future internet

MDPI

Article

Addressing ZSM Security Issues with Blockchain Technology

Michael Xevgenis [1,*], Dimitrios G. Kogias [2], Panagiotis A. Karkazis [3] and Helen C. Leligou [1]

[1] Department of Industrial Design and Production Engineering, University of West Attica, 122 43 Attica, Greece
[2] Department of Electrical and Electronics Engineering, University of West Attica, 122 43 Attica, Greece
[3] Department of Information and Computer Engineering, University of West Attica, 122 43 Attica, Greece
* Correspondence: mxevgenis@uniwa.gr

Abstract: Undoubtedly, we are witnessing a new era of computer networks that aspire to support modern demanding applications by providing the highest Quality of Experience (QoE) to the end user. Next Generations Networks (NGNs) ensure that characteristics such as ultra-low latency, high availability and wide service coverage can be met across the network regardless of the network infrastructure ownership. To accomplish that, beyond the necessary improvements in the radio propagation field, changes have been made in the core network functions which are now characterized as programmable, and software defined. Software Defined Networks (SDNs) and Network Function Virtualization (NFV) are the keystones of the NGNs flexibility. The high expectations of NGNs' performance and the continuous changes in the network conditions lead to the development of new network management frameworks that add elasticity and dynamicity and minimize human intervention. ETSI (the European Standards Organization) presents the Zero-touch Service Management (ZSM) framework that uses hyped technologies such as Artificial Intelligence (AI) and Machine Learning (ML) to achieve full end-to-end automation of the network services' management across one or many different domains. Focusing on multi-domain network service management, there are several security issues identified by the standardization team which mostly derive from the lack of trust among network providers. In the present research, we explore the suitability of blockchain technology adoption for facing these security issues. Blockchain technology inherently addresses security in trustless environments such as the infrastructures defined by the ZSM team. Our contribution is three-fold: (a) we define the architecture of a multi-domain network infrastructure that adopts the ZSM approach and integrates blockchain functionality, (b) we explore the adoption of different blockchain and distributed ledger technologies (DLT) approaches to address ZSM security needs and (c) we provide guidelines to prospective solution designers/implementers on the detailed requirements that this solution has to meet to maximize the offered value.

Keywords: zero touch networks; next generation networks; cross-domain resource management; blockchain/DLT

Citation: Xevgenis, M.; Kogias, D.G.; Karkazis, P.A.; Leligou, H.C. Addressing ZSM Security Issues with Blockchain Technology. *Future Internet* **2023**, *15*, 129. https://doi.org/10.3390/fi15040129

Academic Editors: Christoph Stach and Clémentine Gritti

Received: 17 February 2023
Revised: 24 March 2023
Accepted: 25 March 2023
Published: 28 March 2023

1. Introduction

Next Generation Networks (NGNs) offer network services based on technologies such as Software Defined Networking (SDN) and Network Function Virtualization (NFV). SDN and NFV reshape the nature of modern networks as they support network services via virtualized environments, without the need for a hardware networking device [1,2]. Therefore, the Providers (NPs) can easily trade (virtualized) resources to support modern Network Services (NSs) at different Quality of Service levels without having to resort to optimization of every single algorithm (from routing like [3] to the upper layer). In the new scene, the marketplace of resources grows as new players are entering the market [4–6]. These services are implemented by one or many Virtual Network Functions (VNFs) which are supported by a collection of computational resources in the form of Virtual Machines (VMs) or Containers (i.e., Dockers). The performance of the NSs both in terms of availability and latency affects the Quality of Experience (QoE) of the end-user [7,8]. Therefore, it is

crucial to orchestrate the performance of the individual NSs [9,10]. Considering that modern networks must support applications with very different QoS requirements, the ability of flexible and agile provisioning of high availability, ultra-low latency and 100% coverage is of high importance [11,12] and SDN/NFV-enabled networks play a crucial role in this [13,14]. Massive, seemingly infinite capacity, imperceptible latency, ultra-high reliability, personalized services with extreme improvements in customer experience, global web-scale coverage, and support for massive machine-to-machine communication are only a subset of the requirements that these deployments should fulfill. The flexibility offered by the SDN/VNF architecture opens the opportunity for NPs to enhance the utilization of their resources by the dynamic reconfiguration and allocation of workload to the different devices/resources. For given NS demands, NPs can trade resources to support NSs with predefined network characteristics when needed. To maximize the benefits of resource sharing, NPs need a framework for a highly dynamic, self-optimized resource management process. Additionally, to avoid human errors and reduce the response time of the system, the resource management process should require minimum human intervention.

The requirements of NPs have led the research community to the development of the Zero-touch network and Service Management (ZSM) standardization, kicked off by the ETSI (the European Standards Organization) in 2017 [15]. The pivotal deployment of 5/6G and network slicing gave birth to the need for a radical change regarding the management and orchestration of modern networks and services. More specifically, there is a need to handle: (a) the increased overall complexity of networks derived from their transformation into programmable, software-driven, service-based and holistically managed architectures, (b) the unprecedented operational agility (i.e., real-time management of NS) required to support new business opportunities enabled by technology breakthroughs, such as network slicing. The ultimate automation goal is to enable largely autonomous networks which will be driven by high-level policies and rules; these networks will be capable of self-configuration, self-monitoring, self-healing and self-optimization without further human intervention.

Besides the important benefits stemming from ZSM introduction, a set of security challenges are also introduced in this highly dynamic, automated resource management environment, as already pointed out by their proposers [15]. The concerns are related to the untrusted nature of modern networks where large numbers of NPs are involved and the security level of the automated mechanisms (many times powered by Artificial Intelligence (AI) and Machine Learning (ML)). Since these automation mechanisms are responsible to make important decisions regarding the management of the network, the safeguarding of this mechanism is vital for the network's well-being. These mechanisms must not be compromised, and their decisions must not be manipulated or tampered with. Although several solutions have been discussed in the ETSI documents, the complexity of the system increases as multiple different techniques are combined.

On the other hand, Blockchain technology (one of the most hyped technologies in 2022) is adopted in many different use cases. The ability to establish trust in an untrusted environment, the data integrity and the transaction validity ensured in the absence of a trusted third party are the main characteristics that make blockchain attractive. To accomplish that, blockchain solutions run in a decentralized and distributed network of nodes that are characterized as public, private, permissioned and permissionless, offering different degrees of participation control. In the last few years, blockchain has been successfully adopted in several sectors beyond cryptocurrency, such as supply chain management, maritime and gaming with several distributed applications (Dapps) [16–20].

The current work proposes to adopt blockchain technology to address the security concerns mentioned by the ZSM standardization team in [21] and describes how blockchain technology can be used, i.e., presents the architecture of such an implementation and provides the lifecycle of a management service in a ZSM-supported scenario. Next, it qualitatively assesses this proposition to prove that it inherently addresses the security issues identified by the ZSM group. Furthermore, we identify the criteria against which an

implemented solution should be evaluated. Considering that any prospective developer will use a basis for the solution of an existing blockchain or DLT platform, we evaluate indicative platforms (adopting Blockchains or Directed Acyclic Graphs (DAGs) structures), against the criteria mentioned earlier. To the best of our knowledge, this investigation and solution proposition has not been yet presented in other related works; they may mention that the use of a blockchain-based approach could be beneficial but the details of its design and implementation and the suitability of currently available blockchain approaches are not discussed.

This paper is organized as follows: Section 2 presents research works related to the use of AI/ML and blockchain in modern networks focusing on the topic of ZSM networks. Section 3 highlights the main requirements and elements of the ZSM framework and examines the case of cross-domain procedures placing emphasis on the security-related open issues involved in this scenario. In Section 4, the architecture of the blockchain-enabled ZSM framework is described in detail followed by an analysis of the main components and entities of this architecture. In Section 5, the criteria against which such a solution should be evaluated in real life are presented so as to guide the prospective developers to select appropriate baseline blockchain/DLT frameworks. Section 6 provides the assessment of the proposed architecture while Section 7 is devoted to the examination of baseline Blockchain/DLT platforms that are candidates for building a ZSM-oriented solution on top of them. Finally, Section 8 concludes the paper and additionally provides the potential and the next steps of this research direction.

2. Related Work

This section of the paper presents the related work with respect to (a) AI/ML techniques in resource management focusing on multi-domain scenarios and (b) blockchain-based solutions in NGNs and ZSM-compliant networks. The introduction of AI/ML for automation purposes succeeds in enhancing the automation level at the expense of introducing security vulnerabilities, which can be rectified by blockchain solutions.

