sustainability

Review

Blockchain for Internet of Underwater Things: State-of-the-Art, Applications, Challenges, and Future Directions

Sweta Bhattacharya [1,2], Nancy Victor [2], Rajeswari Chengoden [2], Murugan Ramalingam [2], Govardanan Chemmalar Selvi [2], Praveen Kumar Reddy Maddikunta [2], Praveen Kumar Donta [3], Schahram Dustdar [3], Rutvij H. Jhaveri [4] and Thippa Reddy Gadekallu [1,2,*]

1 Department of Electrical and Computer Engineering, Lebanese American University, Byblos P.O. Box 13-5053, Lebanon
2 School of Information Technology and Engineering, Vellore Institute of Technology, Vellore 632014, Tamilnadu, India
3 Distributed Systems Group, TU Wien, 1040 Vienna, Austria
4 Department of Computer Science and Engineering, School of Technology, Pandit Deendayal Energy University, Gandhinagar 382426, Gujarat, India
* Correspondence: thippareddy.g@vit.ac.in

Abstract: The Internet of Underwater Things (IoUT) has become widely popular in the past decade as it has huge prospects for the economy due to its applicability in various use cases such as environmental monitoring, disaster management, localization, defense, underwater exploration, and so on. However, each of these use cases poses specific challenges with respect to security, privacy, transparency, and traceability, which can be addressed by the integration of blockchain with the IoUT. Blockchain is a Distributed Ledger Technology (DLT) that consists of series of blocks chained up in chronological order in a distributed network. In this paper, we present a first-of-its-kind survey on the integration of blockchain with the IoUT. This paper initially discusses the blockchain technology and the IoUT and points out the benefits of integrating blockchain technology with IoUT systems. An overview of various applications, the respective challenges, and the possible future directions of blockchain-enabled IoUT systems is also presented in this survey, and finally, the work sheds light on the critical aspects of IoUT systems and will enable researchers to address the challenges using blockchain technology.

Keywords: Internet of Underwater Things; ocean ecosystem; privacy; security

check for updates

Citation: Bhattacharya, S.; Victor, N.; Chengoden, R.; Ramalingam, M.; Chemmalar Selvi G.; Maddikunta, P.K.R.; Donta, P.K.; Dustdar, S.; Jhaveriand, R.H.; Gadekallu, T.R. Blockchain for Internet of Underwater Things: State-of-the-Art, Applications, Challenges, and Future Directions. *Sustainability* **2022**, *14*, 15659. https://doi.org/10.3390/su142315659

Academic Editor: Choongwan Koo

Received: 13 October 2022
Accepted: 22 November 2022
Published: 24 November 2022

1. Introduction

Two-thirds of the Earth's surface are covered with water bodies such as oceans, seas, rivers, and ponds. Marine life consists of numerous plants, animals, and other living organisms [1]. The climatic patterns in water bodies often influences severe weather patterns such as cyclones, typhoons, tornadoes, tsunamis, and others [2–4]. Marine transportation plays a significant role in the supply chain management of essential goods such as oil, food, minerals, metals, and more [5]. Fish, crab, prawn, and others are major foods for the majority of the human population across the globe. The livelihood of many people across the globe depends on fisheries [6,7]. Oceans are also rich sources of oil and other natural resources [8]. Hence, constant monitoring of marine life, climatic conditions of the oceans, and transportation systems are of paramount importance not only to the ocean ecosystem, but also to navy applications and the food security of the water population [9]. Most of these water bodies have not been much explored. The Internet of Things (IoT) [10] plays a major role in monitoring the aforementioned activities in water bodies, where several sensors are placed at several locations in water bodies [11–13]. Due to the rapid growth of the IoT and its applications in several forms of human life including monitoring of the underwater environment, a new form of the IoT, namely, the IoUT has emerged.

The IoUT is a network of sensors and smart devices that are placed underwater and are interconnected, which can monitor, sense, relay, and collect data from the water bodies and share the data with the base stations located in terrestrial areas. The IoUT has several applications including marine monitoring, coastal area surveillance, exploration of marine life, oil rig maintenance, defense, and so on [14–16].

The IoUT has been a predominant choice for researchers, having applications in deep sea exploration, system monitoring of divers, generating warnings, naval surveillance systems, and various other applications. IoUT devices are normally fixed or mobile with the ability to move from one location to the other to collect or transmit information using digitally linked devices installed in the water bodies. There are associated devices such as gateways, satellites, and base stations that help in expanding the communication range in such IoUT applications. The recent studies conducted by the United States National Oceanic and Atmospheric Administration (NOAA) revealed the fact that 71 percent of the Earth is covered with water [17]. IoUT devices are integrated with smart sensing devices, which have heterogeneous functionalities. Although various researchers have proposed innovative methodologies and designs to develop various IoUT applications, there exist certain challenges relevant to the type of applications, the channel types, and their characteristics. The benefits of IoT- and IoUT-based devices are numerous, yet there are challenges subject to sensor resource scarcity, wireless network stability, data security, privacy, fault resilience, and several others. The traditional solutions often fail to overcome such challenges due to the inability to handle the large volumes of data collected by the sensor devices, the huge variability in the devices being used, the lack of trust among the participants, and also, transparency issues in the management of data. Various studies have been conducted emphasizing the IoUT, its architecture, technologies, research challenges, and the scope of future research. A review of these studies is presented below.

The study in [18] explored the contribution of the IoUT in monitoring vast areas of unexplored water bodies on our planet. The primary differences between the IoUT and IoT were identified in association with the presentation of a detailed IoUT architectural framework. Furthermore, various applications of the IoUT were highlighted, and the critical challenges in such applications were identified and addressed. The study in [19] presented an exhaustive review of the application of the IoUT emphasizing its contribution to Big Marine Data (BMD) analytics. The traditional use of BMD has its associated challenges, where the classical data processing techniques fail to serve the purpose. The paper thus explored the nexus of BMD with machine learning [20] for handling marine data. The paper also presented the potential directions of research incorporating the use of BMD and the IoUT, inspiring researchers to develop new tools and techniques in this domain. The study in [21] discussed various Underwater Network Management Systems (U-NMSs) that use acoustic communication involving the IoUT. The fault, configuration, accounting, performance, security [22], and constraint management aspects of U-NMSs were also elaborated. The paper also presented the prototype of a U-NMS framework being implemented in a library environment using lightweight machine-to-machine and acoustic technology. In [23], the primary emphasis was on the use of an Underwater Wireless Sensor Network (UWSN) and related technology of the IoUT. Traditional UWSN implementations have associated limitations of the underlying acoustic communication medium, higher levels of energy consumption, and a lack of hardware resources, which are required to perform the computationally intensive tasks. Additionally, UWSN technologies are vulnerable to various attacks, namely wormhole, spoofing, jamming, flooding, and various other attacks, which act as a real threat to secured IoUT implementations, where the frameworks need to function in harsh communication conditions. The study in [23] focused on mitigating the security risks and challenges in the use of UWSNs in IoUT implementations. It is evident from all the aforementioned reviews that an optimal communication network is a necessity for the successful implementation of IoUT applications. The study in [24] highlighted the challenges associated with the physical, Medium Access Control (MAC), and network layers while designing optimal IoUT networks. A huge variability in the underwater ecosystem exists, and hence, detailed knowledge about the prevailing underwater regional profiles makes it a necessity. The understanding of the profiles enables the constraints to be addressed for achieving optimized performance in IoUT networks and their deployment.

The study in [25] highlighted the need for efficient environmental monitoring considering the perspective of smart cities and recent natural disasters that have impacted the globe. Research related to UWSNs and the IoUT have also gained momentum due to the same reason, especially in the development of tethered Remotely Operated Underwater Vehicles (ROUVs), untethered Autonomous Underwater Vehicles (AUVs), Unmanned Autonomous Surface Vehicles (USVs/ASVs), and various other smart underwater technologies. This study conducted a systematic bibliographic analysis of the various studies conducted globally on UWSN implementations in the IoUT prioritizing the African region. The study finally concluded by directing possible technical recommendations in the successful actualization of IoUT and WSN research projects in the African region.

The study in [16] discussed the role of the IoUT as a powerful technology in developing various applications relevant to naval operations, military services, maritime security, natural disaster prediction, and archaeological expeditions. This study introduced an IoUT network framework which works in naturally heterogeneous and unpredictable ocean conditions. The enabling technologies of the IoUT such as channel models, network protocols, topologies, and simulation tools and the use of edge computing, data analytics, Optical Wireless Communications (OWCs), machine learning, and Intelligent Reflecting Surfaces (IRSs) were discussed. The study in [26] presented a comprehensive survey of various unmanned underwater vehicles that use technologies such as cognitive acoustic networks, fog computing, the IoUT, and distinct next-generation underwater networks. These vehicles include ray tracing models that enable target detection and tracking, which are primarily used by military forces. The study in [27] initially discussed the role of acoustic, InfraRed (IR), visible light, Radio-Frequency (RF), and magnetic induction in transmitting information using digitally linked underwater devices. However, these media have their associated challenges relevant to the narrow channel bandwidth, low data rate, and higher cost. Similarly, the optical medium has the associated challenges of high absorption, scattering, and long-distance data transmission. Furthermore, the possibility of malicious nodes stealing underwater data through black hole attacks, routing attacks, and Sybil attacks exists. In [27], an extensive review of the recent trends, applications, communication technologies, challenges, and threats of the UIoT environment are presented. Each of the reviewed articles emphasized recent trends, technologies, applications, use cases, and the challenges associated with IoUT applications. The comparison of this survey with existing surveys is summarized in Table 1. The knowledge gained from the review of these articles reveals the need for an extensive review article focusing on security, the privacy of data, and also, the data transmission in IoUT frameworks. This motivated us to initiate a first-of-its-kind survey focusing on the applications of blockchain in IoUT systems. The key contributions of this survey are as follows:

- A first-of-its-kind survey is presented on applications of blockchain for the IoUT.
- An exhaustive review on the use of blockchain in IoUT applications is presented.
- A discussion on the challenges and future prospects of research relevant to the integration of blockchain in IoUT applications is presented.

The rest of the the paper is organized as follows: Section 2 presents the required background knowledge relevant to blockchain, the IoUT, and its integration with blockchain followed by Section 3, which discusses various applications of the same. Section 4 presents the challenges associated with blockchain-integrated IoUT applications providing insight into the plausible scope of future directions of research. Figure 1 depicts the schematic outline of this study.

