park, "Blockchain based hybrid network architecture for the smart city," Future Generation Computer Systems, vol. 86, pp. 650–655, 2018.

[57] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in 2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS), Sydney, NSW, Australia, pp. 1392–1393, IEEE, 2016.

[58] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, "Blockchain for 5g-enabled iot for industrial automation: A systematic review, solutions, and challenges," Mechanical Systems and Signal Processing, vol. 135, p. 106382, 2020.

[59] R. Rivera, J. G. Robledo, V. M. Larios, and J. M. Avalos, "How digital identity on blockchain can contribute in a smart city environment," in 2017 International smart cities conference (ISC2), Wuxi, China, pp. 1–4, IEEE, 2017.

[60] C. Lazaroiu and M. Roscia, "Smart district through iot and blockchain," in 2017 IEEE 6th international conference on renewable energy research and applications (ICRERA), San Diego, CA, USA, pp. 454–461, IEEE, 2017.

[61] D.-Y. Liao and X. Wang, "Design of a blockchain-based lottery system for smart cities applications," in 2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC), San Jose, CA, USA, pp. 275–282, IEEE, 2017.

[62] J. Vora, P. Italiya, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and K.-F. Hsiao, "Ensuring privacy and security in e-health records," in 2018 International conference on computer, information and telecommunication systems (CITS), Alsace, Colmar, France, pp. 1–5, IEEE, 2018.

[63] S. Tanwar, S. Tyagi, and N. Kumar, Security and Privacy of Electronic Healthcare Records: Concepts, Paradigms and Solutions. Institution of Engineering and Technology, 2019.

[64] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," Journal of medical systems, vol. 40, no. 10, pp. 1–8, 2016.

[65] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in 2016 2nd international conference on open and big data (OBD), Vienna, Austria, pp. 25–30, IEEE, 2016.

[66] H. Wang and Y. Song, "Secure cloud-based ehr system using attribute-based cryptosystem and blockchain," Journal of medical systems, vol. 42, no. 8, pp. 1–9, 2018.

[67] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," IEEE access, vol. 6, pp. 11676–11686, 2018.

[68] H. Kaur, M. A. Alam, R. Jameel, A. K. Mourya, and V. Chang, "A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment," Journal of medical systems, vol. 42, no. 8, pp. 1–11, 2018.

[69] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," Journal of medical systems, vol. 42, no. 7, pp. 1–7, 2018.

[70] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "Continuous patient monitoring with a patient centric agent: A block architecture," IEEE Access, vol. 6, pp. 32700–32726, 2018.

[71] Y. Sun, R. Zhang, X. Wang, K. Gao, and L. Liu, "A decentralizing attribute-based signature for healthcare blockchain," in 2018 27th International conference on computer communication and networks (ICCCN), Hangzhou, China, pp. 1–9, IEEE, 2018.

[72] S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, "Blockchain technology in healthcare: A comprehensive review and directions for future research," Applied sciences, vol. 9, no. 9, p. 1736, 2019.

[73] P. Bhattacharya, S. Tanwar, U. Bodke, S. Tyagi, and N. Kumar, "Bindaas: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications," IEEE Transactions on Network Science and Engineering, 2019.

[74] A. Tandon, A. Dhir, A. N. Islam, and M. Mäntymäki, "Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda," Computers in Industry, vol. 122, p. 103290, 2020.

[75] E. Chukwu and L. Garg, "A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations," IEEE Access, vol. 8, pp. 21196–21214, 2020.

[76] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, "Healthblock: A secure blockchain-based healthcare data management system," Computer Networks, vol. 200, p. 108500, 2021.

[77] U. Chelladurai and S. Pandian, "A novel blockchain based electronic health record automation system for healthcare," Journal of Ambient Intelligence and Humanized Computing, vol. 13, no. 1, pp. 693–703, 2022.

[78] J. Zhang, N. Xue, and X. Huang, "A secure system for pervasive social network-based healthcare," Ieee Access, vol. 4, pp. 9239–9250, 2016.