2.1. The Role of AI/ML in the Implementation of the ZSM Concept

Artificial intelligence and Machine Learning techniques have been pursued to support the profiling of a service, the forecasting of the quality a service will experience for a given deployment scenario, and the placement of an NFV among others.

Dalgkitsis et al. [22], examine the use of Reinforcement Learning (RL) and more specifically, they leverage a Deep Deterministic Policy Gradient (DDPG) RL algorithm to solve the NFV placement problem in a scenario that consists of a Data Center (DC) and multiple Mobile Edge Computing (MECs) infrastructures. The goal is to minimize latency for ultra-Reliable Low Latency Communications (uRLLC). Uzunidis et al. [23], focus on the resource management process in NGNs and the proper network service profiling and placement in order to offer high QoE to the end user. In this work, authors present a framework to address the problem of service profiling and to predict the system's "critical points", focusing on complex services running over containers. In [24], the authors focus on the problem of choosing the proper amount of resources to support applications based on VNFs, especially in Mobile Edge Computing (MEC) environments where the computational resources are limited. They argue that AI technology can solve this problem in 5G networks, and they use it to develop a predictive autoscaling mechanism in NFV MANO that could automatically adapt the resources beforehand to the workload used by the application without any human intervention. Authors in this paper leverage Federated Learning (FL) techniques to design deep learning models for predictive Virtual MEC Application Functions (VMAF) autoscaling in a multi-domain setting that can better react to the changing service requirements, optimize the network resource usage, and also comply with data protection policies. Authors in [25] present a framework for Zero Touch Networks that use AI technology and microservices to perform self-orchestration of end-to-end network services. The presented research is part of the European H2020 program called

CHARITY. The goal is to increase the QoE by respecting Key Performance Indicators (KPIs), which are based on NGNs characteristics such as high availability and ultra-low latency. The outcome of this research is an Artificial Intelligence based Resource aware Orchestration (AIRO) framework in Cloud Native Environment that has been tested through simulation. However, the authors do not address the security issues when AI technology is used. This is anticipated to raise new challenges [26] when federated learning approaches enabling different NPs to contribute to the model training will be brought to the scene.

2.2. Examining Blockchain as a Mean for the Security Enhancement in NGNs

Authors in [27], present a combination of AI technology and DLTs in order to increase the security and trust in multi-operator mobile/cellular networks. The authors highlight the ability of AI to offer characteristics such as self-adaptation and self-reaction to next-generation networks which are susceptible to changes regarding the network conditions. This research is part of the 5GZORRO project, and its goal is to present a conceptual architecture of a solution that uses AI and DLTs. Another work of the same project [28] proposes the use of Smart Contracts (SCs) coupled with Cloud-Native operational Data Lakes to provide a zero-touch solution for the automated service assurance of multi-domain network slices. The SLAs which define the proper performance of the services are applied in the form of Smart Contracts (SCs) deployed in a blockchain network to increase the transparency of the process and to facilitate the integrity of the agreement. This research presents an architecture for a Smart Contract-based service assurance mechanism for network slices in a multi-domain environment that is SLA-driven. Additionally, this work aims to present a definition of AI-driven SLA breach detection and mitigation mechanisms implemented as modular Cloud-native services.

Benzaid et al. [29], describe the concept of Zero Touch Networks (ZTNs) and how AI can be used to automate the service management of modern networks. However, beyond the advantages of AI-driven ZTNs, security and trust are considered open issues by the authors when AI is used. According to the authors, it has been proven that ML techniques are vulnerable to several attacks targeting both the training phase and the test phase. Since data are used by the AI mechanism, their integrity and provenance are important for the proper operation of the mechanism. Authors claim that blockchain technology can be the antidote to these security limitations, due to its immutability and distributed nature, without providing any architecture or details for the design of such a solution.

In [30], the authors discuss the considerations regarding trust in modern multi-stakeholder networks and propose the use of blockchain technology to deal with trust issues. Smart Contracts (SCs) deployed in blockchain networks are ideal to create Service Level Agreements (SLAs) among stakeholders and control SLA violations in a transparent and secure manner. Based on the table presented by the authors, blockchain can be combined with many other technologies to solve trust and security issues in modern networks. Some of these technologies are VNFs, AI and ML. Moreover, sensitive data in modern networks can be protected using blockchain technology in order to guarantee their integrity and provenance. The authors discuss a use case where data are used as fuel for AI and ML focusing on the importance of data security and highlighting that data security is extremely important in AI/ML-based solutions. Data must be untampered and protected in order to avoid dataset poisoning which may lead to wrong decisions taken by the AI and ML mechanisms. In this use case, the data can be relevant to the service deployment parameters and the measured quality while blockchain technology could solve the security and trust issues.

In their survey paper, Liyanage et al. [31] present the progress of ZSM standardization and highlight the main goals and challenges. The security threats highlighted in this work by the authors are ML/AI-based attacks, open API security threats, intent-based security threats, automated Closed-Loop network-based security threats, and threats due to programmable network technologies. Moreover, the multidomain and heterogeneous nature of modern networks labels trust among different entities as a major issue. According

to the authors these open issues have not been sufficiently explored, although there are some published ideas where the use of blockchain is discussed as a solution.

Concluding, to the best of our knowledge none of the existing works clearly propose an architecture to answer how cross-domain resource management could be implemented in a secure manner using blockchain technology in ZSM-aligned networks. The current research aims to present a blockchain-enabled ZSM architecture for the secure E2E service deployment where blockchain and ZSM are combined. Combining several studies together to address all the issues would not necessarily result in solving all of them as unintended interactions/interplays may be revealed. Additionally, adopting the definition of complexity of [32], the combination of technologies and the introduction of large numbers of components would result in a significant complexity increase, while relying on a single technology (blockchain technology) introduces less complexity.

3. The ZSM Framework Overview: Architecture and Open Security Issues

ZSM is expected to become one of the dominating frameworks of NGNs according to ETSI and many articles in the literature such as [31]. The goal is the development of a framework that will include solutions and management services to achieve orchestration and automation of the emerging end-to-end network slicing technology, as well as of the end-to-end, cross-domain service orchestration and automation. Additionally, the ETSI standardization team works on generic enablers and solutions for closed-loop as well as on advanced topics for next-generation closed-loop operations. In this course of action, ZSM has highlighted the use of Artificial Intelligence (AI) and Machine Learning (ML) technologies in NGNs aiming to leverage the benefits they provide towards the automation and optimization of the service management process [33].

The reference architecture of the framework is presented in [34] and enables the definition of the functionality and the requirements that should be met in any ZSM implementation. For example, in cross-domain services, QoS requirements and service interoperability should be guaranteed across different management domains. In a multi-stakeholder scenario, a Management Domain (MD) is usually the administrative area of an NP that is responsible for the proper functioning of services running in this area. When E2E cross-domain services are deployed, the ZSM framework should guarantee the proper collaboration of MDs in order to support the E2E service with appropriate resources.

One of the main factors that affect the performance of the service is the time needed for the management tasks to be completed. The management tasks related to the deployment of E2E services should be executed within the limited processing time according to the ZSM reference architecture requirements. Functional and non-functional requirements defined by the ETSI standardization team in their manuscript determine the successful operation of the framework. The satisfaction of those requirements ensures the efficient operation of the network.

3.1. Description of ZSM Architecture and Main Elements

The main blocks in the ZSM architecture are illustrated in Figure 1 and are the following: the management services, the management functions, the management domains (MD), the end-to-end (E2E) service management domain, the cross-domain integration fabric and the data services. Management services are the core component as they can be offered and consumed by other services and ZSM participants to support network services and applications. The management services consumption and/or offering is conducted using management functions as presented in Figure 1. A management function can either be a "management service producer", a management "service consumer", or both at the same time. Moreover, management domains are used to define different areas of responsibility that belong to different ZSM participants. Each management domain can use its own management services or services offered for consumption by other management domains using the ZSM framework. The E2E service management domain depicted in the upper part of Figure 1, is a special management domain that provides end-to-end management of customer-facing services, composed of the customer-facing or resource-facing services pro-

vided by one or more management domains. The "cross-domain integration fabric" located at the center of Figure 1 is responsible for the interoperation and communication between the management functions within or across different domains. The registration, discovery and invocation of management services and the communication between management functions are implemented by the integration fabric. Finally, data services enable consistent means of shared management data access and persistence by authorized consumers across management services within or across management domains.