Table 1. Comparison with existing surveys.

Ref	Contributions	Limitations
[18]	-The role of the IoUT in preserving natural water resources is discussed. -The differences of the IoUT and IoT are highlighted. -The architecture and applications of the IoUT are presented. -The potential challenges and solutions are addressed.	-The integration of the IoUT with other advanced technologies are not explored. -The security aspects of the IoUT applications are not explored.
[19]	-The concept of BMD is initiated considering the enormous size and variability of marine data collected from harsh and heterogeneous environments using the IoUT. -The traditional challenges of using BMD processing is explored. -The use of ML in handling BMD is presented. -The potential scope of future research in the IoUT and BMD is highlighted.	-More emphasis is given to underwater communication and network protocols and BMD data handling. -Security and privacy aspects of handling BMD are not considered.
[21]	-Underwater Network Management Systems (U-NMS) using acoustic communication and the IoUT are discussed. -A prototype implementation of a U-NMS in a library environment is presented.	-The viability of the prototype model in a real-world setup is not justified.
[23]	-Emphasizes the security threats related to UWSNs in IoUT implementations.	-Risk mitigation activities include the use of network protocols. -Alternative advanced approaches such as blockchain are not explored.
[24]	-Presents a review of existing research relevant to signal processing and routing for developing efficient IoUT systems. -The challenges mostly emphasize exploring various forms of network attacks and possible solutions along with research testbeds.	-The MAC protocol, QoS metrics, and related performance issues are discussed. -Solutions focus on secured transmission of data and not on the storage aspect of the same.
[25]	-The use of WSNs and the IoUT in developing underwater vehicles (ROUVs), untethered Autonomous Underwater Vehicles (AUVs), Unmanned Autonomous Surface Vehicles (USVs/ASVs), and various other smart underwater technologies are explored. -Different UWSN-based IoUT implementations in the African region are analyzed.	-The scope of review includes only the African region while missing the security aspect.
[16]	-Different network frameworks used in IoUT applications are discussed. -The use of edge computing, data analytics, Optical Wireless Communications (OWCs), machine learning, and Intelligent Reflecting Surfaces (IRSs) in the IoUT is presented.	-The role of a specific technology and its related contributions are not focused on, making the scope generic.
[26]	-A survey on various unmanned water vehicles is presented. -The use of cognitive acoustic networks, fog computing, the IoUT, and next-generation underwater networks is discussed.	-Primarily emphasizes the target detection and tracking scheme. -Security and privacy aspects of the collected data through the IoUT are not considered.
[27]	-Distinct forms of IoUT attacks in the form of black holes, routing, and Sybil are discussed.	-Focused primarily on IoUT network attacks and their prevention. -Security and privacy aspects of the collected data through the IoUT are not included.
The present survey	-The first-of-its-kind survey on the application of blockchain for the IoUT. -Applications of blockchain in the IoUT are discussed. -Challenges and future prospects of the integration of blockchain with the IoUT are highlighted.	-

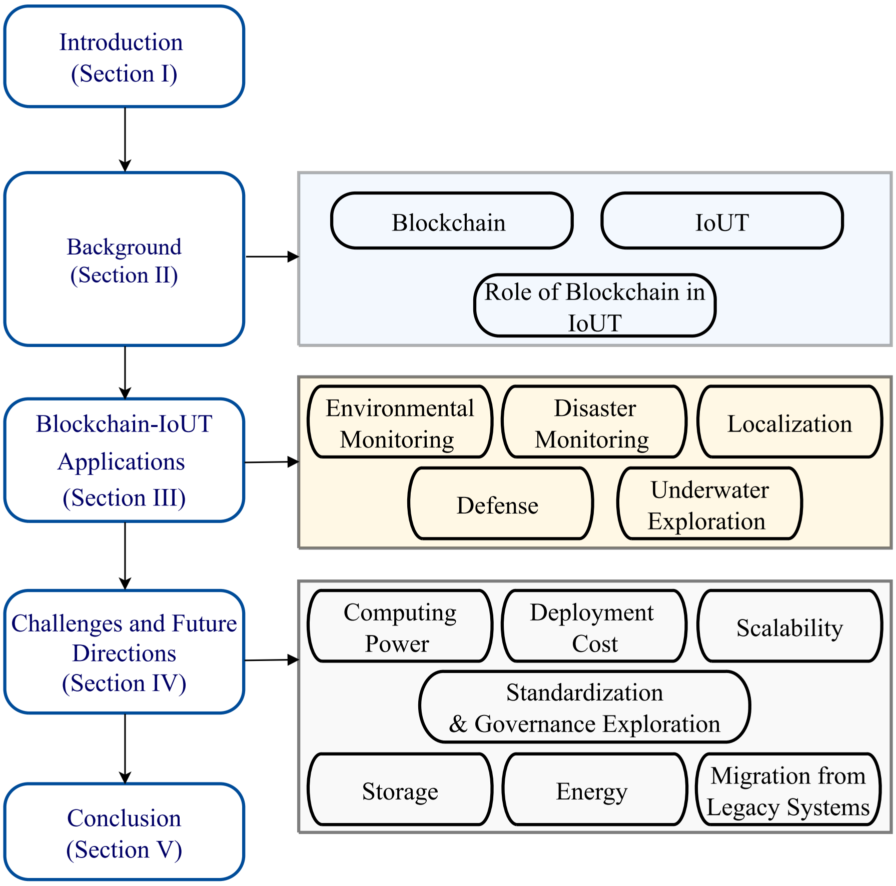

Figure 1. Schematic outline of the work.

2. Background

This section discusses the basic concepts and recent advancements in blockchain and the IoUT, followed by the motivation behind the integration of blockchain with the IoUT.

2.1. Blockchain

Blockchain is a decentralized digital database carrying a chain of cryptographically signed blocks over a peer-to-peer network [28,29]. The advancement of blockchain [30] surpassed the evolution of cryptocurrency and bitcoin with its unique significant features of maintaining transparency and preserving privacy in the distributed network [31,32]. This leverages the power of utilizing blockchain technology in various sectors [33] including finance and trading [34,35], supply chain management [36,37], medicine and healthcare [38,39], the IoT [40–42], and many other industrial services [43–45].

The blocks in the blockchain are generally arranged in a particular order, which contains the original data. Each block points to the preceding block using a hash value. The first block, called the genesis block, does not point to any block and, thus, is the parent/root block to the other subsequent child blocks. Each child holds a unique hash key, which is linked to the preceding block, also known as the parent block [46,47]. The simplified architecture of blockchain and its components is illustrated in Figure 2.

Figure 3 illustrates the connection of blocks and the Merkle tree connecting transactions to the block header. The digital signature is another significant component in the blockchain architecture. The user possesses two keys: public and private key. The transactions are secured by signing using the private key, and this digitally signed transaction is shared across the whole network. The public key is used to access the data present in the transaction by the authorized user. Hence, the generation of the digital signature is a two-step process, which includes the signing and verification process [48].

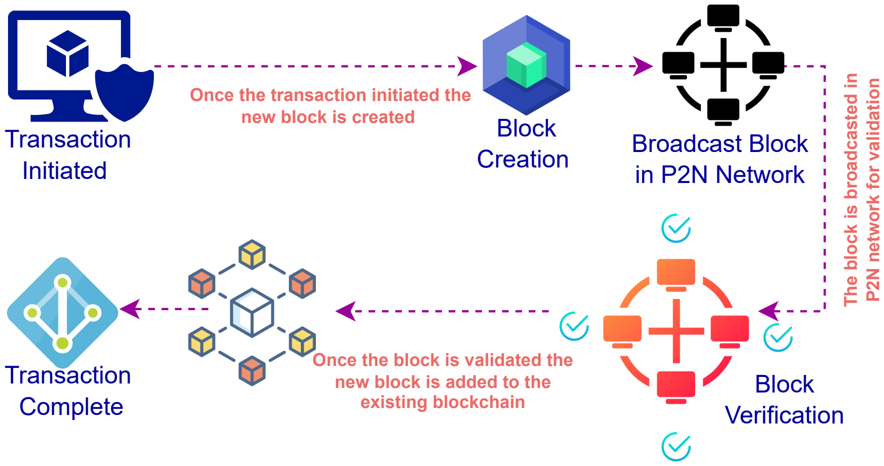

Figure 2. Data communication using blockchain technology.

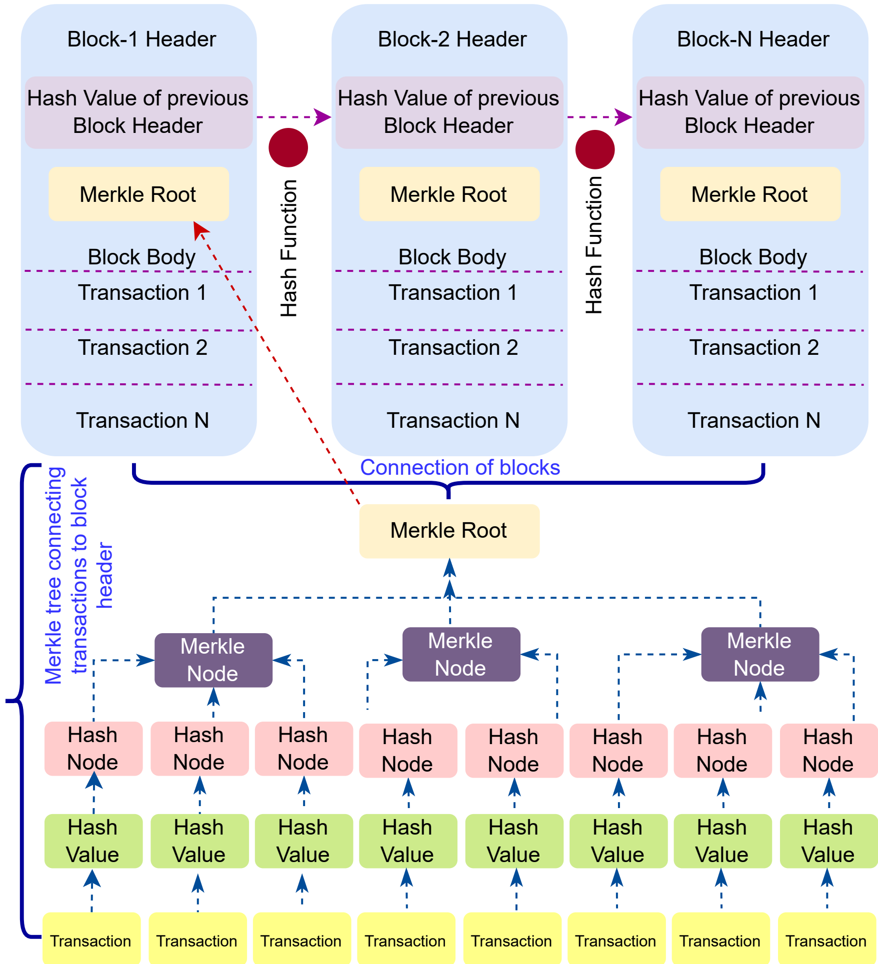

Figure 3. Connection of blocks and Merkle tree connecting transactions to a block header.

