IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 19 July 2024, accepted 17 September 2024, date of publication 26 September 2024, date of current version 21 October 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3468611

SURVEY

The Role of Blockchain in Transforming Industries Beyond Finance

C. VANMATHI[1], AHMED FAROUK[2], SARAH M. ALHAMMAD[3], R. MANGAYARKARASI[1], SWETA BHATTACHARYA[1], AND MEENAVOLU S. B. KASYAPA[1]

[1]School of Computer Science Engineering and Information Systems, Vellore Institute of Technology, Vellore, Tamil Nadu 632014, India
[2]Department of Computer Science, Faculty of Computers and Artificial Intelligence, Hurghada University, Hurghada 83523, Egypt
[3]Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh 11671, Saudi Arabia

Corresponding author: Ahmed Farouk (ahmed.farouk@sci.svu.edu.eg)

This work was supported by Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia, through the Researchers Supporting Project PNURSP2024R442.

ABSTRACT Blockchain technology is rapidly transforming how businesses and individuals interact. Its inherent security features, including immutability, tamper-proofing, and verifiable data provenance, are driving its adoption across numerous sectors. The financial sector heavily influences blockchain for its tamper-proof nature, leading to the rise of cryptocurrencies, the technology offers much more. Beyond security, it streamlines processes, reduces costs, and improves customer experience. Smart contracts are one of the predominant key components that automate predetermined operations, further enhancing blockchain's capabilities. Understanding the importance of blockchain in non-financial applications is crucial for fully exploiting its potential. This analysis explores the fundamentals of blockchain technology and its applications beyond finance. To meet the growing demand across various sectors, blockchain must integrate with other trending technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), and the edge-cloud paradigm. The analysis examines the role of these technologies in facilitating blockchain-enabled applications. Furthermore, the paper researches the specific use cases such as insurance, energy, healthcare, digital voting, supply chain management and government. Concentrating on these sectors elucidates how organisations harness blockchain to tackle intricate challenges, thereby fostering the advancement of sophisticated digital processes and contributing to societal progression.

INDEX TERMS Blockchain, non-financial applications, energy, insurance, healthcare, decentralization.

I. INTRODUCTION

In recent years, digital dependency has sparked a rush to enhance digital data safeguards, reliability, and transparency. Modern technologies present a paradigm shift to address these complicated issues. In this regard, Blockchain Technology has become a disruptive force by offering a unique solution. Initially, Blockchain Technology is intended to serve as the foundational technology for financial applications. Which enables the creation of cryptocurrencies like bitcoin [1]. Blockchain Technology's safe and decentralized system holds the potential to bring revolution beyond financial applications like supply chain management, healthcare, energy, and more by completely transforming the way businesses function, work, and share data.

Although data from reliable sources like Scopus and IEEE suggests that the adoption of non-financial applications is now relatively low, as shown in Figure 1. This study explores how Blockchain Technology is transforming other industries outside of finance. This paper aims to provide a thorough understanding of the profound influence that blockchain is having on the transformation of industries, paving the way for a new era of decentralized, transparent, and efficient business operations. We'll closely examine real-world use cases and industry-specific applications to show how blockchain impacts many industries now or

The associate editor coordinating the review of this manuscript and approving it for publication was Barbara Guidi.

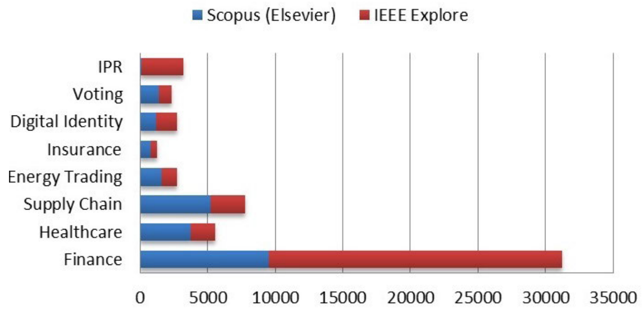


FIGURE 1. Papers published on Scopus and IEEE with Blockchain.

has the potential to do so. Furthermore, the paper will thoroughly examine the obstacles and potential developments related to the extensive integration of blockchain technology throughout many sectors.

A. NON-FINANCIAL APPLICATIONS (NFA)

Though blockchain finds its application in diverse sectors, there are use cases that rely on blockchain to streamline core operations apart from dealing with financial aspects. Modern technologies are revolutionising this non-financial sector by redefining procedures and addressing the issues in various industries, including healthcare, insurance, energy sector, Supply chain management, digital voting and Identity verification. Blockchain technology in healthcare ensures secure and tamper-proof patient records, enhancing data privacy and compliance. It facilitates efficient and transparent data sharing among healthcare providers, improving coordination and patient outcomes. Additionally, blockchain can streamline supply chain management for pharmaceuticals, ensuring the authenticity and safety of medical products. Similarly, in Supply chain management, improving transparency to build trust is worthwhile. Mainly in the cold goods supply chain context, goods temperature throughout the delivery process from source to destination is essential. It is achieved by openness and transparency. Transparency and fraud reduction are enhanced in insurance by blockchain technology through secure, immutable records of transactions and claims. Processes such as underwriting and claims management are also streamlined, improving efficiency and trust between insurers and policyholders. Blockchain technology in the energy sector enables decentralized energy markets, allowing peer-to-peer energy trading and enhancing grid efficiency. It improves transparency and traceability in energy transactions, reducing fraud and ensuring accurate billing. Additionally, blockchain facilitates the integration of renewable energy sources, optimizing energy distribution and promoting sustainability. In digital voting Blockchain ensures secure, transparent, and tamper-proof election processes. In another scenario, like online authentication, use Identity verification for security improvement. Blockchain Technology becomes more evident and prominent in non-financial sectors as it develops. Its intelligent contract automation capability, immutability, and decentralisation will solve long-standing problems and promote efficiency, transparency, and trust across various industries.

II. BLOCKCHAIN PRINCIPLES

A. DECENTRALIZED TECHNOLOGY

A paradigm known as distributed technology is a decentralised recording of information or transactions among a network of users. Blockchain Technology, Inter Planetary File System (IPFS), and Apache Cassandra are prominent technologies in this category. Distributed File Systems (DFS), Distributed Databases, and Distributed Ledger Technology (DLT) are the primary categories of distributed technologies. DFS allows interconnected computers to share data as well as storage resources. It is essential to distributed computing because it offers scalable and effective ways to store and manage information among a network of computers. The best examples are IPFS, Hadoop Distributed File System (HDFS), and Google File System (GFS). Similarly, Data in distributed databases is dispersed among several network nodes or servers. In contrast to conventional centralised databases, which keep all the data on one server, distributed databases store the data on several servers, frequently spread over various geographic regions. The main objectives of distributed databases are fault tolerance, performance, and scalability. The best examples are Apache Cassandra, MongoDB, Amazon DynamoDB, and Microsoft Azure Cosmos DB. Other than the two types of distributed technologies discussed, DLT offers more security. It offers an immutable nature and a duplicate ledger for every user or node. In DLT, data entry is secured and validated through consensus processes. It has been used in many different contexts. Blockchain Technology is one of the best instances of DLT [2]. With blockchain as its underlying technology, DLT has become well-known in the financial sector thanks to cryptocurrencies like Bitcoin [1]. In non-financial applications, blockchain intelligent contracts offer great flexibility by acting as self-executing agreements with conditions. It provides efficiency and confidence by automating and enforcing contractual commitments.

B. BLOCKCHAIN FUNDAMENTALS

Revolutionizing the way data is stored and exchanged, blockchain technology has the potential to transform the way businesses and governments operate, impacting how people interact, transact and consume. Blockchain is a distributed ledger technology that enables records of transactions to be securely stored and replicated across multiple computers. It comprises a vast digital ledger distributed across a decentralized peer-to-peer network, guaranteeing the data's accuracy and integrity. Blocks act as cryptographically protected links in the chain, and each node in the network holds a complete and permanent record of all transactions that have ever occurred. Moreover, cryptographic hashes ensure that any modifications to the data are immediately detected [3]. Additionally, the security of a blockchain network is strengthened by the consensus mechanism [4]. The consensus mechanism is the process by which the network nodes agree on a transaction's validity.

In the blockchain domain, many architectures provide distinct features and applications to meet a range of purposes. These architectures are mentioned in figure 2. Among these, public blockchains are a prominent distributed and public subset, meaning that anybody can access and use the network. Users validate transactions and receive rewards for their efforts by employing validation methods such as Proof-of-Work and Proof-of-Stake. These include Bitcoin [1], Ethereum [5]. Private blockchains, on the other hand, function inside closed systems and only allow transactions with the help of a system administrator. They are appropriate for companies with restricted network access because they emphasize efficiency, scalability, and confidentiality. Hyperledger Fabric [6] and Multichain [7] are two well-known examples. Hybrid blockchains combine elements of their private and public counterparts to provide more control and customization possibilities. This version improves transparency and security by letting users protect particular data using the distributed ledger. Last but not least, consortium blockchains are a hybrid approach in which a group of organizations jointly own and run the blockchain, requiring authorization to access. Quorum and R3 Corda [8] are two instances that highlight the flexibility and diversity of the blockchain ecosystem.

C. BLOCKCHAIN COMPONENTS

1) SMART CONTRACTS

Self-executing or smart contracts have their terms encoded directly into the code. When specific requirements are satisfied, they automatically carry out and enforce contractual agreements. Utilising the security, transparency, and decentralisation that blockchain technology offers, smart contracts run on blockchain platforms. These smart contract adoptions have gone beyond the finance sector to optimise workflows and cut supply chain management and healthcare expenses. One such instance is in supply chain management. When unavoidable circumstances are met, these contracts automatically carry out tasks, including order fulfilment, shipment tracking, and payment processing. It lowers the possibility of fraud and mistakes, increasing efficiency and reducing costs. Similarly, smart contracts ensure that only authorised parties have permission to access and amend health records stored on a blockchain. These are just a glimpse of smart contract usage for non-financial applications in blockchain.

By guaranteeing trust and enabling job automation, smart contracts encourage a variety of fields for blockchain adoption. One of the top blockchain platforms for smart contracts is Ethereum [5]. With many decentralised apps (DApps) and smart contracts installed on its network, it still holds a dominant position in this market. Ethereum primarily uses Solidity for the creation of smart contracts. Chaincode is the term for smart contracts in Hyperledger Fabric [6]. Programming languages used to write chaincode include Go, JavaScript, and Java. The architecture of Hyperledger Fabric enables a more adaptable and modular smart contract design. The ability to run multiple chaincodes on the same channel allows for more customisation. Agreements between parties are referred to as contracts in Corda [8]. Tezos's smart contracts are written in a language known as Michelson [19]. Formal verification is highly valued by Tezos, enabling developers to demonstrate the accuracy of their smart contracts by mathematical means. Overall Smart contracts are more efficient, but they come with drawbacks such as scalability issues, legal recognition issues, and possible coding flaws [20].

2) CONSENSUS ALGORITHM

Consensus algorithms are essential to distributed systems because they provide agreement and trust among various users or parties involved in distributed applications. So it is an integral part of blockchain technology to maintain network integrity and security. The blockchain consensus mechanism has two components: one is sybil resistance, and the other is chain selection. Sybil resistance safeguards against attacks where a single entity controls multiple identities, while chain selection determines the valid chain in the event of conflicts or forks in the blockchain. Proof of Work (PoW) is the initial algorithm used on blockchain platforms like Bitcoin and Ethereum. It has emerged as a prominent algorithm for addressing Sybil resistance on blockchain platforms. POW gives a mathematical problem to solve to validate transactions and create a block, which requires more processing capacity. Hence It creates problems for attackers to create multiple nodes as it involves high costs.

Later, due to the high energy consumption and performance issues for large applications, researchers looked for more efficient alternatives [21]. Proof of Stake (POS) [22] is the most promising replacement for POW. It addressed sybil resistance through staking cryptocurrency tokens rather than computational power. However, emergence of these new mechanisms leads to another problem, like utilizing these new algorithms for already established platforms and applications, which is a complex process. For instance, Ethereum shifted from its initial POW algorithm to POS. To check the working performance and security of this new approach, they created a testing network called The Beacon Chain, and after successful testing, they merged it into the main Ethereum Network, forming Ethereum 2.0 [23]. In addressing the complexities of adopting new consensus mechanisms, Hyperledger, like private blockchain frameworks, gave the option to use their consensus mechanisms. With this flexibility, new applications have the facility to achieve efficiency and scalability by applying new mechanisms, but still, existing applications and network upgrading are complex processes. Several Authors have discussed the popular Consensus metrics in their research, like Ahmad et al. [24] and Hussein et al. [25].

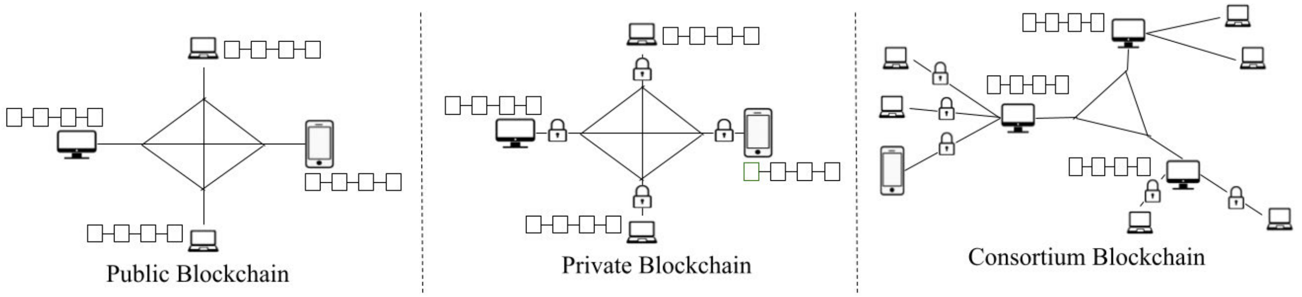


FIGURE 2. Types of blockchain.

In summary, consensus algorithms are vital components of blockchain technology, encompassing Sybil resistance and chain selection. While PoW serves as a crucial component in addressing Sybil resistance, it's essential to recognize that consensus involves multiple components and implementations. Consensus performance is critical for maintaining consistency, fault tolerance, and overall system reliability in systems handling large volumes of data, such as big data analytics, distributed databases, or internet-scale applications. In financial applications, real-time processing is frequently required, yet data quantities are typically smaller, so the consensus algorithm performance effect may be less noticeable. On the other side, the importance of consensus algorithm performance becomes more apparent in non-financial applications, particularly those involving massive datasets. Consensus performance is critical to maintaining consistency, fault tolerance, and overall system reliability in systems that handle large volumes of data.

D. BLOCKCHAIN USECASES

Blockchain technology is widespread, and its applications include cryptocurrency, Data sharing, supply chain management, and Digital voting. Famous use cases of blockchain in both financial and non-financial are mentioned in the figure 3.

1) FINANCIAL APPLICATIONS

Cryptocurrency, the primary application of blockchain technology, is a digital asset that enables fast and secure payment transactions without the need for a third-party facilitator. It relies on cryptographic algorithms for privacy and security. Bitcoin [1] is the perfect example of Cryptocurrency, and most of the Blockchain platforms have their own Cryptocurrency. Similarly, cross-border transactions are another use case. Efficiency and simplification of international money transfers can be enhanced using Blockchain Technology. Quicker and more affordable cross-border payments are possible through the removal of many intermediaries, a reduction in processing times, and an improvement in transparency. Ripple is a well-known platform used for cross-border payments [9]. Currency exchange is also a famous use case, similar to cross-border payments. Uniswap is one of the examples of currency exchange with Blockchain, which works with Ethereum Blockchain [10]. Another prominent use case is Trading. Depending on the context, it can have both financial and non-financial applications. The company tZero introduced a Trading-based application in 2023 [11], which is the product of Overstock.com.