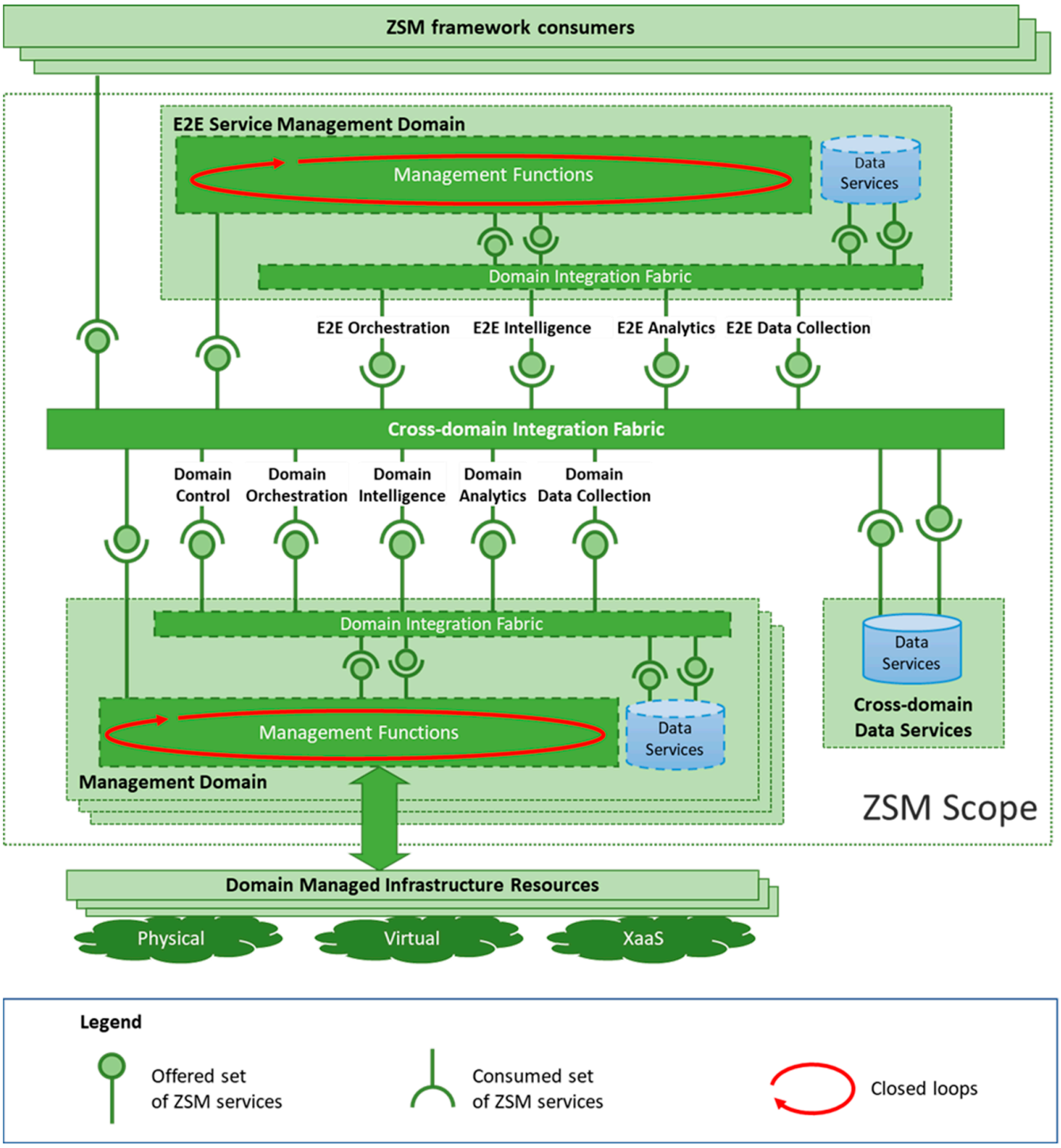

Figure 1. The ZSM architecture [34].

Considering the role of the aforementioned blocks, an example of ZSM operation is examined: supposing there is a multi-domain network where a network provider (say NP1) is responsible to support a demanding network service with characteristics that require a specific set of resources to provide the necessary QoS level. In the presented scenario, assume that NP1's resources are unavailable in the area where the service must be deployed. According to the standard's functionality, NP1 exploits the ZSM elements, such as management functions and cross-domain integration fabric, to find and consume a management service offered by another network provider (say NP2), which implements the necessary actions to cover the needs that NP1 has defined.

3.2. Open Security Issues

Among the requirements defined in [34], there are certain open security issues that are extremely vital for the ZSM's operation. The main issues and security risks of the ZSM framework as defined in [21], are as follows (and are also tabulated in Table 1):

- The trust relationship between multiple management domains: As new NPs form their management domain and embrace the ZSM concept, the collaboration among different domains in an automated manner requires a level of trust. Their proper operation is based on a service level agreement (SLA) signed among NPs (NP1 and NP2 in the example provided above), which must facilitate the proper network conditions for the desired operation of E2E service.
- Security risks introduced by the vulnerability of management function and security assurance of ZSM management function: Since the core functionality of ZSM is based on management services, the possibility of a security threat breach in the operation of those functions would be catastrophic. Therefore, the immutability and the high-security level of management functions are extremely important in ZSM networks.
- Security isolation and security requirement fulfillment in a multi-tenancy environment of ZSM framework: The multitenant nature of ZSM networks should not affect the security of services supported by virtualized resources. The isolation feature inherited by the virtualization technology that is used in modern networks increases the security level which should be high in every tenant of the network.
- Access control for management service provided by multiple domain service producers of ZSM framework: taking into consideration that numerous NPs provide a management service, the access over this service should be controlled and supervised in order to identify any malicious activity and avoid service malfunction. The normal functionality of these services should be safeguarded since they are the heart of the ZSM framework.
- Leverage existing security specifications to identify security risks of AI/ML models and protect AI/ML models in the ZSM framework: Although AI/ML are key technologies of the ZSM and increase the automation level of modern networks by introducing characteristics such as self-adaptation and self-optimization, their susceptibility in malicious attacks is a major issue. Models used in these technologies are trained using data sets that might be tampered. This type of attack is called dataset poisoning and may lead to wrong AI/ML decisions which are major threats to the framework's proper functionality [35].

Table 1. Solutions to security issues: Current ZSM vs. Blockchain-based ZSM.

Security issues and complexity	Trust relationship between multiple management domains	Security risks due to the vulnerability of management functions	Access control for management services in a multi domain scenario	Security risk of AI/ML model and protection of AI/ML models in ZSM	Complexity level
Current ZSM approach—Solutions	Reflective and adaptive trust model	GSMA Network Equipment Security Assurance Scheme (NESAS)	Authentication and authorization mechanisms, which check the trust relationship among entities	Risk assessment based on the Adversarial ML Threat Matrix	High—Use a bunch of technologies to increase ZSM security
Blockchain-based ZSM approach—Solutions	Achieve trust in trustless environment using blockchain	Use of SCs to eliminate the vulnerabilities which are automatically and securely executed	Use SCs for management services and apply visibility rules to achieve access control	Store the AI/ML decisions in the ledger and guarantee dataset integrity using both blockchain and IPFS	Low—Use blockchain technology and take advantage of its inherent characteristics

In [21], the standardization team proposes countermeasures to overcome the security issues mentioned above. Regarding the trust relationship among entities, they propose a reflective and adaptive trust model to build mutual trust among entities in the ZSM framework. The goal of this process is to ensure the confidentiality, integrity, availability, and regulatory compliance of every MD. To accomplish this, each entity that owns an MD needs to evaluate the trustworthiness of the other entity also owning an MD, based on threat and risk analysis and by examining the security policies applied in the entity. The outcome of this process leads to the building of a trust relationship among entities, followed by authentication procedures between parties and the formation of a secure channel where the behavior of each entity is tracked. Although this solution seems to tackle the trust problem, other approaches can also be investigated.

The safeguarding of management functions which are crucial for the operation of ZSM is addressed using the GSMA Network Equipment Security Assurance Scheme (NESAS). This methodology defines security requirements and performs an assessment for secure product development and product lifecycle processes, using 3GPP's defined security processes for the evaluation of network equipment. Although this solution is tested for the security assurance of network equipment following the 3GPP's Security Assurance Methodology (SECAM), other technologies could be studied to protect management functions. Additionally, the multitenancy issue is answered using policies applied to each tenant that uses the ZSM framework. The policy mechanism aims to provide a sufficient security layer for the users of the ZSM framework to avoid the exploitation of multi-tenancy which may lead to the loss of sensitive data of E2E services and the loss of the frameworks' reputation. However, this solution is based on security requirements defined by authors and cannot by itself be considered as a high-security level solution. Moreover, the access control of management services (MnS) is another major issue, as the exhaustive usage of management resources by a malicious entity may cause the mis-operation of these critical services. Robust access control mechanism, including identification processes, authentication, authorization and audit of MnS usage, should be applied to prevent MnSs and other management resources of the ZSM framework from being misused by MnS consumers, according to the authors. Considering that ZSM is implemented in a multi-domain environment, the standardization team proposes techniques to enhance the security of MnSs by introducing authentication and authorization mechanisms, which check the trust relationship among entities in ZSM.