Following are the salient features of blockchain technology [49] that contribute to the powerful applications [50,51] in this digital era:

1. *Immutability*—Blockchain is a permanent and unalterable network that promises no chance of changing the nodes in the network. The blockchain network has several nodes chained to each other, and every node maintains a copy of the digital ledger in the network. Hence, any transaction initiated in the network is authenticated and

verified to be included in the ledger. As a result, the data stored in any transaction are highly impossible to tamper with, as they are strictly protected by the nodes of the given network. This promotes the network to be highly transparent and secure, creating successful transactions with the consensus of all nodes in the network. Thus, it allows anyone to view the transactions, but does not give access to edit or modify the data in the transactions.

2. *Decentralization*—The framework is not operated under a single authority; rather, a collection of nodes is involved in managing and maintaining the blockchain network. The network is deployed on a peer-to-peer network, enabling each node to have a copy of the digital ledger, unlike the conventional banking system. Hence, the cost to hack such a decentralized network is more expensive, making it one of the most important features of blockchain technology.
3. *Smart contracts*—Blockchain executes the transactions in a faster way by applying the smart contract principle. Smart contracts are self-executing digital contracts that automatically execute the transactions when certain conditions and agreements are satisfied for the current transaction.
4. *Consensus protocol*—The consensus mechanism is the fault-tolerance mechanism in which nodes in the peer-to-peer network accede a common agreement about the current state of transactions in the network. This ensures the data reliability and trustworthiness of transactions among the nodes of blockchain. The Proof-of-Work (PoW) is the robust consensus protocol used widely in banking services and other applications. The PoW ensures that the new block is created by solving extreme and computationally complex puzzles to avoid unreliable transactions [52,53].
5. *Transparency*—The blockchain network renders unparalleled transparency, which ensures advanced data security solutions [54]. Hence, every single transaction taking place within the decentralized network is confirmed by the majority of the nodes in the network. Thus, any updated transaction can be viewed by the user while managing the transparency within the network.

2.2. Internet of Underwater Things

The IoT is revolutionizing society through applications such as smart cities, precision agriculture, smart healthcare, and more [55,56]. It is defined as an ecosystem that interconnects a physical device to other physical devices or things across the world, which are interconnected through the Internet. The IoT can play a vital role in several activities/applications in the marine industry as well. The continuous improvement of IoT technology in marine applications has led to the development of a new class known as the Internet of Underwater Things (IoUT) [16,57]. The IoUT is described as the interconnection of smart intelligent devices that are either fixed or mobile under the water's surface. In recent years, several underwater smart objects have been developed, of which the Autonomous Surface Vehicles (ASVs) [58], Autonomous Underwater Vehicles (AUVs) [59], and Remotely Operated underwater Vehicles (ROVs) [60] are prominent smart devices for exploring the underwater resources.

The IoUT has some similarities with the terrestrial counterpart the IoT such as structure and function. However, it also has different characteristics [18] when compared with the terrestrial IoT such as:

1. Different communication technologies;
2. Different tracking methodologies;
3. Difficulty in recharging the battery;
4. Different energy harvesting technologies;
5. Different network density;
6. Different localization techniques.

The IoUT ecosystem is deployed with an enormous number of intelligent smart objects. As a consequence, the growing demand for device communication and networking with these devices brings a new challenge to this ecosystem. The intrinsic component required for the device communication is the medium or channel through which the information is shared among the smart objects within the network [24]. The UWSN is one of the existing network systems for underwater communication, which is used in several recent IoUT projects [61–63]. UWSN systems are deployed with numerous underwater sensors mounted with acoustic modems, which are responsible for collecting further significant information such as water temperature, chemical components, pressure, and so on. The collected data are forwarded to different agents on the water surface called the sinks, which are designed with acoustic and radio modems. The sink transfers the information received from the sensor node (acoustic modem) to the remote monitoring center (radio modem) [64].

With the advancement of the IoUT, several researchers are actively exploring underwater research to interact with the communication devices, thus enabling smart sea technology. As a result, a significant number of IoUT sensors act not only as data collection points, but also facilitate the functioning of other underwater components such as cameras, hydrophones, actuators, and others. Among these, a few remarkable sensors were discussed in [19]. AUVs use acoustic sensors to measure the navigation path and positioning of the smart objects. To detect whether the smart objects are present or not, proximity sensors are used to find the nearby objects by sending electrical signals. Pressure sensors are utilized to determine the pressure level, which is helpful for environmental monitoring applications. Ocean researchers use this significant information generated by the sensors in the IoUT to carefully investigate the unexplored parts of ocean life and underwater resources.

2.3. Integration of Blockchain with the IoUT

The principal motivations to integrate blockchain with the IoUT are discussed as follows:

1. *Improving security in underwater communication*—The sensors capture the significant information and relay and send the data to the monitoring center present on the land surface. The information transmitted is highly sensitive, which brings several problems such as data stealing, network hacking, and breaking the communication systems [65]. There is also a dire need to provide secured and trusted solutions for the processing and storage of the enormous amount of data being generated from the IoUT devices. The blockchain-based network architectures provide solutions to the aforementioned challenges by providing immutability and trustworthy data sharing and management and also enable efficient monitoring and tracking of the underwater devices, processes, and related resources. Blockchain [66] ensures secured and trusted data sharing in the underwater communications without interventions from humans or third parties. Furthermore, the need for autonomous decision-making in the hostile underwater environment with fickle network connectivity with base stations is supported by blockchain. The smart contract features of blockchain enable such dynamic and autonomous decision-making, ensuring secured data storage and the reliability of such frameworks.
2. *Trustworthiness of IoUT smart devices*—With the substantial growth of IoT technology, more and more sensor devices are introduced, which are used for building the data communication network. Similar to the IoT, the IoUT also has several smart devices embedded with sensors, which are developed and utilized for data communication in the UWSN. The data generated from these UWSN devices may be very sensitive for critical applications such as defense [67]. The consensus algorithm is the decision-making process for the group of active nodes in the communication network while building trustworthy transactions in blockchain.
3. *Availability of the data in the IoUT*—Blockchain [68] uses the fault-tolerant mechanism, building an effective network for the availability of data transmitted through the IoUT devices. The decentralized and distributed structure of blockchain is a very important feature to confirm the availability of data perpetually. This property of blockchain is vital for making the data available to oceanographers to conduct their research analysis and investigations at their convenience [69]. The decentralized system stores

the information spread across the globe so that there is no single point of failure. This is achieved by storing the blockchain data over millions of devices on the distributed network of nodes; hence, the data and network are highly resistant to any malicious attack or technical failure in the network. Because of this, the availability of data in the blockchain-enabled IoUT communication network is possible.

4. *Privacy of the data in the IoUT*—Attackers cannot misuse or obtain the data, as the users can control their data with the private and public keys in a blockchain transaction, thereby enabling data ownership. The data owners can control when, how, and to what extent a third party can access the data. The privacy of data generated from IoUT devices can thus be preserved with blockchain technology.

Furthermore, with the substantial magnification of underwater marine technology, the fusion of blockchain with the IoUT leads the way to explore the world's underlying water resources and can be best used for the benefit of humans and marine life. The motivation behind the integration of blockchain with the IoUT is depicted in Figure 4. In the following section, the notable applications of the IoUT are analyzed, discussing the role of the IoUT and its significance.

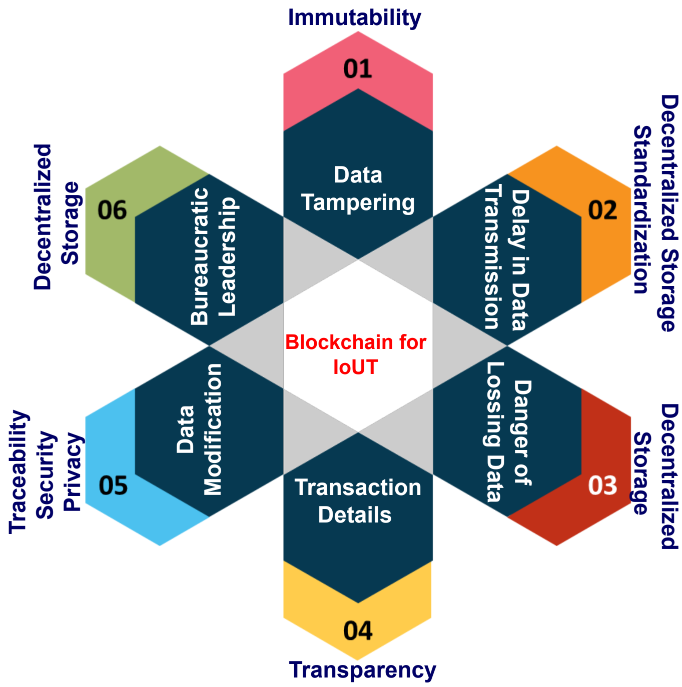

Figure 4. Integration of blockchain in the IoUT.

3. Applications

This section focuses on the exploration of recent advances in the IoUT and how blockchain [70–72] can help improve the existing practices for underwater applications in distrusted environments.