2) NON FINANCIAL APPLICATIONS

Blockchain has the potential to significantly improve many different fields beyond finance, like supply chain, voting, healthcare, insurance, and the academic world. In the supply chain, Blockchain enables a decentralized and tamper-resistant record of transactions, allowing stakeholders across the supply chain to access a single version of the truth. This transparency is precious in tracking and verifying the provenance of goods, reducing fraud, and enhancing traceability [12]. IBM Blockchain is one of the most popular platforms for supply chain solutions. One such instance is Walmart's pork and mango supply chain with IBM [13]. In healthcare, Blockchain improves the security and effectiveness of interchanging health information. Avaneer Health is one example, providing healthcare data-sharing functionalities with the Hyperledger Fabric platform [14]. In a different scenario, Blockchain improves election procedures' security, integrity, and openness, providing a revolutionary solution. It offers an open and verifiable voting trail to promote confidence among democratic participants. Notably, the United States is the first country to utilize this approach. In 2018, West Virginia state used the blockchain-based Voatz mobile application in federal elections [15]. Energy trading can be considered in the non-financial section of trading applications. Blockchain in the energy sector is used to keep track of certifications, mainly for usage in smart grids [16]. An Australia-based company called Powerledger introduced an Ethereum-based blockchain application. In recent years, one project has been launched by the Uttar Pradesh government in India [17] for solar power trading. Like these, numerous non-financial applications are available with blockchain. Estonia, a northeastern European country, has become the global leader in blockchain adoption. It launched an E-Residency Program with the help of the Keyless Signature Infrastructure (KSI) blockchain to digitize the complete country activities [18].

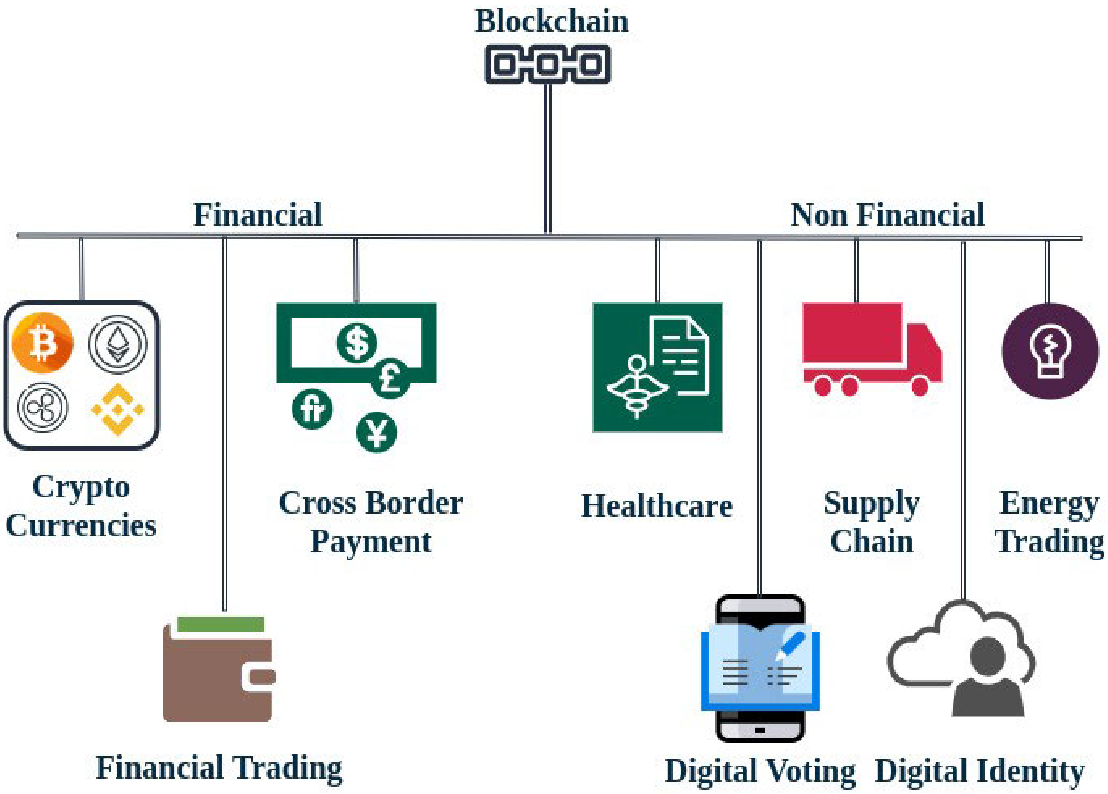


FIGURE 3. Applications of blockchain.

III. BLOCKCHAIN NON-FINANCIAL USE CASES

Blockchain's openness and decentralization have piqued the curiosity of a wide range of businesses and government agencies. Many industries (including insurance, digital voting, private transport and ride-sharing, government and public services, retail and real estate, etc.) have begun integrating blockchain technology to cut costs, promote transparency, and foster a culture of trust. Using blockchain technology, the IoT may provide an immutable public ledger of transactions. If this were missing, devices would not be able to have honest and trustworthy conversations with one another. It can be used to build a trustworthy and decentralized network for IoT gadgets, making them more resistant to cyberattacks. By dispersing information over its network, the blockchain mitigates some of the vulnerabilities of central data repositories. Since the blockchain database doesn't keep its data in a centralized location, all its records are freely accessible to the public and can be independently verified. One possible source of interruption is removed because a hacker cannot access a centralized version of this data. Its information is replicated on millions of computers at once, making it available to anybody with an internet connection. The following section will discuss how blockchain technology can be applied beyond the financial sector.

A. HEALTHCARE APPLICATIONS

Transferring patient records is one of the critical challenges in the healthcare industry. It also requires high integrity for tracking the records. It leads to a costly history-based diagnosis because of the complexity, privacy issues, and fragmentation of medical data. However, blockchain allows reliable record storage and an easy track-tracking mechanism, which could reduce service and tracking costs. Secure data storage, patient control, interoperability, and integrity are essential Blockchain features that can be applied in the healthcare industry. Health records are kept tamper-resistant and decentralized when maintained securely on a blockchain, lowering the possibility of fraud, data breaches, and unauthorized access. The decentralized nature of Blockchain enhances patient control by giving people more ownership and control over their health data. It encourages a more patient-centric approach to healthcare by allowing patients to allow or deny access to their information. By utilizing blockchain capacity to establish a standardized, safe, and decentralized platform for exchanging health data among various healthcare providers and systems, interoperability can be enhanced, which is a chronic problem in healthcare. Furthermore, the immutability of ensures that once data is uploaded, it cannot be changed without the blockchain network's consent, protecting the integrity of health information. These characteristics show how blockchain technology can completely change the healthcare sector by fostering a more connected, safe, and patient-focused ecosystem.

For example, Azaria et al. [140] proposed a permission management framework for existing cloud-based healthcare applications to increase accessibility and transparency in

TABLE 1. Blockchain applications in healthcare.

paper	Implementation	Overview
[140]	Ethereum-based smart contracts for healthcare data permission management	Acts as a database Gatekeeper keeps an unchangeable record of authorization rights, guaranteeing a thorough record for efficient data access and thorough auditing.
[110]	A cloud-assisted eHealth solution is suggested to guard outsourced EHRs from unauthorized alteration using the Ethereum blockchain.	For the patient, a treatment key is generated. It establishes a secure connection between the patient, the hospital, and the assigned specialists. Every EHR process was integrated as an operation onto the blockchain. Showed a greater level of efficacy and security assurance for the offered solution.
[111]	EHR exchanging employed the Ethereum blockchain on a mobile cloud platform (AWS) and integrated it with the distributed file system IPFS.	A dependable access control technique was created using smarter contracts. Additionally, a mobile app prototype was demonstrated using the Ethereum blockchain. Based on empirical findings, the proposed approach provides a practical solution for reliable cloud-based data interchange in the face of potential risks.
[112]	proposed a personal blockchain-based safe healthcare framework for multimedia data processing in IoT healthcare systems.	The experimental analysis of the framework shows its efficacy against malicious IoT devices against drop ratio, falsification attacks, wormhole attacks, and probabilistic authentication scenarios, with an 86% success rate.
[72]	Data exchange with Mobile Edge Computing (MEC) based blockchain for Internet of Medical Things (IoMT)	Presented a data offloading technique that allows mobile devices to offload IoMT health data to the nearest MEC server. Then smart contracts carry out decentralized user access verification at the edge network.
[113]	Ethereum-based Machine learning approach for heart disease prediction.	Data Stores on blockchain. This data is accessed with smart contract for prediction with machine learning and the Sine Cosine Weighted K-Nearest Neighbor algorithm.
[114]	integration of runtime microservices workflows, cloud computing, and Blockchain to increase the security and productivity of IoMT.	Used deep learning-based algorithms SARSA-PoW, Q-learning, and Q-learning PoPMV to enhance the efficiency of microservices workflows for malware detection in IoMT. But taking more time to analyze.
[146]	Hyperledger Fabric-based blockchain-powered electronic health record sharing system.	Hyperledger caliper used for testing the application. Membership Service Provider has been created to manage participants certifica.
[147]	Ethereum-based framework for Healthcare Group Decision Making (GDM).	A decentralized GDM framework has been introduced to facilitate expert consultation in the healthcare system, addressing the challenges encountered in decision-making for healthcare issues.
[148]	Hyperledger Fabric-based blockchain framework for Indian National Health Authority ecosystem.	Proposed a Healthcare ecosystem to integrate all healthcare related functioning. No practical implementation not available.
[149]	Personal blockchain with IPFS off chain storage for Healthcare data.	Proposed a customised blockchain with AES symmetric encryption technique for data security. Used light weight nodes for scalability.
[150]	Hyperledger Fabric-based blockchain framework for health information exchange.	An attribute-based granular approach to enhance the EHR accessing process is used to increase EHR management efficiency.
[151]	Personal blockchain with mobile cloud environment for EHR management.	Elephant Herding Optimization with Opposition- based Learning key generation has been used to minimise the key generation to increase the performance.

TABLE 2. Blockchain applications in supply chain.

paper	Implementation	Overview
[13]	IBM blockchain for Walmart food supply chain.	Used for pork and mango distribution from form to market. Guaranteeing that the food is secure and untampered.
[117]	Ethereum-based private blockchain for Blood Donation Supply Chain	To specify access, a role-based smart contract method is utilized. Ensures a high degree of trust, security, and privacy protection for each participant.
[116]	Ethereum-based framework for Agriculture food supply chain.	A provider-consumer network created to increase transparency, and decrease errors leads to better management.
[118]	IoT-based Building Information Modelling with Hyperledger Fabric.	By emphasizing real-time communication and interoperability from planning to installation, concerns with traceability and information exchange offsite manufacturing.
[144]	Ethereum-based framework for the healthcare supply chain	Effective management of the healthcare supply chain requires collaboration, openness, data integrity, and data provenance across stakeholders.
[145]	Ethereum with a proof-of-authority framework for the US beef cattle industry supply chain.	maintain and interact with multiple entities in order to maintain user anonymity, improve data privacy, and assure trace data integrity.
[152]	A safe and automatic supplier selection method is enabled by the Ethereum blockchain.	Suppliers are ranked using TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution rank). It makes fraud detection and selection easy.
[153]	Hyperledger sawtooth based Drug tracing supply chain.	PoET consensus algorithm used for better performance and users can set system specifications based on their requirements.
[154]	Hyperledger Fabric based COVID-19 vaccines supply chain.	It provides availability for governments, suppliers, and consumers to register and get genuine products to eliminate counterfeit vaccines.
[155]	Ethereum with IPFS offchain storage based Fishery supply chain.	fish seed company manages supply chain with 5 smart contracts. Keccak256 algorithm used for encryption.
[156]	Hyperledger Fabric based wine supply chain called PrevChain.	Zero Knowledge Range Proofs have been used by Grape suppliers instead actual data. Incentive amounts will be transferred for providing proofs.

healthcare management. Similarly, Kassab et al. [141] illustrated that Blockchain can reduce medical errors and fraud in the medical supply chain and medical insurance while simultaneously enhancing the security and privacy of healthcare data. Omar et al. [109] conducted another study that emphasized the usage of Blockchain in clinical trials concerning data authenticity, transparency, and traceability. Several authors [142], [143] investigated how blockchain may be used in various health care scenarios to save costs and improve efficiency. While blockchain technology improves security and transparency in healthcare applications, it is critical to remember that new technologies such as the Internet of Things (IoT), machine learning (ML), and artificial intelligence (AI) are frequently required to reach their full potential. For example, IoT devices [72] can collect real-time patient data, which can be securely stored and accessible via blockchain. This data can then be analyzed using ML and AI algorithms to find patterns, predict results, and provide individualized treatment suggestions [113]. By combining blockchain and various emerging technologies, healthcare organizations may not only secure data security and integrity but also use advanced analytics to improve patient care, streamline operations, and drive innovation in the healthcare business. Some of the healthcare applications with blockchain are mentioned in Table 1. These integration's are covered in detail in Section IV.

B. SUPPLY CHAIN MANAGEMENT AND TRACEABILITY

Nowadays, supply chains have to deal with a wide range of issues, such as fraud and counterfeiting, disjointed data management, ineffective logistics, and a lack of transparency and traceability. The potential of blockchain technology to improve supply chain management's efficiency, traceability, and transparency is becoming more widely acknowledged [12]. Recording transactions in a safe, unchangeable ledger is one of blockchain's primary benefits for the supply chain. It guarantees visible and verifiable documentation of every stage in the supply chain, from the production of items to their delivery to final customers. Because blockchain technology is decentralized, a central authority is no longer needed, which lowers the possibility of fraud and illegal data changes. By giving various supply chain stakeholders an identical, standardized platform for exchanging information, blockchain also tackles the problems of data silos and interoperability. This may result in more teamwork, less paperwork, and more productivity.

Blockchain-based supply chains can be implemented in a wide range of applications. Dhingra et al. [115] highlighted blockchain integration in the healthcare supply chain. Madumidha et al. [116] proposed an agriculture-based supply chain. Sadri et al. [117] proposed a cold chain for ensuring blood quality in transferring. One real-time application of blockchain in the supply chain is IBM-based Walmart's food supply chain [13]. Some of the supply chain frameworks with blockchain are discussed in 2. Blockchain alone cannot fulfill the supply chain management process. It only gives security to the data. For instance, supply chains like Coldchain [117] have to maintain the goods temperature at a certain level according to the medicine type. In the blood supply chain, the temperature must be 1 to 10 degrees Celsius, similarly for TT injections, which must be kept between 2 and 8 degrees Celsius, and polio vaccines, which must be kept between 15 and 25 degrees Celsius. To achieve this, cold goods supply chains require more blockchain integration, like IoT's for regular temperature access and ML for predicting possible malfunctions in refrigerators or other equipment, enabling maintenance to be done in advance of a breakdown. By considering this, blockchain-based supply chains need to be combined with other technologies and integrated into existing systems to fully support the complex and dynamic nature of supply chain management.

C. INSURANCE

Blockchain Tecchnology has the potential to completely transform the insurance sector by resolving several underlying issues in traditional systems [119]. Promoting transparency throughout the insurance life cycle is one of its main benefits. Blockchain Tecchnology reduces the possibility of fraud and builds trust by offering an immutable, shared ledger available to all parties. Blockchain's ability to implement smart contracts will greatly assist claims processing by automating and accelerating settlement processes and lowering the possibility of conflicts [120]. The technology's ability to withstand data manipulation improves overall data quality by augmenting the accuracy and dependability of information throughout the insurance ecosystem. Contracts and transactions can be securely recorded and managed on the blockchain, streamlining reinsurance procedures. In addition, the decentralized structure of blockchain facilitates a more efficient underwriting procedure, providing insurers with verified consumer data and possibly quickening the issue of policies and reducing cost [121]. Blockchain's cryptographic characteristics support data privacy and security, easing worries about breaches and illegal access and improving operational efficiency. Despite these benefits, obstacles such as legal restrictions and the requirement for industry-wide cooperation must be overcome before blockchain technology is widely used in the insurance sector. Some Blockchain-based insurance frameworks are discussed in 3.

D. ENERGY TRADING

Technologies such as rooftop solar panels, electric vehicles, and smart metering have consistently fueled expansion in the energy industry. One use of blockchain technology in the energy sector is to keep track of certifications, mainly for usage in smart grids [16]. Numerous power plants produce electricity, and certificates attesting to the overall energy produced are then issued and traded. Several concerns need to be addressed, including overcoming regulatory hurdles and ensuring that all market participants have equal access. This blockchain system allows for the efficient issuing and tracking of energy certificates.