AI and ML are the main technologies used in the ZSM framework and their reliability and robustness should not be left open to dispute. The decisions of AI/ML affect the ZSM network operation as they perform closed-loop operations for the efficient deployment of

E2E cross-domain services. A comprehensive risk assessment for the AI/ML vulnerability issue based on the Adversarial ML A Threat Matrix is presented in [21] and possible countermeasures are proposed at a high level only.

4. The Architecture of the Blockchain-Enabled ZSM Approach

The proposed blockchain approach aims at increasing the security of the ZSM framework by addressing the aforementioned security issues and at the same time maintaining the complexity level low (as will be explained) using the blockchain technology and the benefits it inherently provides. Focusing on the scenario of E2E service deployment in a multi-domain environment and having in mind the architecture described in [34], we propose the introduction of blockchain technology in the cross-domain integration fabric component as it is depicted in Figure 2.

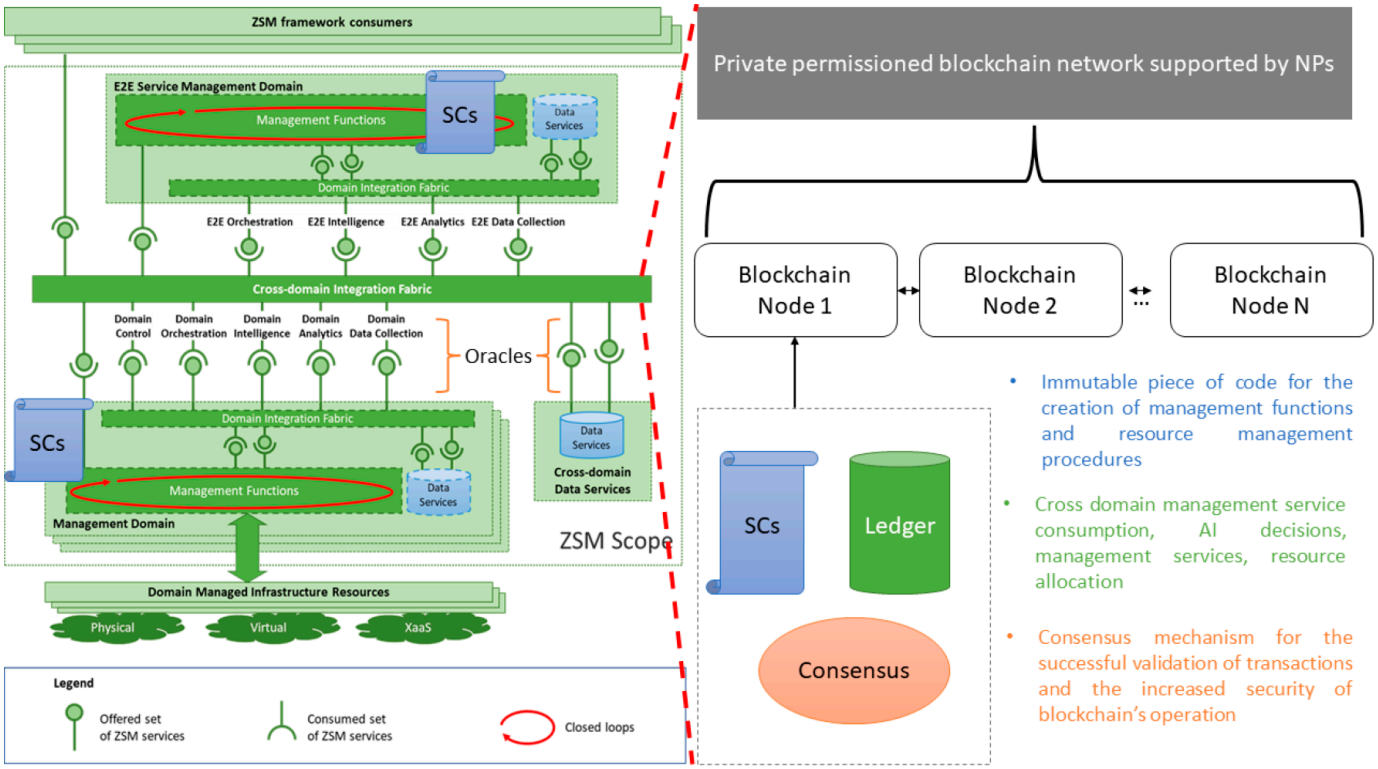

Figure 2. The architecture of blockchain-based ZSM.

In the presented approach, each NP is part of the ZSM framework and hosts a blockchain node that belongs to a *private permissioned blockchain network* as depicted in the figure above. The private and permissioned characteristic of the network increases the security of this approach as we are able to control which NPs participate in the network and at the same time minimize the possibility of a malicious participant. This is also the approach adopted in [36] for Secure Routing for Multidomain SDN-Enabled IoT Network. The NPs are registered in the blockchain and obtain a unique address (IDs) used for their identification in the network. In addition, the ledger of the blockchain includes not only the IDs of the NPs but also the addresses of the Smart Contracts (SCs) deployed in the network. Both the E2E service management domain and the management domain of the ZSM participant create and execute *management functions, which are deployed in the form of SC in the blockchain network*. According to the ZSM standard, the development and execution of management functions are implemented using closed loops. Closed loops are based on AI/ML technology which uses mathematical models trained by secure datasets of the framework. It is worth mentioning that no AI/ML code runs inside the blockchain. It is *the decisions* generated by the closed-loop mechanisms that *are registered in the blockchain* so as

to ensure the immutability and traceability of the decisions. Additionally, every change in the ZSM network in a cross-domain scenario, which in our case can be *the consumption* of a management function, is considered a transaction and *is stored in the ledger*. The registration of an NP, the creation of an SC that utilizes a management function and the outcome of an SC are considered blockchain transactions and are permanently written in the ledger of the blockchain. Moreover, the blockchain interacts with other ZSM components using *oracle mechanisms to ensure that valid information is exchanged from and towards the blockchain*. Oracles in our case are software mechanisms developed to provide a secure interface between the blockchain network (including the SCs deployed in it) and ZSM services. To accomplish that, oracles use cryptography or/and consensus techniques applied on-chain or off-chain, to establish a secure connection between blockchain and other services outside of it. In the current research, oracles are used by the cross-domain integration fabric component as presented in Figure 2.

Let us examine how the multi-domain scenario described in the previous section changes with the integration of blockchain technology. Assuming that NP1 has a request to support a demanding streaming application based on predefined network services. In this scenario, NP1 cannot support the application using its own resources and uses the ZSM framework to complete the request. Using the management services, NP1 finds another management service in a different domain that can fulfill the request. NP1 decides to consume the management service of the other provider (i.e., NP2) by executing a management function in the form of SC. An example of this SC is described in an abstract manner by the following pseudocode.

```
NP1.ZSM(search_MnS[network_resources, MD]) = true;
ZSM.returns true; “This is the result of ZSM that triggers the SC via the oracle mechanism”
function requestResources(NP1, NP2, MnS) public returns{
    if NP2 is true:
        NP2[id].lease[MnS] to NP1
        transfer_resources(NP2, NP1);   "This is a transaction stored in the ledger"
        oracle.transaction(NP2,NP1, MnS); “Triggers ZSM to implement the agreed NSs”
}
```

Pseudocode 1. Example of a Management Function in the form of SC.

The consumption of NP2's service by NP1 is registered as a transaction in the blockchain and the details of this transaction are defined by the SC. Finally, since the network is zero-touch, the decision regarding the consumption of a management service by the NP1 provider can be made by an AI/ML mechanism. Blockchain stores the decisions of AI in the form of transactions. (It could additionally be used to check the validity of datasets stored in an Inter Planetary File System (IPFS) structure which were used to train the ML model). Figure 3 illustrates the complete lifecycle of the described resource management operation that follows the blockchain-enabled ZSM approach.