[79] A. Nayyar, Handbook of Cloud Computing: Basic to Advance research on the concepts and design of Cloud Computing. BPB Publications, 2019.

[80] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "How blockchain could empower ehealth: An application for radiation oncology," in VLDB Workshop on Data Management and Analytics for Medicine and Healthcare, pp. 3–6, Springer, 2017.

[81] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "Medshare: Trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, vol. 5, pp. 14757–14767, 2017.

[82] N. Rifi, E. Rachkidi, N. Agoulmine, and N. C. Taher, "Towards using blockchain technology for ehealth data access management," in 2017 fourth international conference on advances in biomedical engineering (ICABME), Beirut, Lebanon, pp. 1–4, IEEE, 2017.

[83] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC), pp. 1–5, IEEE, 2017.

[84] G. Magyar, "Blockchain: Solving the privacy and research availability tradeoff for ehr data: A new disruptive technology in health data management," in 2017 IEEE 30th Neumann Colloquium (NC), pp. 000135–000140, IEEE, 2017.

[85] A. Theodouli, S. Arakliotis, K. Moschou, K. Votis, and D. Tzovaras, "On the design of a blockchain-based system to facilitate healthcare data sharing," in 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, pp. 1374–1379, IEEE, 2018.

[86] M. Samaniego and R. Deters, "Hosting virtual iot resources on edge-hosts with blockchain," in 2016 IEEE International conference on computer and information technology (CIT), Nadi, Fiji, pp. 116–119, IEEE, 2016.

[87] A. Kumari, S. Tanwar, S. Tyagi, and N. Kumar, "Fog computing for healthcare 4.0 environment: Opportunities and challenges," Computers & Electrical Engineering, vol. 72, pp. 1–13, 2018.

[88] M. A. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges," Future generation computer systems, vol. 82, pp. 395–411, 2018.

[89] M. Singh, A. Singh, and S. Kim, "Blockchain: A game changer for securing iot data," in 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), pp. 51–55, IEEE, 2018.

[90] M. Pustišek and A. Kos, "Approaches to front-end iot application development for the ethereum blockchain," Procedia Computer Science, vol. 129, pp. 410–419, 2018.

[91] S. Huh, S. Cho, and S. Kim, "Managing iot devices using blockchain platform," in 2017 19th international conference on advanced communication technology (ICACT), PyeongChang, Korea (South), pp. 464–467, IEEE, 2017.

[92] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with iot. challenges and opportunities," Future generation computer systems, vol. 88, pp. 173–190, 2018.

[93] Z. Li, L. Liu, A. V. Barenji, and W. Wang, "Cloud-based manufacturing blockchain: Secure knowledge sharing for injection mould redesign," Procedia Cirp, vol. 72, pp. 961–966, 2018.

[94] A. E. C. Mondragon, C. E. C. Mondragon, and E. S. Coronado, "Exploring the applicability of blockchain technology to enhance manufacturing supply chains in the composite materials industry," in 2018 IEEE International conference on applied system invention (ICASI), Chiba, Japan, pp. 1300–1303, IEEE, 2018.

[95] R. Winkler-Goldstein, F. Imbault, T. Usländer, and H. de la Gastine, "Fractal production reprogramming "industrie 4.0" around resource and energy efficiency?," in 2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), Palermo, Italy, pp. 1–5, IEEE, 2018.

[96] A. Angrish, B. Craver, M. Hasan, and B. Starly, "A case study for blockchain in manufacturing:"fabrec": A prototype for peer-to-peer network of manufacturing nodes," Procedia Manufacturing, vol. 26, pp. 1180–1192, 2018.

[97] A. V. Barenji, Z. Li, and W. M. Wang, "Blockchain cloud manufacturing: Shop floor and machine level," in Smart SysTech 2018; European Conference on Smart Objects, Systems and Technologies, Munich, Germany, pp. 1–6, VDE, 2018.