3.1. Environmental Monitoring

Rapid urbanization and the development of industries have become an integral part of human growth. Due to this, water contamination and water deterioration have become alarmingly prevalent. Conventional water monitoring methods are lengthy, expensive, inefficient, and insecure, wherein manual testing is performed in laboratories. The monitoring of water quality involves the role of IoUT sensors in transmitting data as sound variations. The acoustic signals that are used for underwater communication consume high propagation delays and high error rates. In addition, sensors are deployed in an antagonistic environment, which remain unattended, making underwater communication more vulnerable to outside attacks. In order to secure sensors from being subjected to such attacks, the authors in [73] proposed a blockchain-based multi-layer hierarchical architecture. This architecture simplified the monitoring and managing process of the IoUT data. Based on the residual energy cluster heads, sensor nodes were clustered and organized. The tracking of nodes and cluster heads was performed by a bloom filter, and two keys were used for communication. The standard secret key was used for the gateways to communicate, and a special secret key was enabled for cluster heads to communicate. Furthermore, the blockchain ledger helped store the routed data. The lightweight blockchain framework in [73] helped provide the legitimacy of data sources. The sensors deployed underwater for quality monitoring are prone to attacks, and there is the possibility for information leakage to occur. This is primarily due to the lack of security features in the underwater environment. A multi-layer hierarchical architecture proposed by the authors offers security to the IoUT nodes. The system significantly helps in protecting the sensors deployed underwater, securing the data transmission and organizing the networks in the underwater environment.

The IoT is a category of pervasive systems that utilize embedded sensors, applications, and networks in smart systems and environments. The IoUT is one of the specific types of IoT systems that relies on underwater sensors in order to consume ocean information in the context of smart oceans. The oceanic information obtained from the group of sensors is very useful to carry out analyses such as water quality monitoring, marine ecosystem monitoring, water pollution monitoring, and so on. Hence, it is critical to create and provide a platform that allows the users to efficiently share and store the IoUT data in ad hoc unsecured environments. To provide distributed access to the users, the authors in [74] suggested the use of blockchain technology. The Ethereum smart contract mechanism can be used to share the IoUT data obtained from the oceanic environment. This smart contract mechanism helps in providing easier access to the users in order to store and manage access roles for the IoUT data. The suggested solution encrypts the IoUT data sent to the interplanetary file system and stores the hash values generated in the blockchain ledger. Sharing the valuable oceanic data over an unsecured ad hoc platform can question the trust and security aspects of the system. The Ethereum smart contract mechanism can be used in such cases to provide better security for sharing the IoUT data to perform various research analysis.

A smart ocean requires various properties of the ocean to be explored exhaustively ensuring thorough understanding. The IoUT demands powerful technologies for creating a smart ocean. A detailed review of current advancements, future communication architectures, challenges, applications, and issues that need immediate attention were discussed by the authors in [75]. IoUT frameworks face similar security and standardization issues as in the case of the IoT. There exists no common standard for the regularization of communication and transmission between underwater devices. In addition, it is also equally important to design an intelligent security system for ensuring normal data transmission between underwater devices. Due to the prevailing complexities in IoT systems, which consist of different networks, the involvement of billions of underwater intelligent objects is inevitable. Additionally, it is essential to guarantee the security and privacy of users in the IoUT. Any IoUT layer may face a threat from malicious attacks from outside, which have the potential to collapse the entire network. The blockchain security features such as the distributed ledger and consensus-based approval can be used to protect smart ocean communication. The smart ocean systems are largely applicable to ocean activities that are closely related to human beings. These activities include ocean pollution monitoring, ocean deep range monitoring, underwater navigation, resource exploration, underwater tourism, disaster management, and various others. These activities help people to understand the ocean to the fullest, utilize the ocean's resources, and secure the ocean more efficiently, enabling enhanced services to be rendered to mankind. To ensure secure transmission of data across multiple networks in an underwater environment, blockchain-based solutions can be used.

3.2. Disaster Management

Emergency handlers handle disasters as recurring events. Disasters are likely to happen every single year, resulting in a follow-up process. The emergency handlers handle a disaster in four phases: preparedness, response, mitigation, and recovery. Disasters happening in water bodies are highly dangerous. This may lead to the loss of human lives and other living organisms in the water [76]. IoUT applications play an important role in all four phases of such emergencies. The IoUT has the ability to sense locations in underwater circumstances. It can process the data locally and transmit the same to the base station via an underwater communication facility available in the IoUT [77]. Seismic sensors can be deployed underwater to detect ground motion when it is shaken by any perturbation. The information received from the underwater sensors should be reliable enough for further analysis and mitigation activities. All course of actions in a disaster rely on the information communicated by the sensor. The IoUT uses acoustic signals for underwater communication. In natural environments and circumstances, the sound emitted becomes affected by the underwater temperature, the density of vegetation, humidity, and various other sounds emitted by living organisms underwater. Besides the above factors, human-involved activities such as industrialization and sounds from ships can also affect the signal. This results in the failure of communication or the failure in anticipating a disaster. Hence, this communication needs to be secured enough wherein the information communicated by the devices reaches the base station on time without unwanted modification. Some factors relevant to acoustic communication were addressed in [78]. Blockchain technology can be used in this regard to protect underwater acoustic communication. Due to the complexity of computation and the underwater scenario, the authors in [79] suggested the use of basic blockchain functions such as adding blocks, block validations, and the implementation of the longest chain rule. Each chain created with blockchain consists of a ledger system to store the information. The ledger is an append-only block structure, which does not allow anyone to remove or modify the block, once it is added to the chain. Through blockchain, communication underwater can be made reliable and instant actions can be taken to prevent disasters. The integrity of information generated by the underwater sensors can thus be preserved using the blockchain-based solutions. This will further aid in taking the right course of action by predicting the disasters that can occur in the oceanic environment.

3.3. Localization

Positioning of underwater devices and other data sources is a key requirement for any location-based underwater application. As the parameters of terrestrial and underwater environments differ in various aspects, the systems adopted for the localization of terrestrial objects may not scale well to fit the needs of underwater systems. Extensive research has been carried out in the field of the localization of underwater objects. A detailed review on various localization schemes for the IoUT were discussed by the authors in [80–82]. The stratification effect and the mobility characteristics make the localization of underwater sensor nodes an even more challenging task to achieve. Apart from these, security and privacy are the key challenges associated with the localization of underwater nodes, especially due to the harsh environmental conditions. As most of the localization schemes are designed for suitable environments, there is the possibility of privacy violations, which may lead to serious consequences, especially in mission-critical applications. The authors in [83] explained the privacy and security concerns with respect to localization in underwater environments. However, very minimal research activities have been actively carried out for dealing with the privacy concerns in the localization of underwater sensor nodes.

The blockchain can be regarded as an effective solution for dealing with the privacy aspects related to localization in underwater environments due to its unique characteristics such as decentralization, consensus, and security. Third party participation can be completely removed if blockchain technology can be integrated with the IoUT. This enables data to be stored securely without requiring any intermediate authority. The data generated from IoUT devices can be processed and validated with the help of blockchain mechanisms. The data privacy issues pertaining to the positioning of underwater devices can be solved efficiently with the help of blockchain technology. The decentralization, consensus, and security aspects of blockchain primarily ensure that the privacy of data is not questioned. This enables location-based applications to adopt blockchain in the existing system. The flip side of applying blockchain in underwater sensor networks is its never-ending demand for power, memory, and computation [84]. The blockchain can be successfully integrated with the IoUT only if the underwater sensor nodes are capable of providing the above said aspects at a low cost. However, many researchers have channelized their efforts in this regard to enforce privacy in the IoUT with the help of machine-learning- [85], deep-learning-, and reinforcement-learning-based systems.

A "multilevel sensor monitoring" architecture was proposed by [73], wherein a layer-based system was implemented for storing and processing data from the IoUT using blockchain technology. A lightweight consensus mechanism was also adopted in this work to process various transactions in an efficient manner. Additionally, the lightweight protocols help in transferring the data to the concerned system. Such an architecture can be efficiently implemented for the localization of underwater devices due to its lightweight protocols and consensus mechanism. "BCTrust" is a blockchain-based authentication mechanism proposed by [86] that is robust, secure, energy efficient, and transparent. This mechanism can be ideally used for systems with storage, energy, and computational constraints. This system can be extended to work with the localization aspects in the IoUT, as it can provide privacy and deals with the harsh underwater environments. The integration of blockchain with the IoUT significantly helps in the localization of various entities associated with the IoUT in a privacy-preserving manner. This is an open research area where the adoption of lightweight technologies has great potential to enhance the current blockchain-based IoUT systems.

3.4. Defense

Naval defense exercise operations include surveillance, mine detection, sub-marine detection, and recovery operations. Underwater Autonomous Vehicles (UAVs) are programmable, self-propelled, and unmanned, capable of carrying out assigned tasks with little or no real-time input from humans [87]. Torpedoes are the first form of UAV used in naval defense systems [88]. Recent research and development witnessed marvelous growth in making these vehicles significant for naval defense applications. It is inevitable to extend the idea of the IoT for underwater things. The IoUT has significantly altered the way the data are collected and stored and the way intelligent decisions are derived from the same. The issues related to data privacy and security in navy-based defense activities are mostly because of the centralized architecture of the IoUT systems used for data storage. Here, data tampering may occur during data transmission between the nodes. Hence, the concept of the immutability and traceability of blockchain can address the aforementioned issues.

Naval defense is one such sector that has enthusiastically adopted the advantages of the IoUT. The IoUT is an interconnected system of computing devices that helps to improve the productivity and efficiency of the data communicated among the water-based vehicles such as ships, submarines, drones, and other water vessels. The current IoUT ecosystem is expensive as it employs large servers to store the data in a centralized manner. Securing the data source is an extremely necessary requirement, since important decisions are obtained from the intelligent devices and stored in a common cloud. The data in the IoUT environment can be accessed and modified by the participating nodes, and the origin of the tampered data may be unknown. Additionally, the current IoUT control systems reduce the data transmission speed, leading to bureaucratic leadership among the nodes. There is also the associated risk of losing the data if there is no recovery mechanisms in place in case of system failures. Communication from remote areas between the IoUT and UAV facilitates vulnerability threats, wherein cyber criminals obtain unauthorized access to connected networks and devices, thereby exposing critical data. The distributed communication nature of the ocean network enables unauthorized users to access data and information by following unethical practices. The centralized architecture of the IoUT in such cases is insufficient in providing secured and efficient IoUT solutions. Blockchain is an advanced technology, which is used for securing and tracking real-time applications and their data. It is a promising technology that leverages the information sharing and accessing process. The authors in [89] emphasized the aspect of data exchange among the participating nodes in the Internet environment, ensuring the same to be secured and immutable. In the blockchain-enabled IoUT environment, the decentralized structure of blockchain is used, wherein all participating nodes share a copy of the transaction, and hence, transparency is maintained. Additionally, the cryptography features such as hashing, digital signatures, and public–private keys enable the data block to securely link with other blocks and, thus, ensures the immutability of the data. Another important aspect of underwater communications in defense is traceability. Each device or vehicle in the network is associated with an ID, which enables the user to track the transactions and generate smart contracts. Smart contracts are shared among various devices and sub-systems in the application. Each task in the system executes its operations using the smart contracts. The advantages of the blockchain-integrated IoUT is manifold in defense applications in oceans.