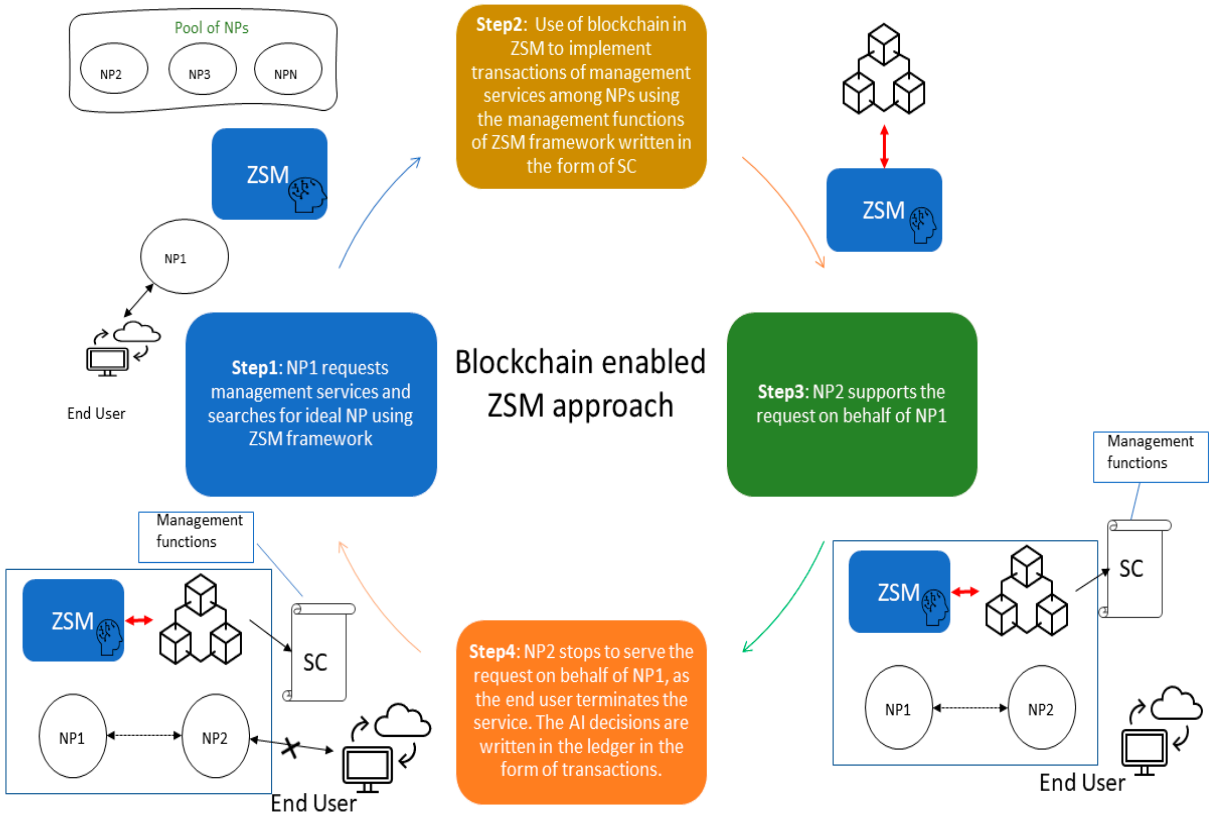

Figure 3. Lifecycle of a blockchain-enabled ZSM scenario.

5. Criteria for the Selection of the Blockchain/DLT Platform to Build the ZSM-Tailored Solution

The selection of the most suitable DLT solution for the development of a blockchain-based ZSM scenario should be based on specific criteria which should be clearly defined. The following section of this paper aims to present the characteristics that a DLT solution should present in order to satisfy the needs of the ZSM use case. Furthermore, we proceed to the identification of the most suitable blockchain and DAG solutions, and we analyze their main functionalities and characteristics. Then we evaluate their suitability for the particular use case and we propose modifications to fulfill the requirements of our scenario.

The performance of the blockchain network directly affects the performance of the overall system which means that characteristics of the network such as latency and throughput affect the end user's QoE. Furthermore, other characteristics such as the accessibility of the network, the resiliency, the scalability and the network's ability to easily accept new features, are vital for the systems' successful operation and future growth. To this end, we define certain characteristics that a DLT solution should present in order to build a secure, scalable and high-performance environment ready to be integrated with the ZSM framework. The DLT solution integrated with the ZSM framework must be:

- ✔ Access controlled: the access and the ability to perform actions in the network should be allowed only to permitted members and should be restricted to anyone else.
- ✔ Scalable: the nodes of the network are hosted by the NPs only. Every provider who wishes to join the network should be able to easily deploy a node and become an active member of the solution.
- ✔ Resilient: the proper functionality of the network should not be affected if a node or a number of nodes become unavailable for a period of time. The network should be resilient to network failures in order to present high availability which is one of the main requirements of NGNs.

- ✔ Very fast: the network should be able to perform multiple actions in a short period of time (in the unit of seconds or even milliseconds), to meet the dynamicity and resource management agility target by NGNs.
- ✔ Programmable: the DLT adopted in this particular use case should be able to support the development of code to implement the necessary functions which proliferate over time.
- ✔ Extensible: the DLT chosen for the implementation of this scenario should be able to accept new features that will upgrade its functionality and cover needs that may occur in the future.
- ✔ Interoperable: the DLT should be able to support interaction with services outside the network in order to successfully communicate with ZSM services. This characteristic increases the ability of the network to interact with the outside world and use services that may leverage the functionality of the whole solution.

The above characteristics are translated in blockchain terms as follows:

- ✔ Permissioned network: only the permitted entities can access the network and perform actions in the form of transactions. This feature increases the security of the system since every entity is known to others, and therefore, it is less possible to act maliciously. It should be noted that the government entity does not control the operation of the network and its role is restricted only to the authorization of the NPs.
- ✔ Private/Consortium network: the network is supported by the NPs only, which means that the nodes of the network are created, managed and maintained by the participants. Although this feature seems to question the sentiment of decentralization in the network, it increases the security of the system since only the NPs are responsible for the proper operation of the network. In this particular use case, an NP who wishes to become an active member of the network should be able to easily deploy a node that will automatically become part of the network. This results in the growth of the network as new NPs with new nodes can easily become part of the solution. As a result, the scalability feature of the entire solution is highlighted, which is a factor that attracts new members.
- ✔ Crash fault tolerance: the network should support fault-tolerant mechanisms in order to ensure that its operation is not affected if a number of nodes become unavailable. Considering that the ZSM framework uses the DLT network to perform crucial tasks, the resiliency of the network is vital in our scenario. The main element that is responsible for the network's proper operation is the consensus. Therefore, the network should be able to use consensus mechanisms that will increase its fault tolerance and guarantee the functionality of the system in hazardous situations.
- ✔ Low consensus convergence time: the proposed solution is expected to receive a large number of transactions which must be validated/executed with the minimum possible delay. As a result, the selection of a consensus algorithm with a low convergence time that is able to cope with a high number of transactions is crucial. This characteristic is related to the previous one, as the consensus mechanism used is able to increase the resiliency of the network and the speed of transaction validation. Therefore, the DLT solution should be able to support a consensus mechanism that can validate transactions fast, and at the same time tolerate failures.
- ✔ Support of SCs: the development of code in DLTs can be accomplished by the creation of SCs that can implement various functionalities of the network in a secure manner. Since the network should interact with ZSM services and provide solutions to many different problems regarding the management of modern networks, the capability of the DLT to support SCs is extremely important.
- ✔ Support of tokens: this feature is related to the previous one and highlights the need to support tokens implemented in the form of special SC functions, which improve the functionality of the solution. Tokens can be used to represent assets, currency and rights (i.e., use a token to access a website). The development of tokens is based on standards that ensure their smooth integration into the network. There are two main well-known token categories, Fungible Tokens (ERC 20) and Non-Fungible Tokens

(ERC 721). In our use case, a Fungible token could be used to create a currency used for the transactions among NPs in order to build a modern marketplace. Additionally, Non-Fungible Tokens (NFTs) could be developed to represent the reputation of an NP which could be related to the successful completion of a number of requests. This feature could be used by NPs as a criterion during the process of NP selection to support their request. It should be mentioned that these scenarios are only examples of how tokens could be used and have not yet been designed for our use case. However, the ability of a network to accept and use new programming features to enhance its functionality and solve any future issues is a very important characteristic.

✔ Interaction with oracle mechanisms: the DLT solution should be able to interact with entities outside the network in a secure manner to leverage the functionality of the whole system and support the ZSM processes. To this end, oracle mechanisms must be supported by the network, while the selection of the most suitable solution should be made based on the security level and performance. On the one hand, the information from and towards the network should be well protected while on the other hand, the latency introduced by the oracle should be the minimum. Having in mind that some oracle solutions use consensus, which automatically introduces extra latency to the system, the selection of other oracles that use different tools seems to be preferred. There are many oracle mechanisms available that use encryption to protect the content of their data and guarantee the origin of the information. The adoption of such a solution may not affect the overall system's performance dramatically.