The blockchain might also be used to profit from renewable energy overages. Power surpluses can be bought and sold after buildings are wired with sensors to measure energy usage and record the data in a distributed ledger [127]. Distributed ledger technology's potential use to track grid components' origins could appeal to the utility sector.

TABLE 3. Blockchain applications in insurance.

paper	Implementation	Overview
[120]	Hyperledger Fabric-based Insurance automation system.	Insurance firms hold complete responsibility and ensure customers do not fraudulently accuse them. Experiments show more nodes lead to longer confirmation time.
[121]	Ethereum blockchain-based Health Insurance system.	The strategy is workable and allows for time and money savings, according to the results.
[122]	Hyperledger Fabric combined with IPFS for Car insurance.	Elliptic Curve Digital Signature Algorithm used for data Encryption. Reduce the cost and increase performance for operations.
[123]	Private Ethereum with Proof of Authority (PoA) consensus.	Provides a secure procedure to execute the insurance process. IoT-based application adoption is required.
[124]	Ethereum and IoT based framework for Health insurance.	IoT data like ECG reports are directly stored in Blockchain. Insurances or need to register for accessing data.
[125]	Hyper Ledger Fabric based claim settlement with IoT for Crops.	Sensors like soil and moisture are used to gather data on the agricultural land to store in blockchain. This data is used in natural disasters to automate the insurance process.
[126]	Ethereum-based fraud detection in Healthcare insurance claim.	SmartPy module has been used to test the framework and Random forest classifier for detecting frauds.
[157]	Hyper Ledger based Transparent Vehicle Insurance Management.	Cahincode smart contracts automate the insurance process to streamline the process to find fraud insurance claimers.
[158]	Ethereum and Hyper Ledger combined Fine-Grained Transportation Insurance.	Smart contract triggered when new trip started then GPS sensors stored in GIS database available with Hyperledger Fabric. Insurance Payments models are stored in Ethereum network.
[159]	Ethereum based Usage-based Insurance .	Tested with Ganache-CLI 1,000 accounts. Driving data encrypted with decompose-and-multiply method.

TABLE 4. Blockchain applications in energy trading.

paper	Implementation	Overview
[129]	Using blockchain and AI to create a conceptual framework for energy management for decentralized, multi-type energy.	Tested on a multi-energy network with four domestic buildings. Particle Swarm Optimization and long short-term memory networks are used for calculating the rate of energy import and export as well as scheduling local energy devices.
[130]	Personal blockchain for electric vehicles (EV) bidirectional smart charging model.	optimal scheduling algorithm with information acquired from Tehran City drivers used to manage State of charge and placement of charge to decrease charging cost.
[131]	Ethereum-based consortium blockchain with PoA consensus electricity data transaction for low-carbon power systems.	To analyze data in a multidimensional manner, the suggested assessment system incorporated uncertainty, timeliness, and completeness. The data were valued using game theory, taking into account actual market power.
[132]	Personal Blockchain with POA to frequency control of an islanded microgrid with FL.	Smart contract participation matrix to balance the needs of consumers and the generation. fractional order recurrent neural network is used to manage the power generation uncertainty.
[160]	Personal Blockchain with Directed Acyclic Graph for Energy Exchange in Networked Microgrids.	untested transform framework proposed to mange hourly load demand for networked micro grids and renewable energy outputs.
[161]	Hyperledger Fabric based energy management system for micro grids.	random information transmission mechanism to handle time-varying communication topology problem.
[162]	Personal blockchain with Byzantine-Based Consensus for Energy Trading.	Energy trading framework for Electric Vehicles and distribution network to decrease attacks in time of data exchange. It has been tested with IEEE 33 bus system.
[163]	Avalanche blockchain with energy proof score (EPS) token for peer - peer Energy Trading.	Proof of Energy Generation (PoEG) Consensus mechanism used for scalability. It has been tested with IEEE 14 bus system which represents US power grid.
[165]	Ethereum blockchain bidirectional energy transfer between electric vehicles (EV) and charging stations (CSs).	Primarily it allows energy trading between EV and CSs with the help of SolarCoin. It also allows to create NFTs to allow trading in energy trading market.

Beyond only tracking where renewable energy comes from, blockchain technology can be used in unique ways to facilitate its distribution. As a result of the high expenses associated with running several trading systems, oil and gas [128] trade can profit from blockchain technology. In addition, the costs of things like labour, data storage, data visibility, settlement delays, and inter-system communication can all be reduced using blockchain. Although there have been some encouraging attempts, blockchain technology's mainstream adoption in the energy sector still faces challenges such as Public blockchains have two key drawbacks: their inability to scale and their high energy consumption in each transaction, not to mention the potential for lengthy confirmation periods due to their design. As much as we've come with technology, there's still room for improvement.

Blockchain standards or worldwide rules are a significant roadblock to the technology's mainstream adoption in the energy sector. Blockchain requires a more interconnected smart grid to realize its full potential in the energy sector, in which new companies may participate in existing smart meters. Blockchain's promise as a game-changing technology is shown by use cases directly relevant to the power sector. Because of its potential, blockchain technology has been met with widespread excitement in the energy business. Some of the energy trading platforms with blockchain are mentioned in Table 4. As the fields of blockchain and

TABLE 5. Blockchain applications in intellectual property rights (IP) and voting system.

paper	Implementation	Overview
[169]	Hyperledger Fabric consortium blockchain framework for trading rural property rights.	Enhanced PBFT Consensus Algorithm used to increase information throughput and latency. To increase adaptability of the framework dual-scoring mechanism has been used to increase performance.
[170]	Personal public blockchain for intellectual property (IP) protection.	Testing done in 10 systems with 100 nodes and Proof-of-contribution consensus mechanism was used for effective protection and management of IP rights.
[171]	personal blockchain for tracing of Original Achievements.	Developed with python programming. POS has used as consensus mechanism. Ingenuity and data storage have been the prominent drawbacks.
[172]	Ethereum based blockchain for digital copyright protection.	Testing i done in local system with Ganache and Truffle environment. Main theme is to facilitate copyright auction system. Large data stored in private clouds and security is provided with LPN homomorphic encryption.
[173]	Hyperledger Composer for immutable trademark system for IP.	Amazon Web Services cloud infrastructure and Docke has been used as testing environment. Offer solutions for the problems relating to finances, procedures, enforcement, and protection.
[174]	Hyperledger Fabric private blockchain for Voting System.	Hyperledger Caliper for evaluating the system's performance and bench marking the framework over several chaincodes. Hybrid encryption used for data security.
[175]	Ethereum based framework for college voting system.	Local environment used for testing with Ganache and Truffle Framework. Meta mask wallet is for connecting to accounts from web3. For Registration uniqueness and security OTP has been used.
[176]	Ethereum based framework for Electronic Voting System.	HAAR Cascade ML algorithm used for voters identification. This Ml classifier is used as a protection mechanism against fraudulent voting to increase integrity.
[177]	personal blockchain for Voting System.	Security is providing based on signature scheme. Signature generation is based on Chinese Remained theorem with discrete logarithmic difficulty.

renewable energy trading continue to develop few popular companies released their own digital coins to facilitate the energy trading. SolarCoin (SLR) [164], KWHCoin [166], and Energy Coin [167] are popular energy coins for energy trading. Especially SLR is used to promote the solar-powered generation and trading. This company offers one SLR for every one Megawatt-hour solar power energy. it also allows exchange with other coins like Uniswap coin on ETH Mainnet. Frameworks like TokenGreen [165] has been proposed with this concept for energy trading. Some of the Blockchain based smart grid solutions and the energy exchange based coins are discussed by authors Mollah et al. [168].

E. INTELLECTUAL PROPERTY AND COPYRIGHT MANAGEMENT

Copyright issues have long been a thorn in the growth of the Internet. with platforms like Napster and Grokster well-known for encouraging the unlawful sharing of copyrighted information. While these services did not directly provide unlawful images, they reflected the greater issue of unauthorized sharing of digital content, including photographs, which remains a difficulty in the internet space. File holders frequently violate copyrights, making file sharing and the consumption of copyrighted content significant ongoing problems. To address the copyright issues that plague illegal online image use, many alternatives are being examined, with blockchain technology emerging as a potential tool [133]. Blockchain networks, with their decentralized structure and immutable records, provide a transparent and tamper-resistant platform for preserving ownership and transaction history. For consistency, this network updates and reconciles file copies thousands of times with decentralized data management. Manipulation and corruption are complex without central storage, and ledger modifications are permanent, which increase reliability. When copyrighted material is illegally utilized, a digital ledger with the owner's identity and past transactions becomes publicly accessible and verifiable [134], especially in cases of copyright issues afflicting online image use. Photographers are increasingly using blockchain-based technologies to prevent piracy and establish ownership [135].

Notably, Binded is the world's first blockchain copyright platform. It provides a cryptographic hash as a unique fingerprint for each copyright record [136]. Photographers monitor Instagram and Twitter with Blockchain to track copyrights for Bound with these digital fingerprints. COPYTRACK is another blockchain copyright platform [137]. Some of the blockchain frameworks of Intellectual Property and Copyright Management are discussed in Table 5

F. DIGITAL VOTING

The blockchain is revolutionizing the electronic voting process. By bringing decentralization, transparency, and security. Blockchain in e-voting reduces the dangers of fraud and manipulation by operating on a decentralized network, unlike traditional voting systems, which require a central authority [138]. A vital component of the blockchain is its openness. Each vote is registered on a public ledger that is open to all users and allows for independent election result verification. Blockchain is very resistant to hacking and manipulation since cryptographic procedures strengthen it. Votes become a permanent part of the record after they are cast because of the blockchain's immutability. Furthermore, blockchain voting systems help distant and international voters by providing greater accessibility, enabling participation from any location with an internet connection. The process is further streamlined using smart contracts, which automate results tabulation and eligibility verification procedures. Despite the apparent benefits, obstacles must be carefully considered, including protecting voter privacy, dealing with scalability concerns, and accommodating voters without access to technology [139]. Blockchain voting could be a key component of safe, open, and easily accessible democratic elections as a result of ongoing research and practical applications. One real-time incident is the 2018 West Virginia state elections. It used blockchain-based Voatz mobile application in federal elections [15]. Some of the blockchain frameworks of voting system are discussed in Table 5

IV. EXPANDING HORIZONS: BLOCKCHAIN INTEGRATION WITH EMERGING TECHNOLOGIES

This section focuses on how Blockchain Technology can revolutionise non-financial applications and how well it works with other cutting-edge technology. We explore how Blockchain Technology acts as a foundational layer for trust and decentralisation, from promoting safe and transparent data exchanges in the Internet of Things (IoT) space to redefining collaborative paradigms in Edge Computing, Machine Learning (ML), Federated Learning, and Artificial Intelligence (AI). We draw attention to the ways Blockchain seamlessly combines with these fields, providing new solutions, improving data integrity, and ultimately changing non-financial operations in the digital world, in addition to financial transactions.

A. IOT

Recently, IoT devices have found their value in almost every sector. It integrates smart devices to gather information and enable smart decision-making. However, it is vulnerable to privacy and security issues due to a lack of essential security measures [48] in the architecture. Usually, in traditional IoT ecosystems, data from sensors is transmitted to a centralized cloud server. With this method, cloud servers are managed by third parties, which leads to privacy concerns. In addition, the possibility of single points of failure and the difficulties involved in updating firmware for millions of smart devices raise security concerns [49]. Utilizing blockchain architectural weaknesses of IoT can be addressed [50]. The immutable ledger feature guarantees IoT data authenticity and integrity, and process automation through smart contracts builds participant trust. Furthermore, the decentralized structure of blockchain reduces the possibility of single points of failure, enhancing dependability in extensive Internet of Things implementations. Additionally strengthened are transparency and traceability since blockchain's distributed ledger gives every network user a uniform view of the data.

On the other hand, blockchain gains practical applications from IoT [178]. IoT device real-world data can act as oracles, providing real-time decision-making information to smart contracts [51]. IoT sensor integration enhances supply chain transparency by enabling safe and transparent record-keeping of the complete supply chain process. IoT devices enable autonomous decision-making based on gathered data in decentralized energy grids, while blockchain controls safe transactions. Additionally, IoT facilitates blockchain-based identity and access management, boosting security via decentralized identity systems. Several researchers have extensively studied the benefits of combining Blockchain with IoT and highlighted numerous advantages across multiple fields. Popular applications with IoT and Blockchain integration are presented in Figure 4.

Al-Nbhany et al. [52] discussed the IoT integration in healthcare, addressing remote patient monitoring, disease prediction, and medical record security. Further research by Mollah et al. [53] on intelligent transportation systems (ITS) suggested this combination helps to establish smart, safe, and effective transportation systems. It ensures it by establishing secure, efficient, and traceable vehicular communication. Another popular application that benefits from this combination is agriculture or farming operations. IoT sensors could be installed in farms to capture the data at a specified interval, which helps to predict soil moisture and pH levels and detect the health of the crops. The blockchain handles these IoT device's data security. This possibility has been discussed by researchers Ferrag et al. [54]. IoT and Blockchain combinations are not limited to these applications. Other than these, it can be beneficial in supply chains [55],smart homes [56], the emergency sector [57], e-government [58], smart cities [177] and the defence sector [59].

Even though Blockchain offers potential answers to IoT security issues, it also brings several new difficulties that must be considered appropriately [60], [61]. There are several benefits and particular difficulties associated with integrating blockchain technology with IoT that must be carefully considered to be implemented successfully. Scalability, interoperability, resource constraints, and implementation costs are notable difficulties. Scalability is one major obstacle because standard blockchain transaction processing speeds could not keep up with the real-time requirements. Standardization is necessary since different blockchain platforms and IoT devices use different protocols, which might cause interoperability problems. Resource limitations are a problem, especially for lightweight, energy-efficient solutions that must consider the Internet of Things devices' constrained processing and storage capabilities. Cost factors include infrastructure costs and transaction fees related to running blockchain networks, particularly in the case of extensive IoT installations. Preserving the privacy and integrity of IoT data and protecting the decentralized ledger from any vulnerabilities are the main challenges of security. Lastly, concerns about governance and compliance surface, necessitating the development of strong governance models and legal frameworks to manage regulatory complications and guarantee Blockchain's moral and legal use in the IoT. To address these barriers, Solutions include off-chain scaling [62], standardization, edge

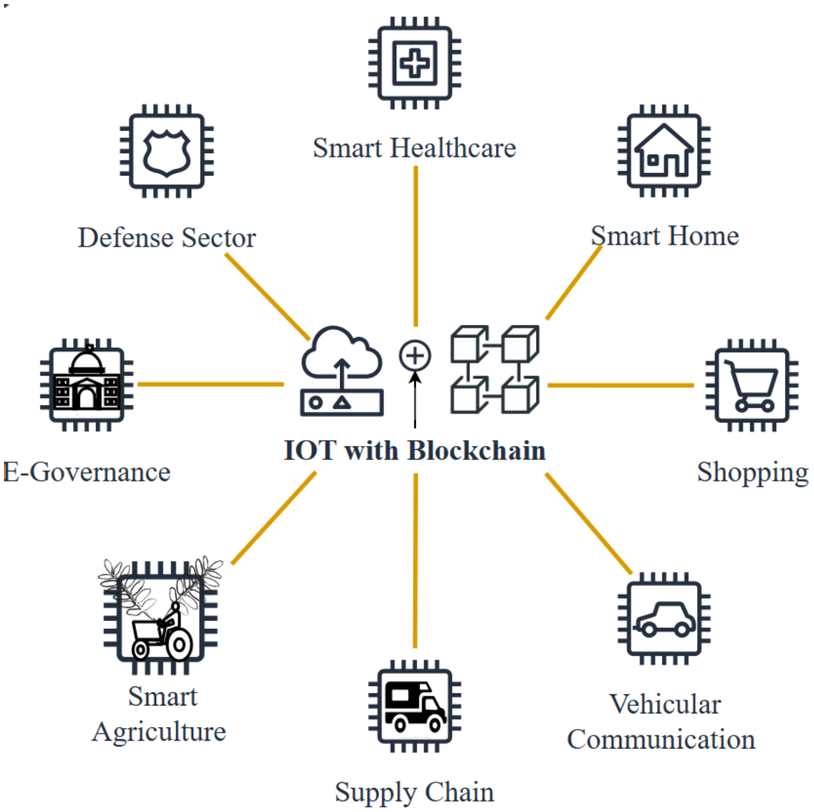


FIGURE 4. Popular applications with IoT and blockchain.

computing [63], lightweight protocols [64], fee optimization, advanced encryption, private blockchains, and regulatory frameworks.