[98] T. Kobzan, A. Biendarra, S. Schriegel, T. Herbst, T. Müller, and J. Jasperneite, "Utilizing blockchain technology in industrial manufacturing with the help of network simulation," in 2018 IEEE 16th International Conference on Industrial Informatics (INDIN), Porto, Portugal, pp. 152–159, IEEE, 2018.

[99] P. Rimba, A. B. Tran, I. Weber, M. Staples, A. Ponomarev, and X. Xu, "Comparing blockchain and cloud services for business process execution," in 2017 IEEE International Conference on Software Architecture (ICSA), pp. 257–260, IEEE, 2017.

[100] L.-N. Lundbaek and M. Huth, "Oligarchic control of business-to-business blockchains," in 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 68–71, IEEE, 2017.

[101] X. Wang, X. Xu, L. Feagan, S. Huang, L. Jiao, and W. Zhao, "Inter-bank payment system on enterprise blockchain platform," in 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, pp. 614–621, IEEE, 2018.

[102] B. Carminati, C. Rondanini, and E. Ferrari, "Confidential business process execution on blockchain," in 2018 ieee international conference on web services (icws), San Francisco, CA, USA, pp. 58–65, IEEE, 2018.

[103] J. Mendling, I. Weber, W. V. D. Aalst, J. V. Brocke, C. Cabanillas, F. Daniel, S. Debois, C. D. Ciccio, M. Dumas, S. Dustdar, et al., "Blockchains for business process management-challenges and opportunities," ACM Transactions on Management Information Systems (TMIS), vol. 9, no. 1, pp. 1–16, 2018.

[104] H. Johng, D. Kim, T. Hill, and L. Chung, "Using blockchain to enhance the trustworthiness of business processes: a goal-oriented approach," in 2018 IEEE international conference on services computing (SCC), San Francisco, CA, USA, pp. 249–252, IEEE, 2018.

[105] K. S. Jhala, R. Oak, and M. Khare, "Smart collaboration mechanism using blockchain technology," in 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Shanghai, China, pp. 117–121, IEEE, 2018.

[106] M. Attaran and A. Gunasekaran, "Blockchain principles, qualities, and business applications," in Applications of blockchain technology in business, pp. 13–20, Springer, 2019.

[107] S. B. Patel, H. A. Kheruwala, M. Alazab, N. Patel, R. Damani, P. Bhattacharya, S. Tanwar, and N. Kumar, "Biouav: Blockchain-envisioned framework for digital identification to secure access in next-generation uavs," in Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond, DroneCom '20, (New York, NY, USA), p. 43–48, Association for Computing Machinery, 2020.

[108] V. A. Patel, P. Bhattacharya, S. Tanwar, N. K. Jadav, and R. Gupta, "Bfledge: Blockchain based federated edge learning scheme in v2x underlying 6g communications," in 2022 12th International Conference on Cloud Computing, Data Science Engineering (Confluence), pp. 146–152, 2022.

[109] V. Strobel, E. Castelló Ferrer, and M. Dorigo, "Managing byzantine robots via blockchain technology in a swarm robotics collective decision making scenario," 2018.

[110] E. C. Ferrer, "The blockchain: a new framework for robotic swarm systems," in Proceedings of the future technologies conference, pp. 1037–1058, Vancouver, Canada, Springer, 2018.

[111] P. Bhattacharya, S. Tanwar, R. Shah, and A. Ladha, "Mobile edge computing-enabled blockchain framework—a survey," in Proceedings of ICRIC 2019 (P. K. Singh, A. K. Kar, Y. Singh, M. H. Kolekar, and S. Tanwar, eds.), (Cham), pp. 797–809, Springer International Publishing, 2020.

[112] A. Verma, P. Bhattacharya, U. Bodkhe, M. Zuhair, and R. K. Dewangan, "Blockchain-based federated cloud environment: Issues and challenges," Blockchain for Information Security and Privacy, pp. 155–176, 2021.

[113] R. Gupta, D. Reebadiya, and S. Tanwar, "6g-enabled edge intelligence for ultra -reliable low latency applications: Vision and mission," Computer Standards & Interfaces, vol. 77, p. 103521, 2021.