6. Assessment of the Architecture

We examine how the proposed solution tackles the security issues mentioned in Section 3.2 one-by-one in the sequel and also tabulate them in Table 1.

As new NPs join the ZSM framework, the number of blockchain nodes increases and the network grows, assuming that each NP hosts/deploys at least one blockchain node. The private and permissioned characteristics of the network minimize the possibility of the existence of a malicious player which is also tackled by the applied consensus mechanism. Since the blockchain network is private and permissioned, we assume that a trusted governance entity is responsible for registering the NPs to the network. Automatically, a trust layer among competitive NPs is created and the *trust issue among multiple management domains* (security issue 1) highlighted by the ETSI team is addressed.

To reduce the *vulnerabilities of management functions* (security issue 2) we take advantage of the immutability feature of Smart Contracts (SCs). We propose the use of SCs for the implementation of the management functions defined in [34]. The rationale behind this is the following: an SC is an immutable deterministic piece of code stored and used in the blockchain network. An SC's functionality cannot be undermined, and its content cannot be tampered with as it is stored in the ledger. When an SC is created, it is related to a unique blockchain address used by other entities in the network in order to execute its functions. Additionally, an SC is a set of promises that are executed when predefined conditions are met. This feature allows SCs to execute functions automatically without human intervention. Given the *security concerns regarding the vulnerability of management functions* in ZSM, the use of SCs for their implementation is ideal.

Moreover, the ability to control an SC's visibility to other blockchain participants is supported in various blockchain solutions and can be used to increase the confidentiality of a transaction or the non-disclosure of SC's information in multitenant environments, if this is required. As a result, we can achieve *access control to sensitive information*, such as management functions, stored in the network.

Blockchain can also be used to monitor the behavior of AI/ML by storing the decisions in the form of transactions. The traceability feature of blockchain allows us to examine the decisions of AI/ML components during their operation and identify any suspicious activity. At the same time, the credibility of the decisions' history cannot be questioned since it is a valid blockchain transaction registered in the ledger. Furthermore, the training

of mathematical models used in these technologies is based on datasets that should be safeguarded. Although the first thought would be to store datasets in the blockchain, the scalability issue of this technology forces us to design an alternative solution. Datasets which usually include enormous amounts of information can be stored in Inter Planetary File System (IPFS) distributed structures and the link that points to the data location can be stored in the form of a hash as a valid transaction. As a result, the origin and quality of data are guaranteed, and an *extra layer of security is added to the AI/ML components of ZSM*.

Finally, with respect to the complexity, we adopt the definition presented in [32] where the complexity level of the system is defined based on the number of parts comprising the system. According to the definition, a system that uses a smaller number of parts is less complex than a system that uses a higher number of parts. In this paper, the solutions proposed by the standardization team use many different technologies and techniques (e.g., NESAS, Adversarial ML Threat Matrix) to tackle security issues. Our approach aims to eliminate these issues by using only blockchain technology.

It is worth stressing that based on our experience from the implementation of a solution that supports resource trading among NPs (which is presented in [37,38]), the transaction speed using the Ethereum-Quorum platform as the basis for the solution is in the order of a few seconds and highly depends on the adopted consensus mechanisms while the number of nodes in the network does not have a significant impact on this performance aspect. Furthermore, the infrastructural resources required for the implementation of this functionality are definitely affordable by a network provider. In our experiments presented in [37,38], we implemented a blockchain network supported by blockchain nodes in the form of VMs with the following characteristics: four CPU cores, 8GB memory (RAM) and 30GB storage. Additional insights on the parameters that affect the performance of blockchain-based solutions are provided in [39,40].

7. Assessment of Blockchain and DAG Platforms to Be Used for the ZSM-Solution Implementation

Having defined the main characteristics that a DLT solution should present to become the ideal choice for our scenario, we proceed to the assessment of several well-known DLT solutions. In this section of the paper, we identify the main characteristics of Hyperledger Fabric (HLF) [41], Ethereum Quorum [42] and R3 Corda [43] which belong to the blockchain family and then we focus on two DAG solutions, the IOTA [44] and the Hedera Hashgraph [45]. The reason for their selection is that they present characteristics that are more likely to fulfill the requirements of our scenario. At the end of our assessment, we tabulate our findings to guide prospective implementers.

7.1. Candidate Blockchain and DAG Solutions for Our Approach

7.1.1. Hyperledger Fabric (HLF)

This blockchain solution is an open-source permitted platform that is established and maintained under the umbrella of the Linux Foundation. HLF's architecture is modular and configurable in order to easily adapt to a wide spectrum of industry use cases. The versatility of this platform makes it ideal for several sectors such as healthcare, supply chain and others, while its ability to support SCs written in general-purpose programming languages (i.e., Java, Go and Node.js) makes it very attractive to organizations. In addition, this platform is permission; therefore, the participants are known to each other which automatically grows a sentiment of security. This means that while the participants may not fully trust one another (they may, for example, be competitors in the same industry), a network can be operated under a governance model [41].

Another important characteristic of this platform is its ability to support pluggable consensus mechanisms. This feature allows HLF to be effectively customized in order to fit various use cases. For instance, in the ZSM scenario where only known NPs are members of the network, a fully byzantine fault tolerant mechanism might be considered unnecessary and an excessive drag on performance and throughput. In order to maintain high-performance

standards and increase the availability of the solution, a crash fault-tolerant consensus might be the preferred option. This modular architecture allows the platform to rely on well-established toolkits for crash fault-tolerant or byzantine fault-tolerant ordering. Fabric currently offers a crash fault-tolerant ordering service implementation based on the etcd library of the Raft protocol. Moreover, Fabric can leverage consensus protocols that do not require a native cryptocurrency to incent costly mining or to fuel smart contract execution.

The aforementioned design features make HLF one of the better-performing platforms both in terms of transaction processing and transaction confirmation latency, and it enables privacy and confidentiality of transactions and the smart contracts that implement them. It should be mentioned that many research papers have been published where the performance metrics of the HLF are studied and tested using the Hyperledger Caliper. Authors in [46] scaled HLF to 20,000 transactions per second [41]. Concluding the presentation of HLF, this solution supports the creation and management of tokens and is able to use several oracle mechanisms in order to become suitable for several use cases that demand the interaction of blockchain with the outside world.

7.1.2. Ethereum Quorum

Quorum is a permitted implementation of Ethereum and it was initially developed by JP Morgan. The goal of this blockchain is to cover the needs of scenarios designed to operate in a controlled network where the identity of the members is known and access to the public is restricted. Therefore, it is considered an ideal solution for the implementation of private and consortium networks.

In contrast to the traditional Ethereum network, Quorum supports two different types of consensus mechanisms: the Raft and the IBFT. This feature allows developers to use a mechanism that suits better to their use case. For example, the Raft which belongs to the Crash Fault Tolerance (CFT) consensus family is preferred in cases where the existence of a malicious participant is unlikely and the need for fault tolerance is high. Nevertheless, in cases where many different entities are participating in the Quorum network and the likelihood of a malicious member is high, the IBFT mechanism is preferred since it introduces byzantine fault tolerance.

Similar to Ethereum, the network of Quorum supports the use of tokens and SCs that allow the creation of distributed secure applications. This feature broadens the application area of Quorum as many DApps can be developed to implement various scenarios. However, a major difference between these two blockchains is that Quorum supports privacy which was one of its main design goals. More specifically, it allows subsets of parties in a consortium to transact with one another without making the transactions public to members of the larger consortium. Quorum practically splits the ledger into a public and a private ledger. All nodes of the network can observe the public ledger, while the private ledger is visible only to the transacting parties. Only a hash of the private transaction appears on the public ledger and is visible to other nodes that are not counterparties to the transactions. This process can be conducted also for the deployment of private smart contracts which would be visible only to the transacting parties [47].

Moreover, another significant difference between Quorum and Ethereum is the fact that Quorum does not adopt the concept of adding cost to a transaction using gas. Although it is a fork of Ethereum and supports the use of gas, it sets this value to zero to run transactions without gas fees. Since Quorum is usually deployed in a consortium or private blockchain, the use of gas in Ethereum terms is not mandatory [47]. Additionally, the Quorum platform can be combined with the oracle mechanism in order to become part of a solution that is not limited only to the blockchain world.

7.1.3. R3 Corda

Another popular blockchain platform is the R3 Corda, which allows the implementation of private permitted networks ready to support various use cases. The consensus process can be implemented using either a crash or byzantine fault-tolerant algorithm. The

selection of the desired algorithm depends on the use case scenario as it is stated earlier. Similar to the previous platforms, Corda supports both BFT and Raft mechanisms. Considering our use case presented previously, a notary [48] that uses Raft between nodes that form a network of NPs will present extremely good performance in terms of throughput and latency, at the cost of being more vulnerable to malicious attack by whichever node has been elected as a leader.