B. CLOUD AND IPFS

Blockchain applications that use cloud computing and the InterPlanetary File System (IPFS) are revolutionary for improving data storage, accessibility, and overall system efficiency. The flexibility of the cloud computing architecture allows blockchain networks to use resources flexibly based on demand. This adaptability makes the system more resilient to potential breakdowns and ensures peak performance. In addition, IPFS, being a peer-to-peer, decentralized file-sharing system, makes it easier to store large datasets safely and effectively. By storing data among numerous nodes instead of a centralized server, IPFS promotes data redundancy and availability. When applied to blockchain applications, combining cloud computing with IPFS enables a resilient ecosystem where decentralized data storage meets the scalability and flexibility given by the cloud. This integration expands the potential applications of blockchain technology across various industries by promoting a more secure and dependable environment for these solutions while optimizing resource utilization.

Especially when combined with IPFS, Blockchain has enormous potential for creating scalable, private healthcare systems. Several current use cases show that it is feasible to combine these two technologies, enabling us to share health records transparently among different stakeholders while guaranteeing anonymity is upheld throughout the lifetime. Figure 5 demonstrates the blockchain applications' integration with clouds and IPFS.

C. EDGE COMPUTING

Edge computing is used to transfer sensible data from the cloud to the edge to ensure network security during data transmission with frequent transmission [65]. IoT performance issues are solved with Edge computing. IoT devices generate data divided in smaller pieces dependent on parameters such as data type, collecting time, and data source. Sensor readings, for example, might be divided into time intervals, and video streams could be segmented. These portions are then kept on several edge servers spread across different regions. This distribution improves the performance of IoT applications by allowing for faster and more efficient data processing and retrieval. These chunks or parts kept in various edge servers, and spread out across multiple places to enhance the IoT applications performance [63]. This segmentation might be based on type of data, features, time period, or the geographic distribution of IoT deployments. By breaking the data into parts, it is possible to distribute it among multiple edge servers. This technique optimizes data

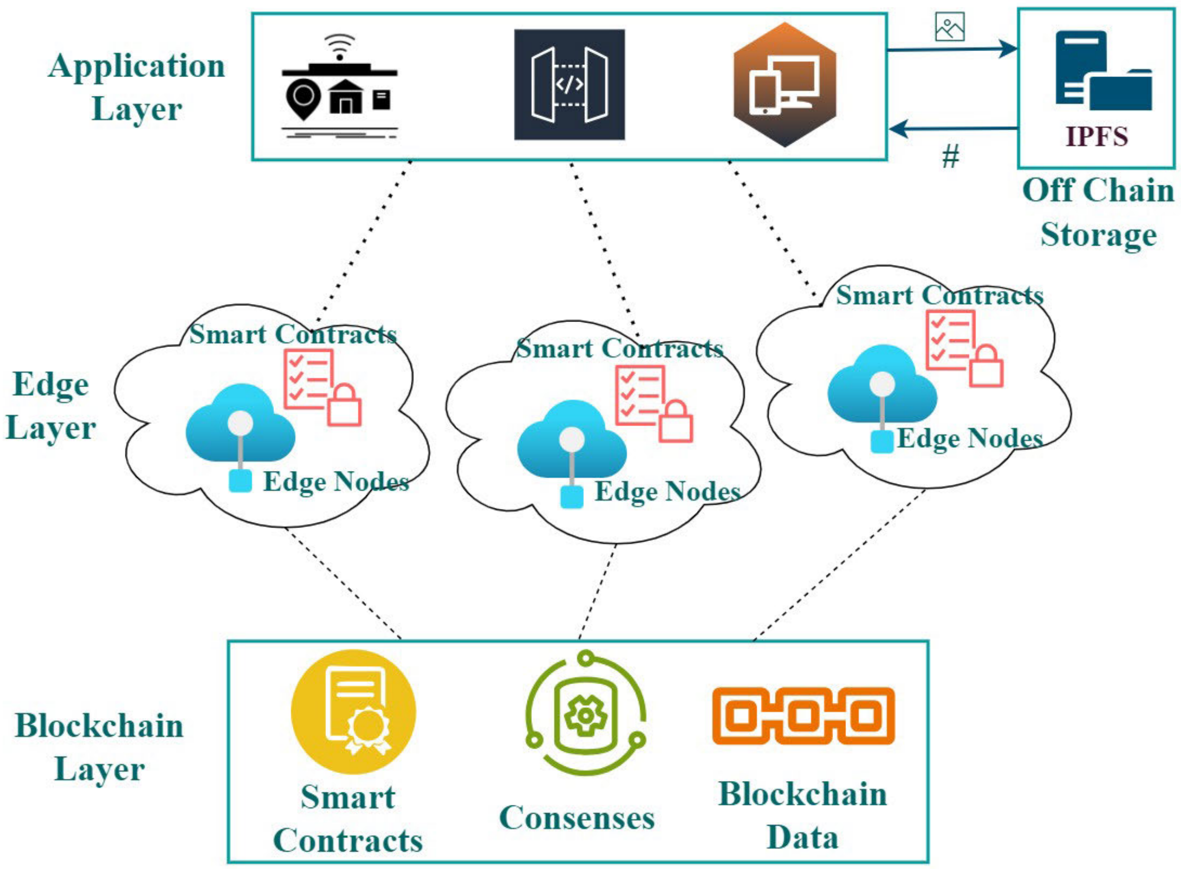


FIGURE 5. DApp architecture with off-chain storage and edge computing.

processing, lowering latency, and allows for quick response times, all of which are essential for increasing IoT system performance [63]. This makes it difficult to guarantee data integrity due to data loss and improper data storage in edge servers [66]. The emerging blockchain technology integration is the best solution to overcome the security issues of edge computing [67]. As shown in figure 5, a distributed and secure edge computing architecture can be created to support the integrity and safety of IoT devices, systems, and other Dapp data throughout its lifetime by integrating edge computing with Blockchain. Regarding robustness, adaptability, and versatility, blockchain and edge computing can be an effective pairing [68]. Edge computing and Blockchain appear to be the ideal complements for establishing a secure, scalable, and distributed IoT platform. Edge computing provides the low-latency, distributed, scalable network that IoT applications depend on, while Blockchain aids in resolving security challenges inherent to edge computing and IoT [69].

Blockchain will help edge-based applications. Similarly, Edge computing also helps the blockchain application performance. In standard blockchain architecture, large-scale applications need more performance, and low-resource devices like mobiles can not compete. Optimizing the limitations of these devices is necessary when integrating them into blockchain applications. This entails creating lightweight wallets, utilizing Simplified Payment Verification (SPV) clients, and permitting smartphones to engage in consensus processes that require fewer resources. These gadgets can also be local processing edge nodes in an edge computing architecture. Smartphone involvement is further facilitated via state channels, private blockchains designed for lower resource demands, and optimized communication protocols. A hybrid solution finds a balance by handling less crucial transactions off-chain and handling significant ones on the main Blockchain. These tactics make it possible for more devices to be included, expanding blockchain networks' potential to include low-power cell phones.

The popularity of blockchain-based edge computing use cases is increasing day by day. Integrating blockchain and edge computing can improve security, real-time data access, processing, storage, and resource usage. Popular applications are Agriculture [70], vehicular services [71], Healthcare [72].

D. AI

Blockchain and artificial Intelligence are the two most predominant technologies adapted to various sectors [73], [74]. Blockchain is a disruptive technology that paves the way for interaction among multiple parties to automate

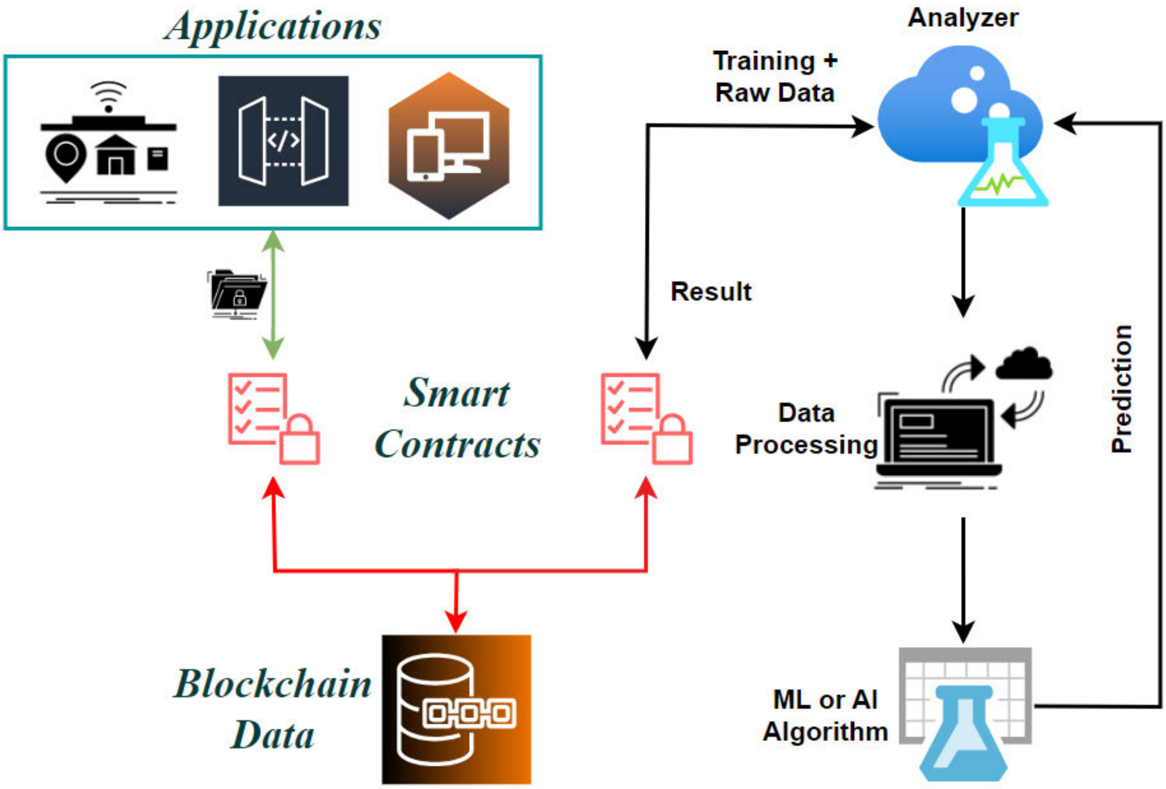


FIGURE 6. ML and AI integration with blockchain.

financial payments and track transactions. On the other hand, AI allows machines to mimic the human brain's decision-making abilities by utilizing data and computational resources. When combined with blockchain, which provides a safe and decentralized mechanism to record transactions and data, AI systems can become more secure, transparent, and trustworthy. The other technologies, such as IoT devices, web pages, and social media portals, believe that the inclusion of AI techniques is essential. The data collected through the IoT devices and web pages are analyzed with the help [75] of artificial Intelligence technique to learn its insight. Integration of AI with Blockchain Technology has been shown in Figure 6

Currently, most artificial intelligence techniques depend on the centralized model to train and validate against datasets. Tech giants Amazon, Google, and Facebook handle vast amounts of data for analysis. The major drawback in deploying the centralized model is that adversaries can tamper with the data, which may affect the model's decisions. To eliminate such data tampering, the decentralized AI is envisioned [76].

The merits of Blockchain and AI are that decentralized AI facilitates data analysis and decision-making with the data stored on various nodes on the Blockchain. Hence, deploying a trusted third-party role became unnecessary. Blockchain and Artificial Intelligence are two technological inventions with merits and demerits. Taxonomy of Blockchain meant for AI, in terms of Decentralized AI operations, infrastructure, applications, and consensus protocols, can be found in [77]. The limitations of AI and Blockchain can be addressed by their integration. AI techniques purely rely on data or information to build an efficient model. Gathered data from multiple resources should ensure reliability and not be tampered with. Blockchain is a distributed ledger technology where data can be stored using cryptographic techniques, and all the transactions should need approval from the miner nodes to ensure high integrity. Smart contract codes are written to validate the transaction, where machine learning algorithms can facilitate enhancing its decision-making ability. Hence, the integration of AI and blockchain [78] creates a reliable, trusted, decentralized repository for sensitive data and paves the way for creating AI-driven systems. This section presents the blockchain-enabled AI application to demonstrate how blockchain technology can influence AI to implement various security aspects such as transparency, trust, and reliability.

A decentralized, multiagent method for vehicle routing is presented in [79], [80]. Ant colonies influence the routing coordination system. The agents scan and forecast the environment to detect congestion on behalf of vehicles. To implement the decentralized traffic domain, the presented approach stored all the anticipated vehicle information in a decentralized manner. Through the forecasted routing information, traffic congestion is significantly reduced. Dynamic routing is not only meant to remove congestion but also assists the driver in reaching the destination faster; moreover, it works to prevent traffic congestion in future. Swarm robots are a method meant to coordinate multiple robots as a system. Swarm robots are highly resilient, and so far, research attention has considered only constrained laboratory settings and ignored the existence of Byzantine robots. Byzantine robots intend to trigger malicious behaviour. The proof of concept [81] from blockchain technology enhances the security aspects of swarm robots. The designed smart contract is executed in the decentralized environment to detect and isolate the Byzantine Robots.

Another sector that could greatly benefit from AI and blockchain technologies is the healthcare sector. Healthcare professionals can store patient healthcare data in blockchain-enabled databases. In contrast, the AI technique can be used to analyze the healthcare variables of a patient and suggest possible treatment steps to the healthcare personnel. Before blockchain technology, healthcare systems relied on centralized repositories; hence, single-point failure and various cyberattacks can easily jeopardize the system. The impact through the single point of failure and some malicious activities are solved using the server client blockchain architecture [82], where the patient's details are encrypted, preventing data tampering. But, the server-client architecture is prone to a single point of failure.

Remote monitoring greatly helps patients suffering from chronic diseases. The authors in [83] designed a smart contract to collect the patient's details through wearable devices and validated the same per the agreements established among the participants, especially such details passed on to concerned healthcare professionals to proceed with the treatment. In two more venues, [84], [85] also presents a smart contract-enabled patient record maintenance system to prevent security breaches.

E. FEDERATED LEARNING

Federated learning (FL) is a kind of artificial Intelligence technique that trains models across multiple nodes with their local data without exchanging them. Federated learning should be distinct from the concept of distributed learning, where the data is stored in a centralized repository; the model is distributed across the networks. Federated learning has many merits: data security, data diversity, and local models are trained continuously, and eventually, the system can handle complex hardware resources for the server. FL adapts to smartphone [86], IoT devices [87], [88]healthcare [89], [90], autonomous vehicles [91], [92], fraudulent activities detection [93], [94] and insurance sector [95]. FL attempts and succeeds well in the process of security optimization in many industry applications. However, the characteristics of FL [96] lead to issues such as privacy ensuring, communication cost in broadcasting the model, and heterogeneous data features. Despite many merits associated with FL by default, challenges are still ahead. The gradient aggregation mechanism used by the FL relies on a centralized server. It is prone to DDoS attacks. Hence, a trustworthy centre node is important, and the activities carried out by the centre node must be transparent enough.

FL systems establish appropriate evaluation and incentive mechanisms to ensure continuous training [97]. Then finally, a robust system to detect malicious nodes is essential for the distributed system. Remarkably, integrating blockchain and Federated learning complements applications' security, scope and performance. This section reports some of the processes and use cases that benefited from such a combination.