3.5. Underwater Exploration

Underwater exploration is an interesting and challenging use case that helps in managing, conserving, regulating, and using the ocean resources that are particularly significant for a nation's economy and the citizens' well-being [90]. According to the World Bank, the blue economy is the "sustainable use of ocean resources for economic growth, improved livelihoods, and jobs while preserving the health of ocean ecosystem" [91]. Underwater exploration mainly deals with the discovery of lost treasures and natural resources. Managing the ocean resources in a sustainable manner is crucial for a nation, as these resources are to be around for the successive generations as well. Based on [92], nearly 14 percent of the U.S. near the coast generates 45 percent of the nation's total GDP. "NOAA Ocean Exploration" is the only federal program by the U.S. dedicated to exploring the unknown or poorly known areas of the deep ocean [93]. Matsya 6000 is a part of India's "Deep Ocean Mission" to discover rare minerals. This is a submersible vehicle under development that can go up to a depth of 6000 m [94]. Similarly, various nations are conducting research on exploring the underwater resources. However, underwater exploration poses several challenges with respect to the nation's security aspects as well. Hence, the data generated and collected should be secure and transparent.

Blockchain technology can be integrated with the IoUT, thus enabling the exploration of underwater resources in a secure, transparent, and traceable manner. The immutability characteristic of blockchain primarily ensures that the data, once uploaded cannot, be tampered with. This particularly helps in guaranteeing that the explored underwater resources are not being misused. PO8 is a blockchain group in The Bahamas that focuses on integrating blockchain, artificial intelligence, and robotics to explore the treasures and tokenize them with NFTs on the Ethereum blockchain [95]. "Non-Fungible Investment Vehicles (NFIVs)" are also created, which provide monetary benefits by generating earnings. The traceability and transparency characteristics of blockchain make it an optimal choice even for tuna traceability. Illegal and unreported fishing can be alleviated to a great extent with the help of blockchain technology. The authors in [96] proposed a cryptographic protocol named "DeepOcean", which uses the "blockchain-agnostic dark pool" for cryptocurrencies. Here, different parties can agree for trade without the need of knowing about their order sizes in advance. The existing underwater technologies can be combined with blockchain for effective underwater exploration. A detailed review of the different sensing technologies for underwater exploration was carried out by [97]. Essential ocean variables were also detailed in the review. The authors in [98] presented a preliminary design of a robotic system for autonomous underwater vehicles. Such frameworks have the ability to be adjusted according to the different environments and can help in the durability of the devices. Even though underwater exploration contributes to the nations' economy on a large scale, the research on the integration of booming technologies such as blockchain for the IoUT is still at its infancy. Figure 5 depicts the use cases of the blockchain-enabled IoUT. Table 2 summarizes the applications of the IoUT, the motivation for IoUT applications to integrate with blockchain, and their associated challenges.

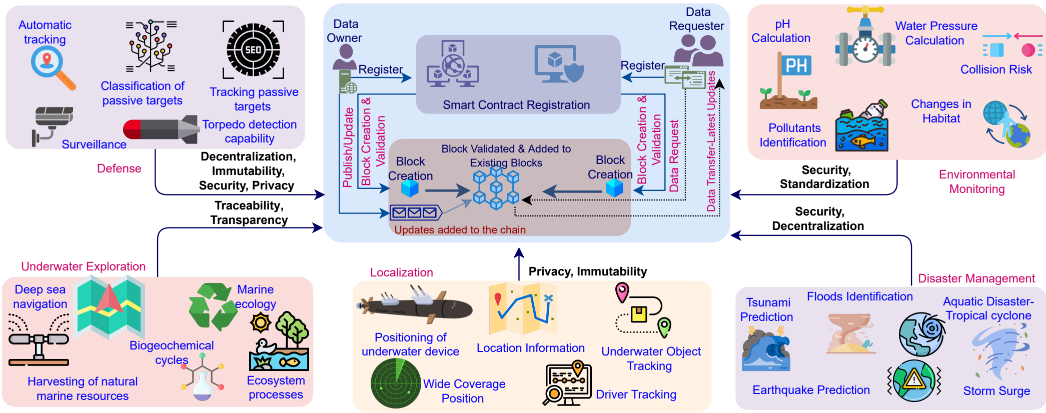

Figure 5. Use cases of the blockchain-enabled IoUT

Table 2. Summary of the applications of and motivations for blockchain for the IoUT and the challenges.

Application	Motivation for Using Blockchain for the IoUT	Challenges of Blockchain–IoUT Integration
Environmental Monitoring	-To provide authenticated and distributed access to the users of the data collected -To guarantee the security and privacy of nodes participating in underwater communication	-Deployment Cost
Disaster Management	-To make a reliable and secure acoustic communication underwater	-Energy Consumption -Computation Complexity
Localization	-To ensure the privacy of location information -To share the massive amount of data collected in a secured manner -Only the participating nodes can view the location -To avoid data tampering, the immutability of blockchain can help	-High demand for power -Memory and computational capacity
Defense	-Securing the data source -To secure the communication between the participating nodes -To validate the transactions	-Migrating from legacy systems -Scalability
Underwater Exploration	-To ensure the transparency of the information collected and shared -To ensure traceability by providing a fully auditable and valid ledger of transactions -To share the data in a secure manner	-Scalability issues -Ocean governance

4. Challenges and Future Directions

The blockchain-integrated IoUT ensures security, consensus, traceability, privacy, and transparency, which makes it a possible solution to many of the challenges faced in an underwater environment. However, integrating blockchain in such a resource-constrained environment indeed poses certain challenges as mentioned below.

4.1. Computing Power

The diverse IoUT ecosystem comprises various devices with different computing capabilities. One of the major reasons for the integration of blockchain with the IoUT is due to the security it offers. The consensus mechanism in blockchain enables no third party involvements, thereby improving the security to a great extent. However, the blockchain–IoUT integration requires a high computational cost in order to make the PoW consensus algorithm work. This requires the miners to use computing systems with very high computational power. As most of the IoUT devices have low computational power, consensus algorithms such as PoW may be difficult to deploy. Hence, lightweight mechanisms such as the one proposed by [73] are required. Another possible solution would be to include devices with high computational power in the IoUT ecosystem.

4.2. Storage Capacity

The adoption of blockchain in the IoUT eliminates the need for a central server to handle the transactions and device data. However, the ledger needs to be stored in the IoUT nodes themselves. The number of such ledgers can increase over time and become quite challenging to handle. IoUT devices usually have very low storage space. The comparatively lower disk space and memory of IoUT devices and network connectivity issues are some of the key factors affecting the adoption of blockchain technology in an IoUT environment. Most of the current blockchain implementations can handle only a few transactions per second. This would be another bottleneck in the case of an IoUT environment. However, the data generated from IoUT sensors are very huge, making it really difficult to handle such big data. The integration of the IoUT with a decentralized and public blockchain is quite hard and should be dealt with considering the increasing data storage requirements. One of the possible solutions includes leveraging cloud resources. The authors in [99] proposed an "advanced time-variant multi-objective particle swarm optimization algorithm" for the integration of the IoT and blockchain. However, such techniques can be enhanced and used for the integration of the IoUT and blockchain.

4.3. Scalability

One of the notable challenges in deploying the blockchain in the IoUT environment is scalability. The IoUT is very large and will become far larger in the future as the number of underwater objects grows. The goal of the IoUT is to create a worldwide network of interconnected underwater objects and to digitally link to on-shore, off-shore, and underwater elements. There will be numerous transactions generated from the IoUT ecosystem. The blockchain limits the capability of scaling as the network size and transaction volume increase. The blockchain uses a consensus protocol, which enables the users to record irreversible, time-stamped transactions and prevents the creation of false records [100]. The consensus mechanism accommodates all the participants in the network to agree on the transaction and limit the number of transactions. The typical consensus algorithms such as the PoW and Proof of Stack (PoS) require a common transaction to be confirmed by the participating nodes in the blockchain ecosystem. This slows down the transaction validation process. In [101], the authors proposed an approach where users with permission can join, execute, and validate transactions and that does not require much to validate a transaction.

4.4. Standardization and Governance

Standardization is a critical aspect in the blockchain-enabled IoUT systems. The lack of proper standardization and strict governance results in various regulatory challenges in terms of decentralization, anonymity, and immutability. Strict policies are required in terms of the sustainable use of oceans. Ocean governance, therefore, needs to be considered as an important aspect regionally and globally. The authors in [102] addressed how sustainable ocean governance can be implemented by the authorities. Three significant risk factors were addressed in their work: (i) the effect of the over-exploitation of resources, (ii) non-equitable service distribution, and (iii) inadequate adaptation to the ever-changing environmental conditions. A framework that deals with the "equity" aspects in ocean governance was put forward by [103]. The dimensions of social equity in the framework considered include "where", "why", "whom", "what", "when", and "how". The integration of the blockchain with the IoUT also requires effective standardization and policies, thus enabling a fool-proof method of exploring and exploiting the resources.

4.5. Migration from Legacy Systems

The old-fashioned legacy systems that are being used at present in the underwater environment are more vulnerable to data modification and thefts. The applications of underwater things benefit from implementing the blockchain as a solution that adapts DLT. The amalgamation of the IoUT and blockchain projects tends to be complex since both involve niche skills. Finding appropriately skilled developers for implementing blockchain technology in an organization is hard [104]. The governance structure of the blockchain in the IoUT defines the participants, data ownership, exit and entry criteria, and conditions for information sharing among the participants. The tools required for building the blockchain ecosystem are currently in progress. This compounds the complexity of integrating the technology with the existing systems. Migrating from older systems is expensive as the application has to rely heavily on the experts to handle the problems that occur in the initial stages of deployment, thus making it a time-consuming process.