Moreover, the Corda platform supports SCs for the development of several solutions called Cor-Dapps. SCs are defined using a restricted form of Java Virtual Machine (JVM) bytecode, which automatically allows developers to implement the logic of their solution by writing code in a variety of programming languages. Developers are able to use well-developed toolchains and reuse code written in Java or other JVM-compatible languages, which is a fact that widens the application area of this platform. Additionally, Corda supports the development and use of tokens which can be used according to our use case to represent resources, such as CPU, memory and others [48].

Additionally, the privacy feature is supported in this blockchain as Corda uses several techniques to achieve this functionality. This means that the implementation of private transactions or the execution of private SCs is feasible. At the same time, Corda supports the use of oracles, defined as a network service that is trusted to sign transactions containing statements about the world outside the ledger only if the statements are true. This characteristic allows the secure communication of blockchain with entities outside the network such as the ZSM framework and its services. Additionally, Corda presents high-performance values as it can reach up to 20,000 transactions per second according to their benchmarking results illustrated on the platform's website [43,48].

7.1.4. IOTA

IOTA is a very popular DLT solution, which is based on the Tangle DAG. It is supported by the IOTA Foundation which aims at the development of new DLT-based solutions. On July 2016 the IOTA main net was activated and it is considered a public permissionless network. Some of IOTA's main characteristics are the increased scalability, the increased sentiment of decentralization and the zero transaction fees. In contrast to typical blockchain networks which present scalability issues as the transaction number increases, IOTA becomes more efficient and more powerful when the transaction number grows. Since IOTA does not use miners in the network, a node is at the same time the creator and the validator of a transaction. This means that everyone in the network contributes to the consensus process, which is a fact that highlights the decentralized nature of this particular solution. Moreover, the consensus mechanism implemented in the latest IOTA version is a probabilistic leaderless binary voting protocol called fast probabilistic consensus (FPC). This mechanism is responsible for Tangle's validity by addressing issues such as the double spending problem [44].

IOTA supports the creation of smart contracts called ISC and hence the development of several applications for various use case scenarios. ISC is agnostic regarding the virtual machine which executes the SC code. IOTA currently supports two types of SCs: the Rust/Wasm-based and Solidity/EVM-based [49]. Furthermore, IOTA allows the use of tokens that can be exchanged among entities in this DAG-based network. A well-known token used as a cryptocurrency in this solution is the MIOTA which can be purchased by a user in order to buy assets in the network. MIOTA is an example of a fungible token; however, the use of NFTs is also supported. Moreover, the use of oracles is supported in this DLT [50]. Oracles bring off-chain data to decentralized applications and smart contracts on the IOTA network. These mechanisms provide blockchains with outside information, typically for use in smart contracts, or provide interoperability between different distributed ledgers.

7.1.5. Hedera Hashgraph

Another DAG-based solution is presented by Hedera, named Hedera Hashgraph, which uses a distributed network, cryptographic tools and timestamps to store data in the

form of transactions. This platform is considered a public permitted network, although it is currently governed by the Hedera Council which deploys and supports the network nodes. In the future, anyone will be able to host and operate a Hedera Hashgraph node.

The consensus mechanism used in this DLT is called Hashgraph and is based on the gossip protocol [45]. Every node that transacts with another one sends information regarding the current state of the network which is based on information previously received by other nodes. As a result, the information regarding the current state spreads like gossip among the nodes of the network. Therefore, every node in the network contributes to the consensus process and every node is aware of the current state. Hashgraph achieves a high-throughput with 10,000+ transactions per second today and low-latency finality in seconds from its innovative gossip about gossip protocol and virtual voting. Once consensus is reached, the transaction is immutable and available on the public ledger for everyone to transparently see. It should be mentioned that the nodes store only the latest state of the network in their ledger, which automatically increases the scalability of the network.

Additionally, Hedera Hashgraph offers a set of so-called Hedera Services that allow users to perform various tasks such as the creation of SCs and tokens. The Smart Contract service of Hedera allows the creation of contracts using the Solidity language similar to Ethereum-based networks, while Hedera promises fast SC execution with lower cost than blockchain alternatives. Moreover, tokens are supported by the Hedera Token service which allows the configuration and management of native fungible and non-fungible tokens. Having in mind our use case, an NP could receive a payment in the form of token for lending its resources to another NP. In addition, NFTs could be used as a reputation badge to highlight the reliability of an NP in our scenario. The support of SCs and tokens widens the application area of Hedera Hashgraph which can be used in various use cases.

Nevertheless, an additional factor that adds extra flexibility to this platform is its ability to cooperate with oracle mechanisms. Chainlink and Hedera Hashgraph announced in 2019 their collaboration to integrate Chainlink's decentralized oracle solution with Hedera's network. Chainlink is a well-known oracle mechanism that allows smart contracts to securely access and retrieve off-chain information when needed. It uses a similar model to a blockchain, as it implements a decentralized network of independent entities, called oracles, that collectively retrieve data from multiple sources, aggregate it, and deliver a validated single data point to the smart contract to trigger its execution, removing any centralized point of failure [51].

7.2. Assessment of Blockchain/DAG Platforms

Having examined the blockchain and DAG DLTs in the previous subsection, we proceed to the identification of their main characteristics in Table 2, which directly affect their suitability for our use case scenario. The columns of the table present the main attributes that describe the DLT's functionality while at the bottom of the table, the row with the ideal solution defines the properties of the most suitable solution for our scenario.

Table 2. Suitability of the examined blockchain and DAG solutions.

Solution	Public—Private/Consortium	Permissioned—Permissionless	Consensus Type	Support of SCs	Support of Tokens	Support of Oracles
HLF	Private/Consortium	Permissioned	CFT (Raft) or BFT (pBFT)	Yes	Yes	Yes
Quorum	Private/Consortium	Permissioned	CFT (Raft) or BFT (IBFT)	Yes (private SCs)	Yes	Yes
R3 Corda	Private/Consortium	Permissioned	CFT (Raft) or BFT (pBFT)	Yes (private SCs)	Yes	Yes
IOTA	Public	Permissionless	FPC	Yes	Yes	Yes
Hedera Hashgraph	Public	Permissioned	Hashgraph	Yes	Yes	Yes
Ideal solution	Private/Consortium	Permissioned	CFT—rapid convergence	Yes	Yes	Yes

Comparing each of the discussed solutions with the ideal one, we observe that every solution supports SCs, tokens and oracle mechanisms. However, in the Quorum and R3 Corda, we are able to use private SCs and implement private transactions if necessary. This is an extra feature that can be used to add extra functionalities to our solution in the future. For instance, some NPs in the network may sign an agreement of cooperation and fulfill requests with special terms which they might not want to unveil to other NPs in the network.

Furthermore, the blockchain solutions implement private/consortium and permitted blockchains which are the ideal characteristics of the network to be adopted in our scenario. On the contrary, IOTA and Hedera Hashgraph support only public implementations while the IOTA network allows access to anyone as it is a permissionless network. These characteristics decrease the suitability level of those solutions for our use case and should be modified.

In addition, the ideal solution should use a crash fault tolerant consensus mechanism with high convergence time in order to ensure the high availability of the system and achieve high transaction validation numbers, considering that the likelihood of a malicious participant is low. As illustrated in Table 2 the blockchain-based solutions can use consensus mechanisms with these features by implementing the Raft algorithm. However, DAG-based solutions use the FPC and Hashgraph mechanisms which present higher transaction validation speed which seems ideal for our use case. In terms of performance, the DAG solutions present higher numbers (transaction throughput) than the blockchain ones, and therefore, they are considered more suitable for our use case where the transaction number is expected to be extremely high.

The scalability of the DLT solution is also a significant factor that plays a crucial role in the selection of the ideal solution. As was mentioned in previous subsections, the blockchain solutions present scalability issues as every node holds a full copy of the ledger which increases as new transactions are validated. Nevertheless, DAG nodes store only parts of the graphs, and therefore, they scale well when the transaction number increases. Hence, they are considered more scalable than blockchain solutions.

To conclude, the qualitative assessment of blockchain/DAG platforms on which the prospective developer could build the ZSM-oriented solution, currently, none of the examined networks fulfill the criteria to become the ideal solution for our use case. The development of a private/consortium and permissionless DAG network could be the most suitable solution, bearing in mind the main characteristics of the presented DAG-based solutions.