Federated learning imposes a new way of training conventional Machine learning (ML) [98], installing the machine learning models on the local machine to prevent the threat anticipated by compromising the security aspects. IoT networks leverage the FL technology to improve security features. However, Federated learning introduces the idea of distributed machine learning, which could prevent data sharing across the nodes by installing a local model. Ensuring IoT security is a challenging task. However, inferential attacks may be anticipated through compromising privacy while exchanging the model hyperparameters. To prevent such malicious threats, a gradient descent algorithm relying on differential privacy is demonstrated in [99]. Then, data reliability can be ensured by mutually verifying the results obtained through the models. To ensure non-repudiation, the verified results are stored in the blockchain.

Integrating IoT with smart devices (CIoT) meant for personal and domestic needs, revolutionizing human quality of life. Consumer IoT applications depend on edge computing technologies to improve the scalability and support resource-constrained IoT devices by consuming minimal power. Security breaches may be anticipated while analyzing consumer behaviour using Machine learning models with the centralized repository. While dealing with a centralized database, CIoT-based applications are prone to data leakage and single point of failure. To mitigate such data leakage, a Federated learning-based framework, along with the integration of blockchain, could assist in sorting out the addressed issues. Though data leakage could be prevented using FL to some extent, data security can be compromised by extracting the data from the broadcasted model parameters; again, this also leads to a single point of failure at the centralized aggregator. The included FL technology [100] boosts collaborative learning with the user's data, and the inclusion of blockchain technology acts as an alternative solution for replacing the centralized aggregator.

The Internet of Vehicles is a complex wireless communication network that comprises sensors and people to exchange data between them [101]. The application of Federated learning in complementing the operations of the Internet of Vehicles grabbed great attention [102], [103]. Here, too, the threats occurred due to the leakage of sensitive data, such as the location of the vehicle, compromising the privacy aspects of the users. Another concern about the IoV is network congestion and duplicate data transmission. Considering all these facts with the help of a centralized repository leads to some other vulnerabilities. To mitigate the threats, distributed machine learning models are considered a promising solution [104].

Local model installation and data sharing through model parameters are advantages of using FL in the context of the Internet of Vehicles [105]. Threats against the sensitive information may be raised through a centralized model aggregator and also from the participants [106], [107]. To prevent the threat from the aggregator, Homomorphic Encryption (HE) and Verifiable Computing (VC) techniques are used [108]. Hence, security breaches are possible from servers and participating clients. To prevent threats from both sides, [106] additive homomorphic encryption technique is employed. A reputation-based incentive mechanism is implemented through blockchain to validate the honest participants.

V. BLOCKCHAIN TRADE-OFFS: SECURITY THREATS AND THEIR IMPLICATIONS FOR NON-FINANCIAL APPLICATIONS

Blockchain technology, which was originally developed for financial transactions using cryptocurrencies such as Bitcoin, has subsequently grown to provide disruptive possibilities in a wide range of industries. Its basic characteristics of decentralization, transparency, and immutability enable strong solutions in industries ranging from healthcare and supply chain management to voting systems. However, these benefits come with major trade-offs and security risks that must be carefully managed, including issues related to security, scalability, performance, regulatory, third-party vendors, and insufficient testing [26]. This part investigates the delicate balance between security and performance in blockchain architecture, investigates possible ways to attack beyond simple code flaws, and addresses the ethical and societal consequences of blockchain implementation. Understanding these problems allows us to devise effective ways for maximizing blockchain's potential while minimizing its inherent hazards in non-financial applications. Chainabuse, a website for reporting blockchain-based attacks, reported 531,112 scams as of January 2024 (Fig. 7). Table 6 identifies the most common attacks, emphasizing the significance of cybersecurity precautions for all blockchain applications. Non-financial apps must also stay vigilant against similar risks.

A. SECURITY AND PRIVACY CONSIDERATIONS IN BLOCKCHAIN ARCHITECTURE

Blockchain security considerations cover many aspects to guarantee data availability, integrity, and cryptocurrency theft. While the theft of cryptocurrencies is one component, other security dangers, such as data alteration, could arise from potential weaknesses.

1) SMART CONTRACT VULNERABILITIES

The most prominent attack related to security is a smart contract vulnerability. Smart contract vulnerabilities can result in several problems, such as loss of funds, data manipulation, or illegal access. The DAO hack is the first attack by en-cashing the loopholes in the smart contract code [27]. It happened in June 2016, and 60 million dollars worth of Ethers (ETH) were stolen. It also comes under data modification because it involves accessing the funds without permission. Another popular hack is the Parity Wallet hack [28]. It happened in July 2017, when 32 million dollars worth of ETH was stolen due to a vulnerability in the smart contract code. Other than that, many other attacks are related to security and privacy.

2) APPLICATION ARCHITECTURE VULNERABILITIES

Weaknesses in a blockchain application architecture might result from different component designs and implementations, like the use of application bridges and third-party applications for external work. Bridges are protocols or other methods that enable interoperability across several blockchain networks and are linked to one significant vulnerability. A notable example is the Lympo Hack [30], in which a security breach at the sports-focused NFT platform Lympo allowed unauthorised access to a hot wallet, resulting in the theft of 165.2 million LMT tokens. Furthermore, an example of a privacy breach brought about by outside unauthorised access is the OpenSea Data Breach [31]. Attackers obtained and disseminated platform users' email addresses using employee access. These events highlight the importance of putting strong security measures in place to guard against unauthorised access and secure user data in blockchain applications.

3) CONSENSUS BASED VULNERABILITIES

Blockchain networks mainly depend on consensus algorithms to reach a consensus among nodes about the ledger's current state. Consensus mechanisms are essential to blockchain security but are also susceptible to misuse and assault. Double-spending, 51% attacks, and self-mining come under consensus-based vulnerabilities. One such instance is the Ethereum Classic Attack [29] that happened in 2020, in which the attackers took control of more than 50% Furthermore, a substantial sum of 238,306 ETC was double-spent on the Ethereum Classic network. The hack highlighted the weaknesses in proof-of-work consensus processes, highlighting the necessity of solid security measures to protect blockchain networks from these attacks. In this attack, attackers can do double-spending, 51%

B. ATTACKS BEYOND CODE

Beyond smart contract and platform vulnerabilities, blockchain applications may be susceptible to various other types of attacks. These could include Phishing, Routing, Sybil, and DDoS attacks.

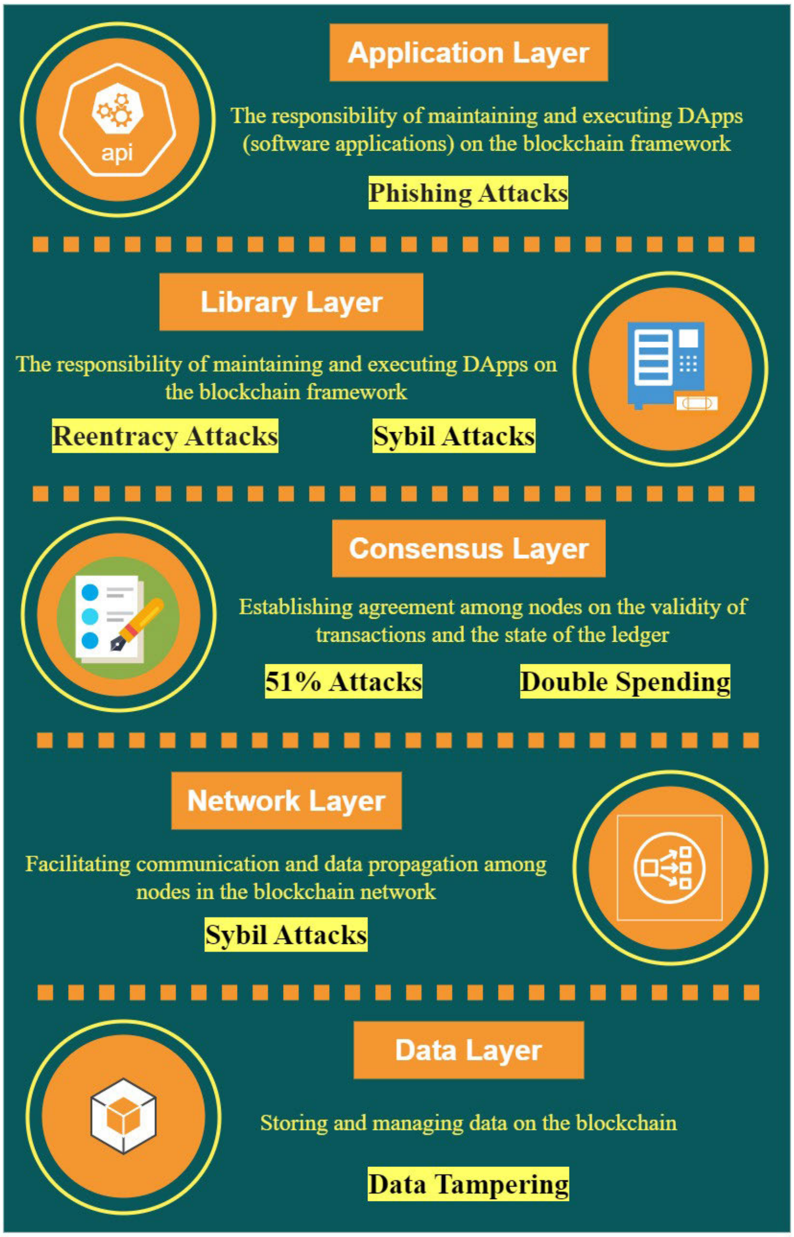

Application Layer
api
The responsibility of maintaining and executing DApps (software applications) on the blockchain framework
Phishing Attacks
Library Layer
The responsibility of maintaining and executing DApps on the blockchain framework
Reentracy Attacks
Sybil Attacks
Consensus Layer
Establishing agreement among nodes on the validity of transactions and the state of the ledger
51% Attacks
Double Spending
Network Layer
Facilitating communication and data propagation among nodes in the blockchain network
Sybil Attacks
Data Layer
Storing and managing data on the blockchain
Data Tampering

FIGURE 7. Layer-wise attacks on blockchain applications.

Phishing is one of the most common types of danger for current web-based applications. It is related to blockchain applications since we use Web3 components for user communication. Emails that appear to be from a legitimate source are sent to wallet key owners by fraudsters. Fake hyperlinks are used in emails to ask for the user's credentials. For the user and the blockchain network, gaining access to a user's credentials and other private information can be disastrous. Prominent attacks that happened using phishing attacks are the Social Engineering Scam [32] and the Discord NFT Hack [33]. Another prominent attack is routing. In this data packet, routing pathways are manipulated, like BGP hijacking [34]. It may result in blockchain node isolation, spying, or interception. It results in possible data interception, hiccups in network operations, and weakened node-to-node communication.

In the context of blockchain, a Sybil attack is a situation in which an evil actor fabricates numerous false identities or nodes to control or impose influence over a network. The attacker hopes to undermine the decentralized and trust-less character of the blockchain by using their disproportionate power to disrupt the network's regular operations. With the help of Sybil attack, 51% attack is also possible. An example of a Sybil assault that gained significant attention in 2021 was

TABLE 6. Attacks on blockchain applications and platforms.

Attack	Type and Nature of Attack	Consequences
Ethereum DAO hack [27]	Security breach happened by exploiting flaws in the smart contract code.	The attackers caused a loss of ETH valued at $60 million by manipulating the smart contract functionality to execute unauthorised fund transfers.
Ethereum Parity Wallet hack [28]	Security breach of multi-signature wallet with Smart Contract fault.	32 million dollars worth of ETH were locked up by taking control of the wallet due to vulnerability in the smart contract code.
Ethereum Classic Attack [29]	Security Consensus Attack, 51% Attack to take control over hash rate.	Attackers restructured 4,236 blocks to receive 14,234.20 ETC block rewards and 238,306 ETC were double spent on the Ethereum Classic.
Lympo Hack [30]	Security breach due to External unauthorized access	In a hot wallet breach, Lympo, a sports-focused NFT and Animoca Brands subsidiary, lost 165.2 million LMT tokens.
OpenSea data breach [31]	Privacy breach due to External unauthorized access	Exploited their employee access to download and distribute platform users email addresses.
Social Engineering Scam [32]	Security breach with Phishing Attack	A fraudulent network consisting of thousands of false Twitter accounts has been pretending to be authentic NFT retailers to defraud customers of their cryptocurrency.
Discord NFT hack [33]	Security breach with Phishing attacks	TRM Labs analysis based on on-chain and off-chain data, the NFT community has lost approximately $22 million since May 2022.

the attack on the Verge cryptocurrency protocol [35]. To rearrange the blockchain network, hackers carried out the Sybil assault, which involved erasing transactions that had been open for more than 200 days. Similarly, Distributed Denial of Service (DDoS) is another prominent threat to Dapps. When a blockchain is attacked with a DDoS attack, an excessive amount of traffic is directed at the network or nodes, causing the system to become unresponsive. This may interfere with the blockchain's operations, leading to hiccups, failed transactions, or even brief shutdowns. Blockchain networks generally employ several security protocols to alleviate the consequences of those attacks. One such instance is the Solana network attack on September 2022 [36]. Due to the DDoS attack, users cannot do any operations for several hours even though Solana's leading platform is running.

C. PERFORMANCE CONSIDERATIONS IN BLOCKCHAIN

Blockchain Technology is developed to combine the list of transaction information and bind it to a block. Massive amounts of data are needed, like images in non-financial applications that need regular processing. The complexity of maintaining and replicating the entire blockchain across all network nodes increases with blockchain size, leading to higher storage requirements and lower speed. Particularly, networks like Filecoin [37] and Ethereum [38] will charge more for image storage. For example, 20,000 gas units are required to store 256 bits of data on Ethereum. Free image storage is provided by other networks such as IoTA Tangle [39] and Hyperledger [40]. Even though it becomes very expensive to store complete data with photos at every node, it is hugely worrying, particularly for smaller businesses or healthcare institutions with limited resources. Another significant area for improvement with blockchain networks is their low transaction throughput. The restriction on how many transactions a blockchain network can finish in a given amount of time is known as this problem. High storage maintenance and low throughput are the most significant issues for blockchain applications [41]. Blockchain Technology scalability and performance issues are researchers Alshahrani et al. [42] and Kohad et al. [43].

D. ETHICAL AND SOCIAL IMPLICATIONS

Transparency on the blockchain is an essential component. Although openness fosters responsibility and trust, it can sometimes run counter to privacy standards, particularly when it comes to sensitive data. Assume that a healthcare organization decides to manage patient medical records on a blockchain platform to increase data integrity and efficiency. On the blockchain, the medical records of every patient are kept as blocks. Healthcare providers gain from fast access to precise patient data, but privacy concerns arise from the blockchain's transparency. Patients could worry that even in cases where the data is pseudonymous, private health information will be accessible to everyone on the network. The conflict between the need for privacy and the demand for transparency draws attention to the moral problem. In another scenario, specific blockchain networks can use much energy, particularly those that employ PoW consensus. According to one survey, Bitcoin mining is causing global warming because it uses PoW consensus. Addressing environmental issues and looking into energy-efficient options are part of ethical considerations [44]. Similarly, when a hard fork happens, Ethical, trust and regularity issues will rise [45].

E. MEASURES FOR NON-FINANCIAL APPLICATIONS

The frequency of blockchain assaults, which usually lead to cryptocurrency losses, provides invaluable experience and motivation for bolstering security protocols. Even though many of the occurrences that have been highlighted have mostly affected financial aspects, it's essential to acknowledge that these difficulties are just stepping stones towards strengthening blockchain technology for more non-financial applications. The observed weaknesses and assaults highlight the necessity of strong security, Scalable frameworks [46], smart contract audits [46], and efficient consensus algorithms [47].

As the technology develops by leveraging the lessons learned, non-financial businesses like supply chain management, healthcare, identity verification, and other non-financial industries are improving their operations by integrating blockchain with other cutting-edge technologies like machine learning (ML), artificial intelligence (AI), and advanced edge computing applications. For instance, authors [176] presented a review on anomaly detection in blockchain infrastructure using artificial intelligence techniques, highlighting the importance of AI in blockchain applications. Further To guarantee the security, dependability, and accuracy of smart contracts implemented on blockchain systems, smart contract auditing tools are essential [46]. Tools like Mythril and MythX use various analytic methods to find coding mistakes, security flaws, and vulnerabilities in the smart contract code. Cloud computing and IPFS offer a revolutionary way to improve data storage, accessibility, and overall system efficiency. Additionally, providing a distributed architecture like edge computing can expand dynamically to handle a range of workloads effectively, which increases system resilience.