[114] F. for Traffic Society, "Users' trust in and concerns about automated driving systems." https://aaafoundation.org/wp-content/uploads/2021/04/21-1084-AAAFTS-Users-Trust-Automated-Driving-Systems_April-2021-1.pdf, 2021. [Online; accessed 03-04-2022].

[115] U. Bodkhe, S. Tanwar, P. Bhattacharya, and N. Kumar, "Blockchain for precision irrigation: Opportunities and challenges," Transactions on Emerging Telecommunications Technologies, vol. n/a, no. n/a, p. e4059.

[116] H. Xiong, T. Dalhaus, P. Wang, and J. Huang, "Blockchain technology for agriculture: applications and rationale," frontiers in Blockchain, vol. 3, p. 7, 2020.

[117] J. Lin, Z. Shen, A. Zhang, and Y. Chai, "Blockchain and iot based food traceability for smart agriculture," in Proceedings of the 3rd International Conference on Crowd Science and Engineering, Singapore Singapore, pp. 1–6, 2018.

[118] Y.-P. Lin, J. R. Petway, J. Anthony, H. Mukhtar, S.-W. Liao, C.-F. Chou, and Y.-F. Ho, "Blockchain: The evolutionary next step for ict e-agriculture," Environments, vol. 4, no. 3, p. 50, 2017.

[119] M. Mittal, Energy conservation for IOT devices concepts, Paradigms and solutions. Springer, 2019.

[120] J. Truby, "Decarbonizing bitcoin: Law and policy choices for reducing the energy consumption of blockchain technologies and digital currencies," Energy research & social science, vol. 44, pp. 399–410, 2018.

[121] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, and A. Peacock, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," Renewable and Sustainable Energy Reviews, vol. 100, pp. 143–174, 2019.

[122] S. Singh and N. Singh, "Blockchain: Future of financial and cyber security," in 2016 2nd international conference on contemporary computing and informatics (IC3I), Greater Noida, India, pp. 463–467, IEEE, 2016.

[123] A. Goranović, M. Meisel, L. Fotiadis, S. Wilker, A. Treytl, and T. Sauter, "Blockchain applications in microgrids an overview of current projects and concepts," in IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society, Beijing, China, pp. 6153–6158, IEEE, 2017.

[124] A. Meeuw, S. Schopfer, and F. Wortmann, "Experimental bandwidth benchmarking for p2p markets in blockchain managed microgrids," Energy Procedia, vol. 159, pp. 370–375, 2019.

[125] A. K. Shrestha and J. Vassileva, "Towards decentralized data storage in general cloud platform for meta-products," in Proceedings of the International Conference on Big Data and Advanced Wireless Technologies, Blagoevgrad Bulgaria, pp. 1–7, 2016.

[126] C. Tenopir, C. L. Palmer, L. Metzer, J. van der Hoeven, and J. Malone, "Sharing data: Practices, barriers, and incentives," Proceedings of the American Society for Information Science and Technology, vol. 48, no. 1, pp. 1–4, 2011.

[127] A. Meadows, "To share or not to share? that is the (research data) question. . . | the scholarly kitchen," 2014.