4.6. Energy Consumption

Energy consumption in a blockchain-implemented IoUT network is different when compared to terrestrial environments. Both of these technologies consume enormous energy for providing their specific services [105]. In the IoUT, all deployed underwater sensors communicate to the central sink sensor for delivering the information that is gathered from different devices. All successfully established IoT networks have faced various challenges when deployed underwater. This includes short-range communication, high attenuation, enormous ultra-violet radiation, the high expense for sensor deployment, and so on. In addition, the underwater environment has its unique characteristics. The terrestrial signal cannot be used for underwater communication. Instead, acoustic signals are preferred. Providing efficient underwater communication through acoustic signals is a challenging task because the signals suffer from high attenuation, long propagation delays, and high bit rates. Due to this, more communication failures may occur between sensors, which can lead to an increased number of data re-transmissions. An IoUT sensor has limited power, and it is not so easy to recharge or replace the battery in the IoUT. Extensive research has been performed to solve the blockchain energy issues, but, still, it remains as a key challenge. When the blockchain services are implemented with the IoUT network, each service requires high energy per transaction. Long delays can also occur before the transaction becomes confirmed. Therefore, the energy consumption of blockchain-enabled IoUT networks is a complex research problem that needs more attention from the research community.

4.7. Cost

The deployment of communication sensors in the underwater environment is a challenging issue. In addition, installation, managing, and maintaining those communication devices are much more complicated processes when compared with terrestrial networks. Moreover, underwater sensors can be easily damaged or lost or become non-functional during the digging process or due to the harsh underwater environments. Therefore, efficient installation of sensors is required, which can reduce the work of re-installation and maintenance. For instance, a communication sensor that demands more energy should be deployed near the surface or near the power source for the ease of management, and also to reduce the cost of deployment. In addition, to avoid the frequent battery failures of the sensors, efficient power-saving protocols can be used for communication.

Table 3 summarizes the challenges of the blockchain-enabled IoUT.

Table 3. Challenges of the blockchain-enabled IoUT.

Sl. No.	Challenge Type	Description	Possible Solutions
1	Computing Power	High computational power is required for the consensus algorithms to work	Lightweight mechanisms need to be introduced; devices with high computational power need to be used
2	Storage Capacity	To handle a larger number of transactions per second and to store ledgers, high storage capacity is required	Use cloud resources
3	Scalability	Scalable solutions are required to accommodate the huge number of transactions	Transactions to be carried out among subnetworks
4	Standardization and Governance	To avoid the over-exploitation of resources and non-equitable service distribution, proper standardization is required	Proper standards are to be formulated; ocean governance needs to be considered regionally, nationally, and globally
5	Migration from legacy systems	Migration from the traditional systems and technologies to adopt blockchain-enabled solutions is expensive and time-consuming	Rigorous training is essential
6	Energy consumption	Acoustic communication demands more energy. Underwater communication suffers high attenuation, long propagation delays, and high bit rates; in addition, the blockchain adaption consumes high energy for successful transactions.	A lightweight energy-efficient blockchain-based framework for IoUT acoustic communication can be used to solve this
7	Cost	Installing, managing, and maintaining the communication devices underwater is a challenging task. Frequent maintenance may be required such as battery change, sensor servicing, and so on	(1) Power-saving protocols can be used to reduce power use and also to avoid battery failures; (2) horizontal axis and vertical axis deployment strategies can be used to reduce the complexity of the network

5. Conclusions

Blockchain can be regarded as the future of the Internet, which has the potential to change the way the current economic and social systems work. The unique characteristics of blockchain help in asset protection, the adoption of cryptocurrency, smart contracts, voting, and so on. This proves to be advantageous in the IoUT ecosystem as well. Even though IoUT communication systems have proven to be beneficial for various systems, ranging from small observatories to harbors to oceans, they pose several challenges. This paper introduced the background related to the IoUT and blockchain and explained how such an integration would help address the challenges in the current IoUT ecosystem. An exhaustive survey was then carried out on the various blockchain-enabled IoUT applications, and we pointed out the benefits of each. Finally, the open issues and challenges in blockchain–IoUT integration were critically analyzed, and the possible solutions were presented.

Author Contributions: Conceptualization, S.B., N.V. and R.C.; methodology, R.C., N.V. and M.R.; software, M.R., G.C.S.; validation, S.D. and P.K.R.M.; formal analysis, P.K.D.; investigation, S.D., R.H.J. and T.R.G.; resources, T.R.G.; data curation, writing—review and editing, S.D., P.K.R.M., S.B. and N.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding

Institutional Review Board Statement: Not applicable

Informed Consent Statement: Not applicable

Data Availability Statement: Not applicable

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Cooley, S.W.; Ryan, J.C.; Smith, L.C. Human alteration of global surface water storage variability. *Nature* **2021**, *591*, 78–81. [CrossRef] [PubMed]
2. Yap, W.; Switzer, A.D.; Gouramanis, C.; Marzinelli, E.; Wijaya, W.; Yan, Y.T.; Dominey-Howes, D.; Labbate, M.; Srinivasalu, S.; Jankaew, K.; et al. Environmental DNA signatures distinguish between tsunami and storm deposition in overwash sand. *Commun. Earth Environ.* **2021**, *2*, 129. [CrossRef]
3. Singh, V.K.; Roxy, M. A review of ocean-atmosphere interactions during tropical cyclones in the north Indian Ocean. *Earth-Sci. Rev.* **2022**, *226*, 103967. [CrossRef]
4. Zhou, R.; Meng, Z.; Bai, L. Differences in tornado activities and key tornadic environments between China and the United States. *Int. J. Climatol.* **2022**, *42*, 367–384. [CrossRef]
5. Zhang, Z.; Huang, J.; Cao, S. Marine cold chain transportation monitoring and route scheduling optimization based on IoV-BDS. *IEEE Access* **2021**, *9*, 20557–20574. [CrossRef]
6. Ertör, I. 'We are the oceans, we are the people!': Fisher people's struggles for blue justice. In *The Journal of Peasant Studies*; Taylor&Francis: Boca Raton, FL, USA, 2021; pp. 1–30.
7. Kadagi, N.I.; Wambiji, N.; Fennessy, S.T.; Allen, M.S.; Ahrens, R.N. Challenges and opportunities for sustainable development and management of marine recreational and sport fisheries in the Western Indian Ocean. *Mar. Policy* **2021**, *124*, 104351. [CrossRef]
8. Leal Filho, W.; Abubakar, I.R.; Nunes, C.; Platje, J.J.; Ozuyar, P.G.; Will, M.; Nagy, G.J.; Al-Amin, A.Q.; Hunt, J.D.; Li, C. Deep seabed mining: A note on some potentials and risks to the sustainable mineral extraction from the oceans. *J. Mar. Sci. Eng.* **2021**, *9*, 521. [CrossRef]
9. Radeta, M.; Zuniga, A.; Motlagh, N.H.; Liyanage, M.; Freitas, R.; Youssef, M.; Tarkoma, S.; Flores, H.; Nurmi, P. Deep learning and the oceans. *Computer* **2022**, *55*, 39–50. [CrossRef]
10. Samir, M.; Elhattab, M.; Assi, C.; Sharafeddine, S.; Ghrayeb, A. Optimizing age of information through aerial reconfigurable intelligent surfaces: A deep reinforcement learning approach. *IEEE Trans. Veh. Technol.* **2021**, *70*, 3978–3983. [CrossRef]
11. Vo, D.T.; Nguyen, X.P.; Nguyen, T.D.; Hidayat, R.; Huynh, T.T.; Nguyen, D.T. A review on the internet of thing (IoT) technologies in controlling ocean environment. In *Energy Sources, Part A: Recovery, Utilization, and Environmental Effects*; Taylor&Francis: Boca Raton, FL, USA, 2021; pp. 1–19. [CrossRef]
12. Reddy, T.; RM, S.P.; Parimala, M.; Chowdhary, C.L.; Hakak, S.; Khan, W.Z. A deep neural networks based model for uninterrupted marine environment monitoring. *Comput. Commun.* **2020**, *157*, 64–75.
13. Reddy Maddikunta, P.K.; Srivastava, G.; Reddy Gadekallu, T.; Deepa, N.; Boopathy, P. Predictive model for battery life in IoT networks. *IET Intell. Transp. Syst.* **2020**, *14*, 1388–1395. [CrossRef]
14. Yazdinejad, A.; Parizi, R.M.; Srivastava, G.; Dehghantanha, A.; Choo, K.K.R. Energy efficient decentralized authentication in internet of underwater things using blockchain. In Proceedings of the 2019 IEEE Globecom Workshops (GC Wkshps), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6.
15. Zhou, Z.; Gupta, B.B.; Gaurav, A.; Li, Y.; Lytras, M.D.; Nedjah, N. An Efficient and Secure Identity-Based Signature System for Underwater Green Transport System. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 16161–16169. [CrossRef]
16. Mohsan, S.A.H.; Mazinani, A.; Othman, N.Q.H.; Amjad, H. Towards the internet of underwater things: A comprehensive survey. *Earth Sci. Inform.* **2022**, *15*, 735–764. [CrossRef]
17. Falkowski, P. Ocean science: The power of plankton. *Nature* **2012**, *483*, S17–S20. [CrossRef]
18. Domingo, M.C. An overview of the internet of underwater things. *J. Netw. Comput. Appl.* **2012**, *35*, 1879–1890. [CrossRef]
19. Jahanbakht, M.; Xiang, W.; Hanzo, L.; Azghadi, M.R. Internet of underwater things and big marine data analytics—A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 904–956. [CrossRef]
20. Saab, S.; Fu, Y.; Ray, A.; Hauser, M. A Dynamically Stabilized Recurrent Neural Network. *Neural Process. Lett.* **2022**, *54*, 1195–1209. [CrossRef]
21. Kesrai, M.D.R.; Lee, J.; Ko, E.; Shin, S.Y.; Namgung, J.I.; Yum, S.H.; Park, S.H. Underwater network management system in internet of underwater things: Open challenges, benefits, and feasible solution. *Electronics* **2020**, *9*, 1142.
22. Alazab, M.; Tang, M. *Deep Learning Applications for Cyber Security*; Springer: Berlin/Heidelberg, Germany, 2019.
23. Yisa, A.G.; Dargahi, T.; Belguith, S.; Hammoudeh, M. Security challenges of internet of underwater things: A systematic literature review. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4203. [CrossRef]
24. Bello, O.; Zeadally, S. Internet of underwater things communication: Architecture, technologies, research challenges and future opportunities. *Ad Hoc Netw.* **2022**, *135*, 102933. [CrossRef]
25. Salami, A.F.; Dogo, E.M.; Makaba, T.; Adedokun, E.A.; Muazu, M.B.; Sadiq, B.O.; Salawudeen, A.T. A decade bibliometric analysis of underwater sensor network research on the Internet of Underwater Things: An African perspective. In *Trends Cloud-Based IoT*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 147–182. [CrossRef]
26. Ghafoor, H.; Noh, Y. An overview of next-generation underwater target detection and tracking: An integrated underwater architecture. *IEEE Access* **2019**, *7*, 98841–98853. [CrossRef]
27. Mary, D.R.K.; Ko, E.; Kim, S.G.; Yum, S.H.; Shin, S.Y.; Park, S.H. A Systematic Review on Recent Trends, Challenges, Privacy and Security Issues of Underwater Internet of Things. *Sensors* **2021**, *21*, 8262. [CrossRef] [PubMed]
28. Feng, Q.; He, D.; Zeadally, S.; Khan, M.K.; Kumar, N. A survey on privacy protection in blockchain system. *J. Netw. Comput. Appl.* **2019**, *126*, 45–58. [CrossRef]