Furthermore, the system's capacity to thwart DDoS and Sybil attacks in real-time is improved by AI-driven security features, including anomaly detection and dynamic threat response. Sybil attacks can be partly avoided by using ML concepts to govern decentralised identification and reputation systems. Furthermore, machine learning methods help validate external data, guaranteeing information accuracy and reducing the possibility of bridge errors. In addition to overcoming smart contract difficulties, blockchain systems can significantly improve their security and performance capacities in the face of changing threats by utilising this cutting-edge technology.

F. FUTURE OF BLOCKCHAIN ADOPTABILITY IN NON FINANCIAL APPLICATIONS

The future of blockchain adaptability in non-financial fields such as insurance, energy, healthcare, digital voting, supply chain management, and government sectors holds significant promise. In insurance, blockchain technology is poised to revolutionize claims processing by providing transparent and secure records that reduce fraud and improve efficiency. Smart contracts can automate policy management and claims settlement processes, ensuring faster and more accurate transactions while enhancing trust between insurers and policyholders. Additionally, blockchain's ability to maintain immutable records can streamline regulatory compliance and auditing, promoting transparency and reducing administrative burdens.

In the energy sector, blockchain enables decentralized energy trading and management, facilitating peer-to-peer transactions and optimizing energy distribution. This decentralized approach not only enhances grid efficiency but also supports the integration of renewable energy sources by providing transparent and traceable energy transactions. Smart grids powered by blockchain can dynamically balance supply and demand, improving overall system resilience and sustainability. Moreover, blockchain's data integrity benefits extend to supply chain management, where it ensures transparency and authenticity throughout the supply chain process. From tracking goods' origins to verifying product quality and reducing counterfeiting, blockchain enhances trust among stakeholders and enables real-time visibility into supply chain operations.

Looking ahead, blockchain's impact on healthcare promises secure and interoperable patient data management, fostering collaboration among healthcare providers while safeguarding patient privacy. Digital voting systems can leverage blockchain to enhance electoral transparency and integrity by ensuring tamper-proof voting records and enabling secure remote voting options. In government sectors, blockchain offers opportunities for more efficient and transparent public service delivery, from identity management and digital credentials to procurement and regulatory compliance. As blockchain continues to evolve and integrate with other emerging technologies like AI and IoT, its adaptability across these non-financial fields will play a pivotal role in shaping more resilient, transparent, and efficient systems for the future.

VI. CONCLUSION

Blockchain technology stands as a transformative force, reshaping industries across the globe. Its foundational principles of immutability, tamper-proofing, and verifiable data provenance revolutionize operational efficiency. While the financial industry has benefited the most from blockchain technology compared to other industries, there is a growing demand to analyze the role of blockchain technology for achieving error-free operations in non-financial applications. To facilitate that, the study presented in this paper reports on blockchain fundamentals and non-financial use cases built upon the merits of blockchain. The study aims to derive insights about how these use cases demonstrate promising performance in data security and operational efficiency. The paper also explores how various trending technologies such as IoT, cloud, edge computing, AI, and federated learning integrate well with the blockchain platform to enhance various non-financial applications. Additionally, it reports on possible cyber-attacks anticipated in the layered architecture of blockchain intended for non-financial applications. Finally, the paper discusses the future scope of blockchain technology, especially for non-financial applications, to incentivize readers.

ACKNOWLEDGMENT

The authors acknowledge Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2024R442), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

REFERENCES

[1] H. Vranken, "Sustainability of Bitcoin and blockchains," *Current Opinion Environ. Sustainability*, vol. 28, pp. 1–9, Oct. 2017.

[2] J. Li and M. Kassem, "Applications of distributed ledger technology (DLT) and blockchain-enabled smart contracts in construction," *Autom. Construct.*, vol. 132, Dec. 2021, Art. no. 103955.

[3] T. M. Fernández-Caramès and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 8, pp. 21091–21116, 2020.

[4] M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and A. Colman, "Blockchain consensus algorithms: A survey," 2020, *arXiv:2001.07091*.

[5] W. Metcalfe, "Ethereum, smart contracts, DApps," *Blockchain Crypt Currency*, vol. 77, pp. 77–93, 2020.

[6] L. Foschini, A. Gavagna, G. Martuscelli, and R. Montanari, "Hyperledger fabric blockchain: Chaincode performance analysis," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6.

[7] A. Ismailisufi, T. Popovic, N. Gligoric, S. Radonjic, and S. Šandi, "A private blockchain implementation using multichain open source platform," in *Proc. 24th Int. Conf. Inf. Technol. (IT)*, Feb. 2020, pp. 1–4.

[8] R. G. Brown, J. Carlyle, I. Grigg, and M. Hearn, "Corda: An introduction," *R3 CEV*, vol. 1, no. 15, p. 14, Aug. 2016.

[9] T. Qiu, R. Zhang, and Y. Gao, "Ripple vs. SWIFT: Transforming cross border remittance using blockchain technology," *Proc. Comput. Sci.*, vol. 147, pp. 428–434, Jan. 2019.

[10] Y. C. Lo and F. Medda, "Uniswap and the emergence of the decentralized exchange," *J. Financial Market Infrastruct.*, vol. 10, no. 2, pp. 1–25, 2021.

[11] TZERO. (2023). *Liquidity Solutions for Companie*. [Online]. Available: https://www.tzero.com/trading

[12] R. Azzi, R. K. Chamoun, and M. Sokhn, "The power of a blockchain-based supply chain," *Comput. Ind. Eng.*, vol. 135, pp. 582–592, Jan. 2019.

[13] R. Kamath, "Food traceability on blockchain: Walmart's pork and mango pilots with IBM," *J. Brit. Blockchain Assoc.*, vol. 1, no. 1, pp. 1–12, Jul. 2018.

[14] Avaneer Health. (2023). *Unlock the Full Potential of Healthcare*. [Online]. Available: https://b14.com/

[15] M. A. Specter, J. Koppel, and D. Weitzner, "The ballot is busted before the blockchain: A security analysis of voatz, the first Internet voting application used in U.S. Federal elections," in *Proc. 29th USENIX Secur. Symp.*, 2020, pp. 1535–1553.

[16] J. Mattila et al., "Industrial blockchain platforms: An exercise in use case development in the energy industry," Res. Inst. Finnish Economy (ETLA), Helsinki, Finland, ETLA, Working Papers 43, 2016.

[17] (2022). *Uttar Pradesh Government, India. Powerledger*. [Online]. Available: https://www.powerledger.io/clients/uttar-pradesh-government-india

[18] N. Heller, "Estonia, the digital republic," *New Yorker*, vol. 18, p. 12, 2017.

[19] V. Allombert, M. Bourgoin, and J. Tesson, "Introduction to the tezos blockchain," in *Proc. Int. Conf. High Perform. Comput. Simulation (HPCS)*, Jul. 2019, pp. 1–10.

[20] A. Vacca, A. Di Sorbo, C. A. Visaggio, and G. Canfora, "A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges," *J. Syst. Softw.*, vol. 174, Apr. 2021, Art. no. 110891.

[21] I. G. A. K. Gemeliarana and R. F. Sari, "Evaluation of proof of work (POW) blockchains security network on selfish mining," in *Proc. Int. Seminar Res. Inf. Technol. Intell. Syst. (ISRITI)*, Nov. 2018, pp. 126–130.

[22] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen, and E. Dutkiewicz, "Proof-of-Stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities," *IEEE Access*, vol. 7, pp. 85727–85745, 2019.

[23] (2023). *Ethereum, Liquidity The Beacon Chain*. [Online]. Available: https://ethereum.org/en/roadmap/beacon-chain/

[24] A. Ahmad, A. Alabduljabbar, M. Saad, D. Nyang, J. Kim, and D. Mohaisen, "Empirically comparing the performance of blockchain's consensus algorithms," *IET Blockchain*, vol. 1, no. 1, pp. 56–64, Mar. 2021.

[25] Z. Hussein, M. A. Salama, and S. A. El-Rahman, "Evolution of blockchain consensus algorithms: A review on the latest milestones of blockchain consensus algorithms," *Cybersecurity*, vol. 6, no. 1, p. 30, Nov. 2023.

[26] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges," *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 653–659, Sep. 2017.

[27] R. Morrison, N. C. H. L. Mazey, and S. C. Wingreen, "The DAO controversy: The case for a new species of corporate governance?" *Frontiers Blockchain*, vol. 3, p. 25, May 2020.

[28] (2017). *Parity Technologies, A Postmortem on the Parity Multi-Sig Library Self-Destruct*. [Online]. Available: https://paritytech.io/a-postmortem-on-the-parity-multi-sig-library-self-

[29] Patrick Thompson. (2020). *Over $1m Double-Spent in Latest Ethereum Classic 51% Attack*. [Online]. Available: https://coingeek.com/over-1m-double-spent-in-latest-ethereum-classic-51

[30] (2022). *Cointelegraph, Thousands of Bogus Twitter Accounts Push NFT Scams to Steal Cryptocurrency*. [Online]. Available: https://www.coinlive.com/news/Animoca-Brands-39-Lympo-NFT-Platform

[31] (2022). *CORY HARDMAN, Important Update on Email Vendor Security Incident*. [Online]. Available: https://blog-v3.opensea.io/articles/important-update-on-email-vendor-

[32] T. Riley. (2022). *Thousands of Bogus Twitter Accounts Push NFT Scams To Steal Cryptocurrency*. [Online]. Available: https://cyberscoop.com/fake-twitter-accounts-nft-scams/

[33] (2022). *TRM, Important Update on Email Vendor Security Incident*. [Online]. Available: https://www.trmlabs.com/post/trms-analysis-of-recent-surge-in-discord-

[34] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking Bitcoin: Routing attacks on cryptocurrencies," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2017, pp. 375–392.

[35] G. Weston. (2024). *Sybil Attacks on Blockchain: Impact and Preventive Measures*. [Online]. Available: https://101blockchains.com/sybil-attack-in-blockchain/

[36] W. Jones. (2022). *Solana Network Encounters Another DDoS Attack, Recent Report Unveils*. [Online]. Available: https://crypto.news/the-solana-network-encounters-another-ddos-attack-

[37] B. Guidi, A. Michienzi, and L. Ricci, "Evaluating the decentralisation of filecoin," in *Proc. 3rd Int. Workshop Distrib. Infrastruct. Common Good*, Nov. 2022, pp. 13–18.

[38] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum, Zug, Switzerland, Yellow Paper 151, pp. 1–32, 2014.

[39] S. Popov, "The tangle," *White Paper*, vol. 1, p. 30, Jan. 2018.

[40] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Proc. Workshop Distrib. Cryptocurrencies Consensus Ledgers*, vol. 310, 2016, pp. 1–4.

[41] M. Dabbagh, K.-K.-R. Choo, A. Beheshti, M. Tahir, and N. S. Safa, "A survey of empirical performance evaluation of permissioned blockchain platforms: Challenges and opportunities," *Comput. Secur.*, vol. 100, Jan. 2021, Art. no. 102078.

[42] H. Alshahrani, N. Islam, D. Syed, A. Sulaiman, M. S. A. Reshan, K. Rajab, A. Shaikh, J. Shuja-Uddin, and A. Soomro, "Sustainability in blockchain: A systematic literature review on scalability and power consumption issues," *Energies*, vol. 16, no. 3, p. 1510, Feb. 2023.

[43] H. Kohad, S. Kumar, and A. Ambhaikar, "Scalability issues of blockchain technology," *Int. J. Eng. Adv. Technol.*, vol. 9, no. 3, pp. 2385–2391, 2020.

[44] C. Mora, R. L. Rollins, K. Taladay, M. B. Kantar, M. K. Chock, M. Shimada, and E. C. Franklin, "Bitcoin emissions alone could push global warming above 2 C," *Nature Climate Change*, vol. 8, no. 11, pp. 931–933, 2018.

[45] F. J. C. da Silva, S. B. Damsgaard, M. A. M. Sorensen, F. Marty, B. Altariqi, E. Chatzigianni, T. K. Madsen, and H. P. Schwefel, "Analysis of blockchain forking on an Ethereum network," in *Proc. Eur. Wireless ; 25th Eur. Wireless Conf.*, May 2019, pp. 1–6.

[46] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H.-N. Lee, "Ethereum smart contract analysis tools: A systematic review," *IEEE Access*, vol. 10, pp. 57037–57062, 2022.

[47] M. Kaur, M. Z. Khan, S. Gupta, A. Noorwali, C. Chakraborty, and S. K. Pani, "MBCP: Performance analysis of large scale mainstream blockchain consensus protocols," *IEEE Access*, vol. 9, pp. 80931–80944, 2021.

[48] P. M. Chanal and M. S. Kakkasageri, "Security and privacy in IoT: A survey," *Wireless Pers. Commun.*, vol. 115, no. 2, pp. 1667–1693, Nov. 2020.

[49] E. Leloglu, "A review of security concerns in Internet of Things," *J. Comput. Commun.*, vol. 5, no. 1, pp. 121–136, 2017.

[50] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, Aug. 2018.

[51] S. S. Arumugam, V. Umashankar, N. C. Narendra, R. Badrinath, A. P. Mujumdar, J. Holler, and A. Hernandez, "IoT enabled smart logistics using smart contracts," in *Proc. 8th Int. Conf. Logistics, Informat. Service Sci. (LISS)*, Aug. 2018, pp. 1–6.

[52] W. A. N. A. Al-Nbhany, A. T. Zahary, and A. A. Al-Shargabi, "Blockchain-IoT healthcare applications and trends: A review," *IEEE Access*, vol. 12, pp. 4178–4212, 2024.

[53] M. B. Mollah, J. Zhao, D. Niyato, Y. L. Guan, C. Yuen, S. Sun, K.-Y. Lam, and L. H. Koh, "Blockchain for the Internet of Vehicles towards intelligent transportation systems: A survey," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4157–4185, Mar. 2021.

[54] M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, "Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges," *IEEE Access*, vol. 8, pp. 32031–32053, 2020.

[55] S. Aich, S. Chakraborty, M. Sain, H.-I. Lee, and H.-C. Kim, "A review on benefits of IoT integrated blockchain based supply chain management implementations across different sectors with case study," in *Proc. 21st Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2019, pp. 138–141.

[56] O. Popoola, M. Rodrigues, J. Marchang, A. Shenfield, A. Ikpehai, and J. Popoola, "A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: Problems, challenges and solutions," *Blockchain, Res. Appl.*, vol. 5, no. 2, Jun. 2024, Art. no. 100178.

[57] 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," *Renew. Sustain. Energy Rev.*, vol. 100, pp. 143–174, Feb. 2019.

[58] R. Qi, C. Feng, Z. Liu, and N. Mrad, "Blockchain-powered Internet of Things, e-governance and e-democracy," in *E-democracy for Smart Cities*. Singapore: Springer, 2017, pp. 509–520.

[59] K. Wrona and M. Jarosz, "Use of blockchains for secure binding of metadata in military applications of IoT," in *Proc. IEEE 5th World Forum Internet of Things (WF-IoT)*, Aug. 2019, pp. 213–218.

[60] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018.

[61] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A survey on the adoption of blockchain in IoT: Challenges and solutions," *Blockchain: Res. Appl.*, vol. 2, no. 2, Jun. 2021, Art. no. 100006.

[62] C. Xu, C. Zhang, J. Xu, and J. Pei, "SlimChain: Scaling blockchain transactions through off-chain storage and parallel processing," *Proc. VLDB Endowment*, vol. 14, no. 11, pp. 2314–2326, Jul. 2021.

[63] J. Pan and J. McElhannon, "Future edge cloud and edge computing for Internet of Things applications," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 439–449, Feb. 2018.

[64] A. Padma and M. Ramaiah, "GLSBIoT: GWO-based enhancement for lightweight scalable blockchain for IoT with trust based consensus," *Future Gener. Comput. Syst.*, vol. 159, pp. 64–76, Oct. 2024.