[128] S. Poslad, Ubiquitous computing: smart devices, environments and interactions. John Wiley & Sons, 2011.
[129] A. K. Shrestha, "Security of sip-based infrastructure against malicious message attacks," in The 8th International Conference on Software, Knowledge, Information Management and Applications (SKIMA 2014), Dhaka, Bangladesh, pp. 1–8, IEEE, 2014.
[130] R. Kanagavelu, Z. Li, J. Samsudin, S. Hussain, F. Yang, Y. Yang, R. S. M. Goh, and M. Cheah, "Federated learning for advanced manufacturing based on industrial iot data analytics," Implementing Industry 4.0, p. 143, 2021.
[131] A. K. Shrestha, J. Vassileva, and R. Deters, "A blockchain platform for user data sharing ensuring user control and incentives," Frontiers in Blockchain, vol. 3, p. 48, 2020.
[132] P. Dolog and J. Vassileva, "Decentralized, agent based and social approaches to user modelling," in Workshop DASUM-05, at the 9th International Conference on User Modeling (UM'05), Edinburgh, Scotland, Citeseer, 2005.
[133] F. Carmagnola, F. Cena, and C. Gena, "User model interoperability: a survey," User Modeling and User-Adapted Interaction, vol. 21, no. 3, pp. 285–331, 2011.
[134] J. Vassileva, G. McCalla, and J. Greer, "Multi-agent multi-user modeling in i-help," User Modeling and User-Adapted Interaction, vol. 13, no. 1, pp. 179–210, 2003.
[135] D. Vrandečić and M. Krötzsch, "Wikidata: a free collaborative knowledgebase," Communications of the ACM, vol. 57, no. 10, pp. 78–85, 2014.
[136] F. Abel, E. Herder, G.-J. Houben, N. Henze, and D. Krause, "Cross-system user modeling and personalization on the social web," User Modeling and User-Adapted Interaction, vol. 23, no. 2, pp. 169–209, 2013.
[137] A. Davoust, Decentralized Social Data Sharing. PhD thesis, Carleton University, 2015.
[138] A. Verma, P. Bhattacharya, U. Bodkhe, A. Ladha, and S. Tanwar, "Dams: Dynamic association for view materialization based on rule mining scheme," in The International Conference on Recent Innovations in Computing, Jammu, India, pp. 529–544, Springer, 2020.
[139] J. Iyilade and J. Vassileva, "A decentralized architecture for sharing and reusing lifelogs.," in UMAP Workshops, Citeseer, 2013.
[140] K. Thilakarathna, H. Petander, J. Mestre, and A. Seneviratne, "Mobitribe: Cost efficient distributed user generated content sharing on smartphones," IEEE Transactions on Mobile Computing, vol. 13, no. 9, pp. 2058–2070, 2013.
[141] M. Assad, D. J. Carmichael, J. Kay, and B. Kummerfeld, "Personisad: Distributed, active, scrutable model framework for context-aware services," in International Conference on Pervasive Computing, New York, USA, pp. 55–72, Springer, 2007.
[142] E. Dim and T. Kuflik, "User models sharing and reusability: a component-based approach.," in UMAP Workshops, 2012.
[143] I. Stoica, R. Morris, D. Liben-Nowell, D. R. Karger, M. F. Kaashoek, F. Dabek, and H. Balakrishnan, "Chord: a scalable peer-to-peer lookup protocol for internet applications," IEEE/ACM Transactions on networking, vol. 11, no. 1, pp. 17–32, 2003.
[144] M. M. Queiroz and S. F. Wamba, "Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in india and the usa," International Journal of Information Management, vol. 46, pp. 70–82, 2019.
[145] F. Tian, "A supply chain traceability system for food safety based on haccp, blockchain & internet of things," in 2017 International conference on service systems and service management, Dalian, China, pp. 1–6, IEEE, 2017.
[146] M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda, "Blockchain-based traceability in agri-food supply chain management: A practical implementation," in 2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany), pp. 1–4, IEEE, 2018.
[147] G. Perboli, S. Musso, and M. Rosano, "Blockchain in logistics and supply chain: A lean approach for designing real-world use cases," Ieee Access, vol. 6, pp. 62018–62028, 2018.
[148] I. Weber, X. Xu, R. Riveret, G. Governatori, A. Ponomarev, and J. Mendling, "Untrusted business process monitoring and execution using blockchain," in International Conference on Business Process Management, Rome, Italy, pp. 329–347, Springer, 2016.