29. Arafeh, M.; El Barachi, M.; Mourad, A.; Belqasmi, F. A blockchain based architecture for the detection of fake sensing in mobile crowdsensing. In Proceedings of the 2019 4th International Conference on Smart and Sustainable Technologies (SpliTech), Bol/Split, Croatia, 18–21 June 2019; pp. 1–6.
30. Murray, M. Tutorial: A descriptive introduction to the Blockchain. *Commun. Assoc. Inf. Syst.* **2019**, *45*, 25. [CrossRef]
31. Dustdar, S.; Fernández, P.; García, J.M.; Ruiz-Cortés, A. Elastic smart contracts in blockchains. *IEEE/CAA J. Autom. Sin.* **2021**, *8*, 1901–1912. [CrossRef]
32. ur Rehman, M.H.; Salah, K.; Damiani, E.; Svetinovic, D. Trust in blockchain cryptocurrency ecosystem. *IEEE Trans. Eng. Manag.* **2019**, *67*, 1196–1212. [CrossRef]
33. Lo, S.K.; Xu, X.; Chiam, Y.K.; Lu, Q. Evaluating Suitability of Applying Blockchain. In Proceedings of the 2017 22nd International Conference on Engineering of Complex Computer Systems (ICECCS), Fukuoka, Japan, 6–8 November 2017; pp. 158–161. [CrossRef]
34. Cucari, N.; Lagasio, V.; Lia, G.; Torriero, C. The impact of blockchain in banking processes: The Interbank Spunta case study. *Technol. Anal. Strateg. Manag.* **2022**, *34*, 138–150. [CrossRef]
35. Boakye, E.A.; Zhao, H.; Ahia, B.N.K. Emerging research on blockchain technology in finance; a conveyed evidence of bibliometric-based evaluations. *J. High Technol. Manag. Res.* **2022**, *33*, 100437. [CrossRef]
36. Sangari, M.S.; Mashatan, A. A data-driven, comparative review of the academic literature and news media on blockchain-enabled supply chain management: Trends, gaps, and research needs. *Comput. Ind.* **2022**, *143*, 103769. [CrossRef]
37. Keresztes, É.R.; Kovács, I.; Horváth, A.; Zimányi, K. Exploratory analysis of blockchain platforms in supply chain management. *Economies* **2022**, *10*, 206. [CrossRef]
38. Adere, E.M. Blockchain in healthcare and IoT: A systematic literature review. *Array* **2022**, *14*, 100139. [CrossRef]
39. Prybutok, V.R.; Sauser, B. Theoretical and practical applications of blockchain in healthcare information management. *Inf. Manag.* **2022**, *59*, 103649.
40. Abdelmaboud, A.; Ahmed, A.I.A.; Abaker, M.; Eisa, T.A.E.; Albasheer, H.; Ghorashi, S.A.; Karim, F.K. Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions. *Electronics* **2022**, *11*, 630. [CrossRef]
41. Pal, S.; Dorri, A.; Jurdak, R. Blockchain for IoT access control: Recent trends and future research directions. *J. Netw. Comput. Appl.* **2022**, *203*, 103371. [CrossRef]
42. Dehury, C.; Srirama, S.N.; Donta, P.K.; Dustdar, S. Securing clustered edge intelligence with blockchain. *IEEE Consum. Electron. Mag.* **2022**, *1*. [CrossRef]
43. Chen, Y.; Lu, Y.; Bulysheva, L.; Kataev, M.Y. Applications of blockchain in industry 4.0: A review. In *Information Systems Frontiers*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 1–15. [CrossRef]
44. Bamakan, S.M.H.; Malekinejad, P.; Ziaeian, M. Towards blockchain-based hospital waste management systems; applications and future trends. *J. Clean. Prod.* **2022**, *349*, 131440. [CrossRef]
45. Lemos, C.; Ramos, R.F.; Moro, S.; Oliveira, P.M. Stick or Twist—The Rise of Blockchain Applications in Marketing Management. *Sustainability* **2022**, *14*, 4172. [CrossRef]
46. Mendling, J.; Weber, I.; Aalst, W.V.D.; Brocke, J.V.; Cabanillas, C.; Daniel, F.; Debois, S.; Ciccio, C.D.; Dumas, M.; Dustdar, S.; et al. Blockchains for business process management-challenges and opportunities. *ACM Trans. Manag. Inf. Syst. (TMIS)* **2018**, *9*, 1–16. [CrossRef]
47. Dustdar, S.; Fernández Montes, P.; García Rodríguez, J.M.; Ruiz Cortés, A. Elastic Smart Contracts across Multiple Blockchains. In *Proceedings of the FAB 2019: Second International Symposium on Foundations and Applications of Blockchain*; University of Southern California: Los Angeles, CA, USA, 2019; pp. 28–34.
48. Jayabalasamy, G.; Koppu, S. High-performance Edwards curve aggregate signature (HECAS) for nonrepudiation in IoT-based applications built on the blockchain ecosystem. In *Journal of King Saud University-Computer and Information Sciences*; Elsevier: Amsterdam, The Netherlands, 2021. [CrossRef]
49. Guo, H.; Yu, X. A Survey on Blockchain Technology and its security. *Blockchain Res. Appl.* **2022**, *3*, 100067. [CrossRef]
50. Xu, X.; Dilum Bandara, H.; Lu, Q.; Weber, I.; Bass, L.; Zhu, L. A Decision Model for Choosing Patterns in Blockchain-Based Applications. In Proceedings of the 2021 IEEE 18th International Conference on Software Architecture (ICSA), Stuttgart, Germany, 22–26 March 2021; pp. 47–57. [CrossRef]
51. Almeshal, T.A.; Alhogail, A.A. Blockchain for Businesses: A Scoping Review of Suitability Evaluations Frameworks. *IEEE Access* **2021**, *9*, 155425–155442. [CrossRef]
52. Hewa, T.M.; Hu, Y.; Liyanage, M.; Kanhare, S.S.; Ylianttila, M. Survey on blockchain-based smart contracts: Technical aspects and future research. *IEEE Access* **2021**, *9*, 87643–87662. [CrossRef]
53. Manzoor, A.; Braeken, A.; Kanhere, S.S.; Ylianttila, M.; Liyanage, M. Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain. *J. Netw. Comput. Appl.* **2021**, *176*, 102917. [CrossRef]
54. Xu, L.D.; Lu, Y.; Li, L. Embedding Blockchain Technology Into IoT for Security: A Survey. *IEEE Internet Things J.* **2021**, *8*, 10452–10473. [CrossRef]
55. Al-Turjman, F.; Zahmatkesh, H.; Shahroze, R. An overview of security and privacy in smart cities' IoT communications. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e3677. [CrossRef]