[65] S. Mittal, N. Negi, and R. Chauhan, "Integration of edge computing with cloud computing," in *Proc. Int. Conf. Emerg. Trends Comput. Commun. Technol. (ICETCCT)*, Nov. 2017, pp. 1–6.

[66] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, "A survey on security and privacy issues in edge-computing-assisted Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4004–4022, Mar. 2021.

[67] C. Luo, L. Xu, D. Li, and W. Wu, "Edge computing integrated with blockchain technologies," in *Complexity and Approximation*. Cham, Switzerland: Springer, 2020, pp. 268–288.

[68] H. Xue, D. Chen, N. Zhang, H.-N. Dai, and K. Yu, "Integration of blockchain and edge computing in Internet of Things: A survey," *Future Gener. Comput. Syst.*, vol. 144, pp. 307–326, Jul. 2023.

[69] T. R. Gadekallu, Q.-V. Pham, D. C. Nguyen, P. K. R. Maddikunta, N. Deepa, B. Prabadevi, P. N. Pathirana, J. Zhao, and W.-J. Hwang, "Blockchain for edge of things: Applications, opportunities, and challenges," *IEEE Internet Things J.*, vol. 9, no. 2, pp. 964–988, Jan. 2022.

[70] X. Zhang, Z. Cao, and W. Dong, "Overview of edge computing in the agricultural Internet of Things: Key technologies, applications, challenges," *IEEE Access*, vol. 8, pp. 141748–141761, 2020.

[71] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4660–4670, Jun. 2019.

[72] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "BEdgeHealth: A decentralized architecture for edge-based IoMT networks using blockchain," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11743–11757, Jul. 2021.

[73] S. Ahmed and N. T. Broek, "Blockchain could boost food security," *Nature*, vol. 550, no. 7674, p. 43, Oct. 2017.

[74] M. Koch, "Artificial intelligence is becoming natural," *Cell*, vol. 173, no. 3, pp. 531–533, Apr. 2018.

[75] A. Prieto, B. Prieto, E. M. Ortigosa, E. Ros, F. Pelayo, J. Ortega, and I. Rojas, "Neural networks: An overview of early research, current frameworks and new challenges," *Neurocomputing*, vol. 214, pp. 242–268, Nov. 2016.

[76] N. A. I. Team, *Nebula AI (NBAI) Decentralized Ai Blockchain Whitepaper*. New York, NY, USA: Academic, 2018.

[77] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10127–10149, 2019.

[78] T. Marwala and B. Xing, "Blockchain and artificial intelligence," 2018, *arXiv:1802.04451*.

[79] R. Claes, T. Holvoet, and D. Weyns, "A decentralized approach for anticipatory vehicle routing using delegate multiagent systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 2, pp. 364–373, Jun. 2011.

[80] E. Osaba, E. Onieva, A. Moreno, P. Lopez-Garcia, A. Perallos, and P. G. Bringas, "Decentralised intelligent transport system with distributed intelligence based on classification techniques," *IET Intell. Transp. Syst.*, vol. 10, no. 10, pp. 674–682, Dec. 2016.

[81] V. Strobel, E. C. Ferrer, and M. Dorigo, "Managing Byzantine robots via blockchain technology in a swarm robotics collective decision making scenario," in *Proc. 17th Int. Conf. Auton. Agents MultiAgent Syst. (AAMAS)*, 2018, pp. 541–549.

[82] A. A. Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," *Future Gener. Comput. Syst.*, vol. 95, pp. 511–521, Jun. 2019.

[83] 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," *J. Med. Syst.*, vol. 42, no. 7, pp. 1–7, Jul. 2018.

[84] A. Abugabah, N. Nizamuddin, and A. A. Alzubi, "Decentralized telemedicine framework for a smart healthcare ecosystem," *IEEE Access*, vol. 8, pp. 166575–166588, 2020.

[85] V. Patel, "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus," *Health Informat. J.*, vol. 25, no. 4, pp. 1398–1411, Dec. 2019.

[86] A. Li, J. Sun, P. Li, Y. Pu, H. Li, and Y. Chen, "Hermes: An efficient federated learning framework for heterogeneous mobile clients," in *Proc. 27th Annu. Int. Conf. Mobile Comput. Netw.*, Oct. 2021, pp. 420–437.

[87] V. Rey, P. M. Sánchez Sánchez, A. Huertas Celdrán, and G. Bovet, "Federated learning for malware detection in IoT devices," *Comput. Netw.*, vol. 204, Feb. 2022, Art. no. 108693.

[88] M. Tahir and M. I. Ali, "On the performance of federated learning algorithms for IoT," *IoT*, vol. 3, no. 2, pp. 273–284, Apr. 2022.

[89] J. Xu, B. S. Glicksberg, C. Su, P. Walker, J. Bian, and F. Wang, "Federated learning for healthcare informatics," *J. Healthcare Informat. Res.*, vol. 5, no. 1, pp. 1–19, Mar. 2021.

[90] M. J. Sheller, B. Edwards, G. A. Reina, J. Martin, S. Pati, A. Kotrotsou, M. Milchenko, W. Xu, D. Marcus, R. R. Colen, and S. Bakas, "Federated learning in medicine: Facilitating multi-institutional collaborations without sharing patient data," *Sci. Rep.*, vol. 10, no. 1, pp. 1–12, Jul. 2020.

[91] A. Nguyen, T. Do, M. Tran, B. X. Nguyen, C. Duong, T. Phan, E. Tjiputra, and Q. D. Tran, "Deep federated learning for autonomous driving," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2022, pp. 1824–1830.

[92] C. S. Hong, L. U. Khan, M. Chen, D. Chen, W. Saad, and Z. Han, "Vehicular networks and autonomous driving cars," in *Federated Learning for Wireless Networks*. Cham, Switzerland: Springer, 2021, pp. 179–220.

[93] D. Myalil, M. A. Rajan, M. Apte, and S. Lodha, "Robust collaborative fraudulent transaction detection using federated learning," in *Proc. 20th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2021, pp. 373–378.

[94] M. Schreyer, T. Sattarov, and D. Borth, "Federated and privacy-preserving learning of accounting data in financial statement audits," 2022, *arXiv:2208.12708*.

[95] H. Gupta, D. Patel, A. Makade, K. Gupta, O. P. Vyas, and A. Puliafito, "Risk prediction in the life insurance industry using federated learning approach," in *Proc. IEEE 21st Medit. Electrotech. Conf. (MELECON)*, Jun. 2022, pp. 948–953.

[96] D. Li, D. Han, T.-H. Weng, Z. Zheng, H. Li, H. Liu, A. Castiglione, and K.-C. Li, "Blockchain for federated learning toward secure distributed machine learning systems: A systemic survey," *Soft Comput.*, vol. 26, no. 9, pp. 4423–4440, May 2022.

[97] W. Liang, Y. Fan, K.-C. Li, D. Zhang, and J.-L. Gaudiot, "Secure data storage and recovery in industrial blockchain network environments," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6543–6552, Oct. 2020.

[98] M. Ali, H. Karimipour, and M. Tariq, "Integration of blockchain and federated learning for Internet of Things: Recent advances and future challenges," *Comput. Secur.*, vol. 108, Sep. 2021, Art. no. 102355.

[99] J. Liu, Q. Miao, X. Fan, X. Wang, H. Lin, and Y. Huang, "Mutual-supervised federated learning and blockchain-based IoT data sharing," *Secur. Commun. Netw.*, vol. 2022, pp. 1–8, Oct. 2022.

[100] A. Alghamdi, J. Zhu, G. Yin, M. Shorfuzzaman, N. Alsufyani, S. Alyami, and S. Biswas, "Blockchain empowered federated learning ecosystem for securing consumer IoT features analysis," *Sensors*, vol. 22, no. 18, p. 6786, Sep. 2022.

[101] X. Lin, J. Wu, S. Mumtaz, S. Garg, J. Li, and M. Guizani, "Blockchain-based on-demand computing resource trading in IoV-assisted smart city," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 3, pp. 1373–1385, Jul. 2021.

[102] D. M. Manias and A. Shami, "Making a case for federated learning in the Internet of Vehicles and intelligent transportation systems," *IEEE Netw.*, vol. 35, no. 3, pp. 88–94, May 2021.

[103] J. S. Ng, W. Y. Bryan Lim, H.-N. Dai, Z. Xiong, J. Huang, D. Niyato, X.-S. Hua, C. Leung, and C. Miao, "Communication-efficient federated learning in UAV-enabled IoV: A joint auction-coalition approach," in *Proc. IEEE Global Commun. Conf.*, Dec. 2020, pp. 1–6.

[104] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Y. Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proc. 20th Int. Conf. Artif. Intell. Statist.*, 2017, pp. 1273–1282.

[105] Y. Zou, F. Shen, F. Yan, J. Lin, and Y. Qiu, "Reputation-based regional federated learning for knowledge trading in blockchain-enhanced IoV," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2021, pp. 1–6.

[106] N. Wang, W. Yang, X. Wang, L. Wu, Z. Guan, X. Du, and M. Guizani, "A blockchain based privacy-preserving federated learning scheme for Internet of Vehicles," *Digit. Commun. Netw.*, vol. 10, no. 1, pp. 126–134, Feb. 2024.

[107] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, "Membership inference attacks against machine learning models," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2017, pp. 3–18.

[108] A. Madi, O. Stan, A. Mayoue, A. Grivet-Sébert, C. Gouy-Pailler, and R. Sirdey, "A secure federated learning framework using homomorphic encryption and verifiable computing," in *Proc. Reconciling Data Anal., Autom., Privacy, Secur., Big Data Challenge (RDAAPS)*, May 2021, pp. 1–8.

[109] I. A. Omar, R. Jayaraman, K. Salah, I. Yaqoob, and S. Ellahham, "Applications of blockchain technology in clinical trials: Review and open challenges," *Arabian J. Sci. Eng.*, vol. 46, no. 4, pp. 3001–3015, Apr. 2021.

[110] S. Cao, G. Zhang, P. Liu, X. Zhang, and F. Neri, "Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain," *Inf. Sci.*, vol. 485, pp. 427–440, Jun. 2019.

[111] T. H. Nguyen, J. Partala, and S. Pirttikangas, "Blockchain-based mobility-as-a-service," in *Proc. 28th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2019, pp. 1–6.

[112] G. Rathee, A. Sharma, H. Saini, R. Kumar, and R. Iqbal, "A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology," *Multimedia Tools Appl.*, vol. 79, nos. 15–16, pp. 9711–9733, Apr. 2020.

[113] H. Hasanova, M. Tufail, U.-J. Baek, J.-T. Park, and M.-S. Kim, "A novel blockchain-enabled heart disease prediction mechanism using machine learning," *Comput. Electr. Eng.*, vol. 101, Jul. 2022, Art. no. 108086.

[114] M. A. Mohammed, A. Lakhan, D. A. Zebari, M. K. A. Ghani, H. A. Marhoon, K. H. Abdulkareem, J. Nedoma, and R. Martinek, "Securing healthcare data in industrial cyber-physical systems using combining deep learning and blockchain technology," *Eng. Appl. Artif. Intell.*, vol. 129, Mar. 2024, Art. no. 107612.

[115] S. Dhingra, R. Raut, K. Naik, and K. Muduli, "Blockchain technology applications in healthcare supply chains—A review," *IEEE Access*, vol. 12, pp. 11230–11257, 2023.

[116] S. Madumidha, P. S. Ranjani, U. Vandhana, and B. Venmuhilan, "A theoretical implementation: Agriculture-food supply chain management using blockchain technology," in *Proc. TEQIP III Sponsored Int. Conf. Microw. Integr. Circuits, Photon. Wireless Netw. (IMICPW)*, May 2019, pp. 174–178.

[117] S. Sadri, A. Shahzad, and K. Zhang, "Blockchain traceability in healthcare: Blood donation supply chain," in *Proc. 23rd Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2021, pp. 119–126.

[118] R. Brandín and S. Abrishami, "IoT-BIM and blockchain integration for enhanced data traceability in offsite manufacturing," *Autom. Construct.*, vol. 159, Mar. 2024, Art. no. 105266.

[119] R. Brophy, "Blockchain and insurance: A review for operations and regulation," *J. Financial Regulation Compliance*, vol. 28, no. 2, pp. 215–234, May 2020.

[120] M. Raikwar, S. Mazumdar, S. Ruj, S. Sen Gupta, A. Chattopadhyay, and K.-Y. Lam, "A blockchain framework for insurance processes," in *Proc. 9th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Feb. 2018, pp. 1–4.

[121] F. Loukil, K. Boukadi, R. Hussain, and M. Abed, "CioSy: A collaborative blockchain-based insurance system," *Electronics*, vol. 10, no. 11, p. 1343, Jun. 2021.

[122] C.-L. Chen, Y.-M. Zheng, D.-C. Huang, L.-C. Liu, and H.-C. Chen, "A blockchain and IPFS-based anticounterfeit traceable functionality of car insurance claims system," *Sensors*, vol. 23, no. 23, p. 9577, Dec. 2023.

[123] A. Hassan, M. I. Ali, R. Ahammed, M. M. Khan, N. Alsufyani, and A. Alsufyani, "Secured insurance framework using blockchain and smart contract," *Sci. Program.*, vol. 2021, pp. 1–11, Nov. 2021.

[124] R. Toyib, E. Sahputra, Y. Reswan, Y. Darmi, and Meisyarah, "Adoption block chain technology and Internet of Thing for medical record in health insurance," in *Proc. 13th Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2022, pp. 1539–1542.

[125] P. Bai, S. Kumar, and K. Kumar, "Use of blockchain enabled IoT in insurance: A case study of calamity based crop insurance," in *Proc. 3rd Int. Conf. Intell. Comput. Instrum. Control Technol. (ICICICT)*, Aug. 2022, pp. 1135–1141.

[126] A. Elhence, A. Goyal, V. Chamola, and B. Sikdar, "A blockchain and ML-based framework for fast and cost-effective health insurance industry operations," *IEEE Trans. Computat. Social Syst.*, vol. 10, no. 4, pp. 1642–1653, May 2023.

[127] V. Brilliantova and T. W. Thurner, "Blockchain and the future of energy," *Technol. Soc.*, vol. 57, pp. 38–45, May 2019.

[128] Z. Mingaleva, E. Shironina, and D. Buzmakov, "Implementation of digitization and blockchain methods in the oil and gas sector," in *Proc. Int. Conf. Integr. Sci.*, 2021, pp. 144–153.

[129] X. Luo and L. Mahdjoubi, "Towards a blockchain and machine learning-based framework for decentralised energy management," *Energy Buildings*, vol. 303, Jan. 2024, Art. no. 113757.

[130] H. Salmani, A. Rezazadeh, and M. Sedighizadeh, "Robust stochastic blockchain model for peer-to-peer energy trading among charging stations of electric vehicles," *J. Operation Automat. Power Eng.*, vol. 12, no. 1, pp. 54–68, 2024.

[131] Z. Liu, B. Huang, Y. Li, Q. Sun, T. B. Pedersen, and D. W. Gao, "Pricing game and blockchain for electricity data trading in low-carbon smart energy systems," *IEEE Trans. Ind. Informat.*, vol. 20, no. 4, pp. 6446–6456, Apr. 2024.

[132] V. Veerasamy, L. P. M. I. Sampath, S. Singh, H. D. Nguyen, and H. B. Gooi, "Blockchain-based decentralized frequency control of microgrids using federated learning fractional-order recurrent neural network," *IEEE Trans. Smart Grid*, vol. 15, no. 1, pp. 1089–1102, May 2024.

[133] A. Savelyev, "Copyright in the blockchain era: Promises and challenges," *Comput. Law Secur. Rev.*, vol. 34, no. 3, pp. 550–561, Jun. 2018.

[134] E. Ferro, M. Saltarella, D. Rotondi, M. Giovanelli, G. Corrias, R. Moncada, A. Cavallaro, and A. Favenza, "Digital assets rights management through smart legal contracts and smart contracts," *Blockchain, Res. Appl.*, vol. 4, no. 3, Sep. 2023, Art. no. 100142.