[149] S. Guerreiro, S. J. van Kervel, and E. Babkin, "Towards devising an architectural framework for enterprise operating systems.," in ICSOFT, pp. 578–585, 2013.
[150] K. Leng, Y. Bi, L. Jing, H.-C. Fu, and I. Van Nieuwenhuyse, "Research on agricultural supply chain system with double chain architecture based on blockchain technology," Future Generation Computer Systems, vol. 86, pp. 641–649, 2018.
[151] D. Mao, F. Wang, Z. Hao, and H. Li, "Credit evaluation system based on blockchain for multiple stakeholders in the food supply chain," International journal of environmental research and public health, vol. 15, no. 8, p. 1627, 2018.
[152] N. Kshetri, "1 blockchain's roles in meeting key supply chain management objectives," International Journal of Information Management, vol. 39, pp. 80–89, 2018.
[153] A. Verma, P. Bhattacharya, D. Saraswat, and S. Tanwar, "Nyaya: Blockchain-based electronic law record management scheme for judicial investigations," Journal of Information Security and Applications, vol. 63, p. 103025, 2021.
[154] S. Shyamsukha, P. Bhattacharya, F. Patel, S. Tanwar, R. Gupta, and E. Pricop, "Porf: Proof-of-reputation-based consensus scheme for fair transaction ordering," in 2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Pitesti, Romania, pp. 1–6, 2021.
[155] Y. Chen, H. Chen, Y. Zhang, M. Han, M. Siddula, and Z. Cai, "A survey on blockchain systems: Attacks, defenses, and privacy preservation," High-Confidence Computing, vol. 2, no. 2, p. 100048, 2022.
[156] H. Guo and X. Yu, "A survey on blockchain technology and its security," Blockchain: Research and Applications, vol. 3, no. 2, p. 100067, 2022.
[157] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," self-published paper, August, vol. 19, no. 1, 2012.
[158] J. Bae and H. Lim, "Random mining group selection to prevent 51% attacks on bitcoin," in 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), pp. 81–82, IEEE, 2018.
[159] X. Yang, Y. Chen, and X. Chen, "Effective scheme against 51proof-of-work blockchain with history weighted information," in 2019 IEEE International Conference on Blockchain (Blockchain), pp. 261–265, 2019.
[160] M. Saad, L. Njilla, C. Kamhoua, and A. Mohaisen, "Countering selfish mining in blockchains," in 2019 International Conference on Computing, Networking and Communications (ICNC), pp. 360–364, 2019.
[161] E. Heilman, "One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner (poster abstract)," in Financial Cryptography and Data Security (R. Böhme, M. Brenner, T. Moore, and M. Smith, eds.), (Berlin, Heidelberg), pp. 161–162, Springer Berlin Heidelberg, 2014.
[162] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse attacks on Bitcoin's Peer-to-Peer network," in 24th USENIX Security Symposium (USENIX Security 15), (Washington, D.C.), pp. 129–144, USENIX Association, Aug. 2015.
[163] S. Zhang and J.-H. Lee, "Double-spending with a sybil attack in the bitcoin decentralized network," IEEE Transactions on Industrial Informatics, vol. 15, no. 10, pp. 5715–5722, 2019.
[164] P. Kumar, R. Kumar, G. P. Gupta, and R. Tripathi, "A distributed framework for detecting ddos attacks in smart contract-based blockchain-iot systems by leveraging fog computing," Transactions on Emerging Telecommunications Technologies, vol. 32, no. 6, p. e4112, 2021.
[165] B. Jia and Y. Liang, "Anti-d chain: A lightweight ddos attack detection scheme based on heterogeneous ensemble learning in blockchain," China Communications, vol. 17, no. 9, pp. 11–24, 2020.
[166] U.-J. Baek, S.-H. Ji, J. T. Park, M.-S. Lee, J.-S. Park, and M.-S. Kim, "Ddos attack detection on bitcoin ecosystem using deep-learning," in 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), pp. 1–4, 2019.
[167] N. Fatima Samreen and M. H. Alalfi, "Reentrancy vulnerability identification in ethereum smart contracts," in 2020 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE), pp. 22–29, 2020.
[168] D. Ron and A. Shamir, "Quantitative analysis of the full bitcoin transaction graph," in Financial Cryptography and Data Security (A.-R. Sadeghi, ed.), (Berlin, Heidelberg), pp. 6–24, Springer Berlin Heidelberg, 2013.