56. Javed, A.R.; Shahzad, F.; ur Rehman, S.; Zikria, Y.B.; Razzak, I.; Jalil, Z.; Xu, G. Future smart cities requirements, emerging technologies, applications, challenges, and future aspects. *Cities* **2022**, *129*, 103794. [CrossRef]
57. Victor, N.; Alazab, M.; Bhattacharya, S.; Magnusson, S.; Maddikunta, P.K.R.; Ramana, K.; Gadekallu, T.R. Federated Learning for IoUT: Concepts, Applications, Challenges and Opportunities. *arXiv* **2022**, arXiv:2207.13976.
58. Khanfar, A.A.; Iranmanesh, M.; Ghobakhloo, M.; Senali, M.G.; Fathi, M. Applications of blockchain technology in sustainable manufacturing and supply chain management: A systematic review. *Sustainability* **2021**, *13*, 7870. [CrossRef]
59. Wen, J.; Yang, J.; Wang, T. Path planning for autonomous underwater vehicles under the influence of ocean currents based on a fusion heuristic algorithm. *IEEE Trans. Veh. Technol.* **2021**, *70*, 8529–8544. [CrossRef]
60. Rubio-Solis, A.; Martinez-Hernandez, U.; Nava-Balanzar, L.; Garcia-Valdovinos, L.G.; Rodriguez-Olivares, N.A.; Orozco-Muñiz, J.P.; Salgado-Jimenez, T. Online Interval Type-2 Fuzzy Extreme Learning Machine applied to 3D path following for Remotely Operated Underwater Vehicles. *Appl. Soft Comput.* **2022**, *115*, 108054. [CrossRef]
61. Subramani, N.; Mohan, P.; Alotaibi, Y.; Alghamdi, S.; Khalaf, O.I. An efficient metaheuristic-based clustering with routing protocol for underwater wireless sensor networks. *Sensors* **2022**, *22*, 415. [CrossRef]
62. Ismail, A.; Wang, X.; Hawbani, A.; Alsamhi, S.; Abdel Aziz, S. Routing protocols classification for underwater wireless sensor networks based on localization and mobility. *Wirel. Netw.* **2022**, *28*, 797–826. [CrossRef]
63. Reddy, T.S.; Chandra, S.; Arya, R.; Verma, A.K. Malicious anchor node extraction using geodesic search for survivable underwater wireless sensor network. *Sci. Rep.* **2022**, *12*, 1–11.
64. Saleh, M.H.; Takruri, H.; Linge, N. Energy aware routing protocol for sparse underwater acoustic wireless sensor network. In Proceedings of the 2022 13th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), Porto, Portugal, 20–22 July 2022; pp. 750–755.
65. Menaka, D.; Gauni, S.; Manimegalai, C.; Kalimuthu, K. Vision of IoUT: Advances and future trends in optical wireless communication. *J. Opt.* **2021**, *50*, 439–452. [CrossRef]
66. Wazid, M.; Das, A.K.; Shetty, S.; Jo, M. A tutorial and future research for building a blockchain-based secure communication scheme for internet of intelligent things. *IEEE Access* **2020**, *8*, 88700–88716. [CrossRef]
67. Wang, H.; Han, G.; Hou, Y.; Guizani, M.; Peng, Y. A Multi-Channel Interference Based Source Location Privacy Protection Scheme in Underwater Acoustic Sensor Networks. *IEEE Trans. Veh. Technol.* **2021**, *71*, 2058–2069. [CrossRef]
68. Belotti, M.; Božić, N.; Pujolle, G.; Secci, S. A vademecum on blockchain technologies: When, which, and how. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3796–3838. [CrossRef]
69. Menon, V.G.; Midhunchakkaravarthy, D.; Sujith, A.; John, S.; Li, X.; Khosravi, M.R. Towards Energy-Efficient and Delay-Optimized Opportunistic Routing in Underwater Acoustic Sensor Networks for IoUT Platforms: An Overview and New Suggestions. *Comput. Intell. Neurosci.* **2022**, *2022*, 7061617. [CrossRef]
70. Shen, B.; Dong, C.; Minner, S. Combating Copycats in the Supply Chain with Permissioned Blockchain Technology. *Prod. Oper. Manag.* **2022**, *31*, 138–154. [CrossRef]
71. Huang, L.; Zhen, L.; Wang, J.; Zhang, X. Blockchain implementation for circular supply chain management: Evaluating critical success factors. *Ind. Mark. Manag.* **2022**, *102*, 451–464. [CrossRef]
72. Schinckus, C. A Nuanced perspective on blockchain technology and healthcare. *Technol. Soc.* **2022**, *71*, 102082. [CrossRef]
73. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasurbramanian, V. A lightweight blockchain based framework for underwater iot. *Electronics* **2019**, *8*, 1552. [CrossRef]
74. Razzaq, A. *Blockchain-Based Secure Data Transmission for Internet of Underwater Things*; Elsevier: Amsterdam, The Netherlands, 2022; SSRN 4127827.
75. Qiu, T.; Zhao, Z.; Zhang, T.; Chen, C.; Chen, C.P. Underwater Internet of Things in smart ocean: System architecture and open issues. *IEEE Trans. Ind. Inform.* **2019**, *16*, 4297–4307. [CrossRef]
76. Higuchi, A. Toward more integrated utilizations of geostationary satellite data for disaster management and risk mitigation. *Remote Sens.* **2021**, *13*, 1553. [CrossRef]
77. Esposito, M.; Palma, L.; Belli, A.; Sabbatini, L.; Pierleoni, P. Recent Advances in Internet of Things Solutions for Early Warning Systems: A Review. *Sensors* **2022**, *22*, 2124. [CrossRef] [PubMed]
78. Stojanovic, M.; Preisig, J. Underwater acoustic communication channels: Propagation models and statistical characterization. *IEEE Commun. Mag.* **2009**, *47*, 84–89. [CrossRef]
79. Wang, Q.; Guo, S.; Yiu, K.F.C. Distributed Acoustic Beamforming with Blockchain Protection. *IEEE Trans. Ind. Inform.* **2020**, *16*, 7126–7135. [CrossRef]
80. Nain, M.; Goyal, N. Localization techniques in underwater wireless sensor network. In Proceedings of the 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 4–5 March 2021; pp. 747–751.
81. Luo, J.; Yang, Y.; Wang, Z.; Chen, Y. Localization algorithm for underwater sensor network: A review. *IEEE Internet Things J.* **2021**, *8*, 13126–13144. [CrossRef]
82. Sah, D.K.; Nguyen, T.N.; Kandulna, M.; Cengiz, K.; Amgoth, T. 3D Localization and Error Minimization in Underwater Sensor Networks. *ACM Trans. Sens. Netw. (TOSN)* **2022**, *18*, 31. [CrossRef]
83. Li, H.; He, Y.; Cheng, X.; Zhu, H.; Sun, L. Security and privacy in localization for underwater sensor networks. *IEEE Commun. Mag.* **2015**, *53*, 56–62. [CrossRef]

84. Chen, G.; Wu, J.; Yang, W.; Bashir, A.K.; Li, G.; Hammoudeh, M. Leveraging graph convolutional-LSTM for energy-efficient caching in blockchain-based green IoT. *IEEE Trans. Green Commun. Netw.* **2021**, *5*, 1154–1164. [CrossRef]
85. Shen, D.; Huo, N.; Saab, S.S. A Probabilistically Quantized Learning Control Framework for Networked Linear Systems. *IEEE Trans. Neural Netw. Learn. Syst.* **2021**. [CrossRef]
86. Hammi, M.T.; Bellot, P.; Serhrouchni, A. BCTrust: A decentralized authentication blockchain-based mechanism. In Proceedings of the 2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain, 15–18 April 2018; pp. 1–6.
87. Hung, N.T.; Rego, F.F.; Pascoal, A.M. Cooperative Distributed Estimation and Control of Multiple Autonomous Vehicles for Range-Based Underwater Target Localization and Pursuit. *IEEE Trans. Control Syst. Technol.* **2021**, *30*, 1433–1447. [CrossRef]
88. Guo, L.; Ma, L.; Zhang, H.; Yang, J.; Cheng, Z.; Jiang, W. An Unmanned Underwater Vehicle Torpedoes Attack Behavior Autonomous Decision-Making Method Based on Model Fusion. *Electronics* **2022**, *11*, 3097. [CrossRef]
89. Islam, A.; Shin, S.Y. *Blockchain Based UAV-Assisted Underwater Monitoring in Internet of Underwater Things*; Korea Telecommunications Society: Seoul, Korea, 2019.
90. Zhou, Y.; Li, B.; Wang, J.; Rocco, E.; Meng, Q. Discovering unknowns: Context-enhanced anomaly detection for curiosity-driven autonomous underwater exploration. *Pattern Recognit.* **2022**, *131*, 108860. [CrossRef]
91. Lee, K.H.; Noh, J.; Khim, J.S. The Blue Economy and the United Nations' sustainable development goals: Challenges and opportunities. *Environ. Int.* **2020**, *137*, 105528. [CrossRef]
92. How Important Is the Ocean to Our Economy? Available online: https://oceanservice.noaa.gov/facts/oceaneconomy.html (accessed on 13 September 2022).
93. About NOAA Ocean Exploration. Available online: https://oceanexplorer.noaa.gov/about/welcome.html (accessed on 13 September 2022).
94. Ananda, R.G.; Vandavasi, B.N.J.; Raju, R.; Narayanaswamy, V.; Sethuraman, R.; Aravindakshan, A.M. Performance assesment of Navigation Systems Used in Deep-Water Scientific Human-Occupied Vehicle MATSYA 6000. In Proceedings of the OCEANS 2021, San Diego, CA, USA, 20–23 September 2021; pp. 1–9.
95. Blockchain Firm PO8 Raises Crypto for Bahamas Hurricane Relief. 2019. Available online: https://cointelegraph.com/news/bahama-blockchain-company-raises-crypto-for-hurricane-dorian-relief (accessed on 12 October 2022)
96. França, B. Deep Ocean: A blockchain-agnostic dark pool protocol. *arXiv* **2019**, arXiv:1910.02359.
97. Sun, K.; Cui, W.; Chen, C. Review of Underwater Sensing Technologies and Applications. *Sensors* **2021**, *21*, 7849. [CrossRef]
98. Tsai, C.H.; Elibol, A.; Chong, N.Y. A UAV-UUV Transformative Housing for Minimal Logistics Underwater Exploration. In Proceedings of the 2021 18th International Conference on Ubiquitous Robots (UR), Gangneung, Republic of Korea, 12–14 July 2021.
99. Nartey, C.; Tchao, E.T.; Gadze, J.D.; Yeboah-Akowuah, B.; Nunoo-Mensah, H.; Welte, D.; Sikora, A. Blockchain-IoT peer device storage optimization using an advanced time-variant multi-objective particle swarm optimization algorithm. *EURASIP J. Wirel. Commun. Netw.* **2022**, *2022*, 5. [CrossRef]
100. Xiao, Y.; Zhang, N.; Lou, W.; Hou, Y.T. A survey of distributed consensus protocols for blockchain networks. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1432–1465. [CrossRef]
101. Polge, J.; Robert, J.; Le Traon, Y. Permissioned blockchain frameworks in the industry: A comparison. *ICT Express* **2021**, *7*, 229–233. [CrossRef]
102. Haas, B.; Mackay, M.; Novaglio, C.; Fullbrook, L.; Murunga, M.; Sbrocchi, C.; McDonald, J.; McCormack, P.C.; Alexander, K.; Fudge, M.; et al. The future of ocean governance. *Rev. Fish Biol. Fish.* **2022**, *32*, 253–270. [CrossRef] [PubMed]
103. Crosman, K.M.; Allison, E.H.; Ota, Y.; Cisneros-Montemayor, A.M.; Singh, G.G.; Swartz, W.; Bailey, M.; Barclay, K.M.; Blume, G.; Colléter, M.; et al. Social equity is key to sustainable ocean governance. *NPJ Ocean. Sustain.* **2022**, *1*, 4. [CrossRef]
104. Joannou, D.; Kalawsky, R.; Martínez-García, M.; Fowler, C.; Fowler, K. Realizing the role of permissioned blockchains in a systems engineering lifecycle. *Systems* **2020**, *8*, 41. [CrossRef]
105. Kesari Mary, D.R.; Ko, E.; Yoon, D.J.; Shin, S.Y.; Park, S.H. Energy Optimization Techniques in Underwater Internet of Things: Issues, State-of-the-Art, and Future Directions. *Water* **2022**, *14*, 3240. [CrossRef]