[135] Z. Meng, T. Morizumi, S. Miyata, and H. Kinoshita, "Design scheme of copyright management system based on digital watermarking and blockchain," in *Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Jul. 2018, pp. 359–364.

[136] Binded. (2019). *Liquidity Copyright Made Simple*. [Online]. Available: https://binded.com/index.html/

[137] Copytrack. (2015). *IND Stolen Images & Enforce Copyrights*. [Online]. Available: https://www.copytrack.com/

[138] M. H. Berenjestanaki, H. R. Barzegar, N. E. Ioini, and C. Pahl, "Blockchain-based e-voting systems: A technology review," *Electronics*, vol. 13, no. 1, p. 17, Dec. 2023.

[139] R. Bosri, A. R. Uzzal, A. A. Omar, A. S. M. T. Hasan, and Md. Z. A. Bhuiyan, "Towards a privacy-preserving voting system through blockchain technologies," in *Proc. IEEE Int. Conf. Dependable, Autonomic Secure Comput., Int. Conf. Pervasive Intell. Comput., Int. Conf. Cloud Big Data Comput., Int. Conf. Cyber Sci. Technol. Congr. (DASC/PiCom/CBDCom/CyberSciTech)*, Aug. 2019, pp. 602–608.

[140] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, Aug. 2016, pp. 25–30.

[141] M. Kassab, J. DeFranco, T. Malas, P. Laplante, G. Destefanis, and V. V. G. Neto, "Exploring research in blockchain for healthcare and a roadmap for the future," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 4, pp. 1835–1852, Oct. 2021.

[142] E. Chukwu and L. Garg, "A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations," *IEEE Access*, vol. 8, pp. 21196–21214, 2020, doi: 10.1109/ACCESS.2020.2969881.

[143] M. S. B. Kasyapa and C. Vanmathi, "Blockchain integration in healthcare: A comprehensive investigation of use cases, performance issues, and mitigation strategies," *Frontiers Digit. Health*, vol. 6, Apr. 2024, Art. no. 1359858.

[144] I. A. Omar, R. Jayaraman, M. S. Debe, K. Salah, I. Yaqoob, and M. Omar, "Automating procurement contracts in the healthcare supply chain using blockchain smart contracts," *IEEE Access*, vol. 9, pp. 37397–37409, 2021, doi: 10.1109/ACCESS.2021.3062471.

[145] T. Ferdousi, D. Gruenbacher, and C. M. Scoglio, "A permissioned distributed ledger for the U.S. beef cattle supply chain," *IEEE Access*, vol. 8, pp. 154833–154847, 2020, doi: 10.1109/ACCESS.2020.3019000.

[146] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102407.

[147] M. Singh, G. Baranwal, and A. K. Tripathi, "Integrating blockchain for healthcare group decision making," in *Proc. IEEE 1st Global Emerg. Technol. Blockchain Forum, Blockchain Beyond (iGETblockchain)*, Irvine, CA, USA, Nov. 2022, pp. 1–6, doi: 10.1109/iGETblockchain56591.2022.10087092.

[148] M. S. Kasyapa, "A privacy protection mechanism for Indian health care data exchange using blockchain," in *Proc. Innov. Power Adv. Comput. Technol. (i-PACT)*, vol. 12, Kuala Lumpur, Malaysia, Dec. 2023, pp. 1–9, doi: 10.1109/i-pact58649.2023.10434770.

[149] J. Jayabalan and N. Jeyanthi, "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy," *J. Parallel Distrib. Comput.*, vol. 164, pp. 152–167, Jun. 2022.

[150] S. Lee, Y. Kim, and S. Cho, "Searchable blockchain-based healthcare information exchange system to enhance privacy preserving and data usability," *Sensors*, vol. 24, no. 5, p. 1582, Feb. 2024.

[151] G. Verma, "Blockchain-based privacy preservation framework for healthcare data in cloud environment," *J. Experim. Theor. Artif. Intell.*, vol. 36, no. 1, pp. 147–160, Jan. 2024.

[152] T. Kumari, M. Singh, G. Baranwal, and A. K. Tripathi, "Supplier selection in healthcare using blockchain," in *Proc. IEEE 1st Global Emerg. Technol. Blockchain Forum, Blockchain Beyond (iGETblockchain)*, Irvine, CA, USA, Nov. 2022, pp. 1–6, doi: 10.1109/iGETblockchain56591.2022.10087053.

[153] A. Nawaz, L. Wang, M. Irfan, and T. Westerlund, "Hyperledger sawtooth based supplychain traceability system for counterfeit drugs," *Comput. Ind. Eng.*, vol. 190, Apr. 2024, Art. no. 110021.

[154] U. J. Munasinghe and M. N. Halgamuge, "Supply chain traceability and counterfeit detection of COVID-19 vaccines using novel blockchain-based Vacledger system," *Expert Syst. Appl.*, vol. 228, Jan. 2023, Art. no. 120293.

[155] P. K. Patro, R. Jayaraman, K. Salah, and I. Yaqoob, "Blockchain-based traceability for the fishery supply chain," *IEEE Access*, vol. 10, pp. 81134–81154, 2022, doi: 10.1109/ACCESS.2022.3196162.

[156] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "PrivChain: Provenance and privacy preservation in blockchain enabled supply chains," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Aug. 2022, pp. 157–166, doi: 10.1109/Blockchain55522.2022.00030.

[157] M. Demir, O. Turetken, and A. Ferworn, "Blockchain based transparent vehicle insurance management," in *Proc. 6th Int. Conf. Softw. Defined Syst. (SDS)*, Rome, Italy, Jun. 2019, pp. 213–220, doi: 10.1109/SDS.2019.8768669.

[158] Z. Li, Z. Xiao, Q. Xu, E. Sotthiwat, R. S. Mong Goh, and X. Liang, "Blockchain and IoT data analytics for fine-grained transportation insurance," in *Proc. IEEE 24th Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Singapore, Dec. 2018, pp. 1022–1027, doi: 10.1109/PADSW.2018.8644599.

[159] Z. Wan, Z. Guan, and X. Cheng, "PRIDE: A private and decentralized usage-based insurance using blockchain," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Halifax, NS, Canada, Jul. 2018, pp. 1349–1354, doi: 10.1109/Cybermatics_2018.2018.00232.

[160] B. Wang, M. Dabbaghjamanesh, A. Kavousi-Fard, and S. Mehraeen, "Cybersecurity enhancement of power trading within the networked microgrids based on blockchain and directed acyclic graph approach," *IEEE Trans. Ind. Appl.*, vol. 55, no. 6, pp. 7300–7309, Nov. 2019, doi: 10.1109/TIA.2019.2919820.

[161] H. Li, H. Hui, and H. Zhang, "Decentralized energy management of microgrid based on blockchain-empowered consensus algorithm with collusion prevention," *IEEE Trans. Sustain. Energy*, vol. 14, no. 4, pp. 2260–2273, Oct. 2023, doi: 10.1109/TSTE.2023.3258452.

[162] A. Sheikh, V. Kamuni, A. Urooj, S. Wagh, N. Singh, and D. Patel, "Secured energy trading using Byzantine-based blockchain consensus," *IEEE Access*, vol. 8, pp. 8554–8571, 2020, doi: 10.1109/ACCESS.2019.2963325.

[163] M. Moniruzzaman, A. Yassine, and R. Benlamri, "Blockchain and cooperative game theory for peer-to-peer energy trading in smart grids," *Int. J. Electr. Power Energy Syst.*, vol. 151, Sep. 2023, Art. no. 109111.

[164] SolarCoin. (2023). *SolarCoin is a Cryptocurrency That Incentivizes a Solar-Powered Planet*. [Online]. Available: https://solarcoin.org/

[165] M. Naik, A. P. Singh, N. R. Pradhan, N. Kumar, A. Nayak, and M. Guizani, "TokenGreen: A versatile NFT framework for peer-to-peer energy trading and asset ownership of electric vehicles," *IEEE Internet Things J.*, vol. 11, no. 8, pp. 13636–13646, Apr. 2024, doi: 10.1109/jiot.2023.3340155.

[166] KWHCoin. (2023). *KWHCoin Whitepaper*. [Online]. Available: https://ww1.prweb.com/prfiles/2018/01/19/15109995/KWHCoin-White-Paper-REVISED.pdf

[167] K. Jian, "Energy coin: A universal digital currency based on free energy," *Amer. J. Mod. Energy*, vol. 6, no. 5, p. 95, 2020.

[168] M. B. Mollah, J. Zhao, D. Niyato, K.-Y. Lam, X. Zhang, A. M. Y. M. Ghias, L. H. Koh, and L. Yang, "Blockchain for future smart grid: A comprehensive survey," *IEEE Internet Things J.*, vol. 8, no. 1, pp. 18–43, Jan. 2021, doi: 10.1109/JIOT.2020.2993601.

[169] C. Hua, S. Wu, Y. Zhang, K. Luo, M. Li, and J. Fu, "A blockchain-based framework for rural property rights transactions," *Electronics*, vol. 12, no. 20, p. 4334, Oct. 2023. [Online]. Available: https://doi-org.egateway.vit.ac.in/10.3390/electronics12204334

[170] H. Song, N. Zhu, R. Xue, J. He, K. Zhang, and J. Wang, "Proof-of-contribution consensus mechanism for blockchain and its application in intellectual property protection," *Inf. Process. Manage.*, vol. 58, no. 3, May 2021, Art. no. 102507.

[171] P. Zhu, J. Hu, X. Li, and Q. Zhu, "Using blockchain technology to enhance the traceability of original achievements," *IEEE Trans. Eng. Manag.*, vol. 70, no. 5, pp. 1693–1707, May 2023, doi: 10.1109/TEM.2021.3066090.

[172] W. Sun, H. Fang, S. Zheng, and Q. Qian, "Blockchain and homomorphic encryption for digital copyright protection," in *Proc. IEEE Int. Conf. Parallel Distrib. Process. Appl., Big Data Cloud Comput., Sustain. Comput. Commun., Social Comput. Netw. (ISPA/BDCloud/SocialCom/SustainCom)*, Exeter, U.K., Dec. 2020, pp. 754–761, doi: 10.1109/ISPA-BDCloud-SocialCom-SustainCom51426.2020.00120.

[173] G. J. Showkatramani, N. Khatri, A. Landicho, and D. Layog, "A secure permissioned blockchain based system for trademarks," in *Proc. IEEE Int. Conf. Decentralized Appl. Infrastruct. (DAPPCON)*, Newark, CA, USA, Apr. 2019, pp. 135–139, doi: 10.1109/DAPPCON.2019.00026.

[174] S. Vidwans, A. Deshpande, P. Thakur, A. Verma, and S. Palwe, ''Permissioned blockchain voting system using hyperledger fabric,'' in *Proc. Int. Conf. IoT Blockchain Technol. (ICIBT)*, Ranchi, India, May 2022, pp. 1–6, doi: 10.1109/ICIBT52874.2022.9807702.

[175] P. M. Bhamare, P. P. Kulkarni, A. Mhetre, K. Shipra, S. Wani, and V. Pai, ''Revolutionizing college elections with a secure blockchain voting solution,'' in *Proc. IEEE 5th Int. Conf. Cybern., Cognition Mach. Learn. Appl. (ICCCMLA)*, vol. 151, Hamburg, Germany, Oct. 2023, pp. 121–125, doi: 10.1109/icccmla58983.2023.10346825.

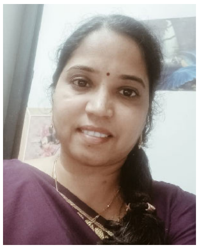
[176] R. B. Ardak and D. A. S. Bardekar, ''Smart voting system using deep learning and computer vision,'' *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 10, no. 5, pp. 4462–4471, May 2022.

[177] L. Wang, M. Hu, Z. Jia, B. Gong, and Y. Lei, ''A signature scheme applying on blockchain voting scene based on the asmuth-Bloom algorithm,'' in *Proc. IEEE 4th Int. Conf. Comput. Commun. (ICCC)*, Chengdu, China, Dec. 2018, pp. 2372–2378, doi: 10.1109/COMPCOMM.2018.8780775.

[178] V. Chithanuru and M. Ramaiah, ''An anomaly detection on blockchain infrastructure using artificial intelligence techniques: Challenges and future directions—A review,'' *Concurrency Comput., Pract. Exper.*, vol. 35, no. 22, p. e7724, Oct. 2023, doi: 10.1002/cpe.7724.

[179] A. Padma and M. Ramaiah, ''Blockchain based an efficient and secure privacy preserved framework for smart cities,'' *IEEE Access*, vol. 12, pp. 21985–22002, 2024, doi: 10.1109/access.2024.3364078.

[180] M. Ramaiah, R. M. Yousuf, R. Vishnukumar, and A. Padma, ''A technologies study on trending for IoT use cases aspires to build sustainable smart cities,'' in *Intelligent Systems and Sustainable Computational Models: Concepts, Architecture, and Practical Applications*. New York, NY, USA: CRC Press, 2024, p. 48.



C. VANMATHI received the bachelor's degree in computer science from the University of Madras, the master's degree in information technology from Sathyabama University, and the Ph.D. degree in information technology and engineering from Vellore Institute of Technology (VIT) University, Vellore Campus, India. She is currently an Associate Professor Senior with the School of Computer Science Engineering and Information Systems, VIT, Vellore Campus. With 21 years of comprehensive teaching and research experience in her role, she specializes in areas, such as image processing, deep learning, computer vision, blockchain, cyber-physical systems, and the Internet of Things. She is an active member of the Computer Society of India and the Soft Computing Research Society.

AHMED FAROUK is currently an Assistant Professor with South Valley University, Hurghada, Egypt. Before that, he was a Postdoctoral Research Fellow with Wilfrid Laurier University and Ryerson University, Canada. He has been awarded the Lindau Nobel Laureate Alumni, CDL University of Toronto Alumni, and Outstanding IEEE Computer Chapter for K-W Region 2020. He is exceptionally well known for his seminal contributions to theories of quantum information, machine learning, and cryptography. He has published over 80 articles in reputed and high-impact publications like the IEEE Internet of Things Journal, IEEE Transactions on Intelligent Transportation Systems, IEEE Wireless Communications, and IEEE Transactions on Industrial Informatics (IEEE TII). His volunteer work is apparent since, he was appointed as the Chair of the IEEE Computer Society Chapter for the Waterloo-Kitchener area and has joined the editorial boards of many reputed journals. Recently, he was appointed as an Officer (Secretary) of the IEEE Technical Committee on Quantum in Consumer Technology.

SARAH M. ALHAMMAD received the Ph.D. degree in computer science from the University of Plymouth, U.K. She is currently an Assistant Professor in computer science with the Department of Computer Science, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Saudi Arabia. A strong theme of her work is computer visualization, software engineering, human–computer interaction, and image processing.

R. MANGAYARKARASI received the M.E. degree in computer science from Anna University and the Ph.D. degree in information technology and engineering from VIT University, Vellore, India. She is currently an Associate Professor with the School of Computer Science Engineering and Information Systems, VIT University. She has attended many national and international conferences and published articles in reputed journals. Her research interests include computer vision, image processing, machine learning, and artificial intelligence.

SWETA BHATTACHARYA received the master's degree in industrial and systems engineering from the State University of New York, Binghamton, USA, and the Ph.D. degree from Vellore Institute of Technology. She is currently an Associate Professor with the School of Information Technology and Engineering, Vellore Institute of Technology (University). She has guided various UG and PG projects and published peer-reviewed research articles. Her research experience includes working on Pill Dispensing Robotic Projects as a fully funded Watson Research Scholar at Innovation Associates, Binghamton, and SUNY. She has completed six Sigma Green Belt Certifications from Dartmouth College, Hanover. Her research interests include applications of machine learning algorithms, data mining, simulation and modeling, applied statistics, quality assurance, and project management. She is also a member of the Computer Society of India and Indian Science Congress.

MEENAVOLU S. B. KASYAPA received the Bachelor of Technology and Master of Technology degrees in computer science and engineering from Jawaharlal Nehru Technological University Hyderabad (JNTUH), in 2011 and 2017, respectively. He is currently pursuing the Ph.D. degree in blockchain with Vellore Institute of Technology (VIT University), Vellore. His research interests include blockchain security and performance.