8. Conclusions

ZSM networks are expected to lead the way toward the development of self-managed and self-optimized networks to form NGNs. The increased automation, in combination with the minimum human intervention, increases the performance of the network and at the same time exposes several security concerns. The current research examined the use of blockchain to tackle the security issues of the ZSM framework. The proposed blockchain architecture was found to address these security issues which further encouraged our interest in selecting the appropriate blockchain/platform on which such a solution would be implemented (to guide prospective implementers). In this course, we defined the selection criteria and examined the representative set of platforms. The conclusion was that for all of them, a modification will be needed as none meeting all the criteria was found. Although blockchain introduces valuable characteristics such as the ability to form a network of trust in a trustless environment without the existence of a trusted third party, the immutability of the data recorded as validated transactions in the ledger and the traceability feature, no technology is weakness-free. There are some drawbacks in this technology, which should be carefully considered during the design of the blockchain-based solution and deserve further research: (a) scalability is one of the main drawbacks of this technology since transactions written in the ledger cannot be deleted afterward; (b) the transaction validation time affects the dynamicity the network can support and mostly depends on the consensus mechanism used in the blockchain software [37,38]; (c) the support of tokens is

also anticipated to add value in this environment for trading the resources. Moreover, the use of cryptocurrency could lead to the development of a modern marketplace where NPs could rent, buy or lease resources using the ZSM framework in a secure manner.

Author Contributions: Conceptualization, M.X. and H.C.L.; methodology, H.C.L.; investigation, M.X.; resources, M.X., D.G.K. and P.A.K.; writing—original draft preparation, M.X.; writing—review and editing, D.G.K., P.A.K. and H.C.L.; visualization, M.X.; supervision, H.C.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are available upon request. Please contact the authors for further information.

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

References

1. Saadon, G.; Haddad, Y.; Simoni, N. A survey of application orchestration and OSS in next-generation network management. *Comput. Stand. Interfaces* **2019**, *62*, 17–31. [CrossRef]
2. Medhat, A.M.; Taleb, T.; Elmangoush, A.; Carella, G.A.; Covaci, S.; Magedanz, T. Service function chaining in next generation networks: State of the art and research challenges. *IEEE Commun. Mag.* **2016**, *55*, 216–223. [CrossRef]
3. García-Otero, M.; Zahariadis, T.; Alvarez, F.; Leligou, H.C.; Población-Hernández, A.; Karkazis, P.; Casajús-Quirós, F.J. Secure geographic routing in ad hoc and wireless sensor networks. *EURASIP J. Wirel. Commun. Netw.* **2010**, *2010*, 1–12. [CrossRef]
4. Unleashing a New Breed of 5G Services: A 2021 Ecosystem Makeover. Available online: https://www.forbes.com/sites/forbestechcouncil/2021/03/01/unleashing-a-new-breed-of-5g-services-a-2021-ecosystem-makeover/?sh=643358bc4c83 (accessed on 20 September 2022).
5. How the Cloud Telecommunications Revolution Changes Business. Available online: https://www.forbes.com/sites/googlecloud/2021/06/21/how-the-cloud-telecommunications-revolution-changes-business/?sh=713312351ecb (accessed on 25 September 2022).
6. Cloud Players Reshape Telecom's Landscape—Industry Voices-Walker. Available online: https://www.fiercetelecom.com/telecom/cloud-players-reshape-telecom-s-landscape-industry-voices-walker (accessed on 27 September 2022).
7. Drampalou, S.F.; Miridakis, N.I.; Leligou, H.C.; Karkazis, P.A. A Survey on Optimal Channel Estimation Methods for RIS-Aided Communication Systems. *Signals* **2023**, *4*, 208–234. [CrossRef]
8. Prekas, S.; Karkazis, P.; Nikolakakis, V.; Trakadas, P. Comprehensive Comparison of VNE Solutions Based on Different Coordination Approaches. *Telecom* **2021**, *2*, 390–412. [CrossRef]
9. Barakabitze, A.A.; Barman, N.; Ahmad, A.; Zadtootaghaj, S.; Sun, L.; Martini, M.G.; Atzori, L. QoE management of multimedia streaming services in future networks: A tutorial and survey. *IEEE Commun. Surv. Tutor.* **2019**, *22*, 526–565. [CrossRef]
10. Chen, X.; Li, Z.; Zhang, Y.; Long, R.; Yu, H.; Du, X.; Guizani, M. Reinforcement learning–based QoS/QoE-aware service function chaining in software-driven 5G slices. *Trans. Emerg. Telecommun. Technol.* **2018**, *29*, e3477. [CrossRef]
11. Mahmoud HH, H.; Amer, A.A.; Ismail, T. 6G: A comprehensive survey on technologies, applications, challenges, and research problems. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4233. [CrossRef]
12. Shahraki, A.; Abbasi, M.; Piran, M.; Taherkordi, A. A comprehensive survey on 6G networks: Applications, core services, enabling technologies, and future challenges. *arXiv* **2021**, arXiv:2101.12475.
13. Yang, G.; Shin, C.; Yoo, Y.; Yoo, C. A Case for SDN-based Network Virtualization. In Proceedings of the 2021 29th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommu-nication Systems (MASCOTS), Houston, TX, USA, 3–5 November 2021; pp. 1–8. [CrossRef]
14. Alam, I.; Sharif, K.; Li, F.; Latif, Z.; Karim, M.M.; Biswas, S.; Nour, B.; Wang, Y. A survey of network virtualization techniques for Internet of Things using SDN and NFV. *ACM Comput. Surv.* **2020**, *53*, 1–40. [CrossRef]
15. Industry Specification Group (ISG); Zero Touch Network and Service Management (ZSM). Available online: https://www.etsi.org/committee/zsm (accessed on 10 October 2022).
16. Xevgenis, M.G.; Kogias, D.; Leligou, H.C.; Chatzigeorgiou, C.; Feidakis, M.; Patrikakis, C.Z. A Survey on the Available Blockchain Platforms and Protocols for Supply Chain Management. In Proceedings of the IOT4SAFE@ ESWC, Herakleion, Greece, 2 June 2020.
17. State of Dapps. Available online: https://www.stateofthedapps.com/ (accessed on 20 October 2022).
18. IBM Food Trust: A New Era in the World's Food Supply. Available online: https://www.ibm.com/blockchain/solutions/food-trust (accessed on 25 October 2022).
19. CargoX. Available online: https://cargox.io/ (accessed on 5 November 2022).
20. Farmers World. Available online: https://farmersworld.io/?utm_source=DappRadar&utm_medium=deeplink&utm_campaign=visit-website (accessed on 5 November 2022).

21. ETSI GR ZSM. General Security Aspects. In *Zero-Touch Network and Service Management (ZSM)*; Technical Report; Zero-touch network and Service Management (ZSM); ETSI Industry Specification Group (ISG); Sophia Antipolis Cedex: Valbonne, France, 2021.
22. Dalgkitsis, A.; Mekikis, P.V.; Antonopoulos, A.; Kormentzas, G.; Verikoukis, C. Dynamic Resource Aware VNF Placement with Deep Reinforcement Learning for 5G Networks. In Proceedings of the GLOBECOM 2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020; pp. 1–6.
23. Uzunidis, D.; Karkazis, P.; Roussou, C.; Patrikakis, C.; Leligou, H.C. Intelligent Performance Prediction: The Use Case of a Hadoop Cluster. *Electronics* **2021**, *10*, 2690. [CrossRef]
24. Subramanya, T.; Riggio, R. Centralized and federated learning for predictive VNF autoscaling in multi-domain 5G networks and beyond. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 63–78. [CrossRef]
25. Boudi, A.; Bagaa, M.; Pöyhönen, P.; Taleb, T.; Flinck, H. AI-based resource management in beyond 5G cloud native environment. *IEEE Netw.* **2021**, *35*, 128–135. [CrossRef]
26. Short, A.; Leligou HCTheocharis, E.; Papoutsidakis, M. Using blockchain technologies to improve security in Federated Learning Systems. In Proceedings of the IEEE COMPSAC (Conference on Computers, Software and Applications), Madrid, Spain, 13–17 July 2020. [CrossRef]
27. Carrozzo, G.; Siddiqui, M.S.; Betzler, A.; Bonnet, J.; Perez, G.M.; Ramos, A.; Subramanya, T. AI-driven ze-ro-touch operations, security and trust in multi-operator 5G networks: A conceptual architecture. In Proceedings of the 2020 European Conference on Networks and Communications (EuCNC), Dubrovnik, Croatia, 15–18 June 2020; pp. 254–258.
28. Theodorou, V.; Lekidis, A.; Bozios, T.; Meth, K.; Fernández-Fernández, A.; Tavlor, J.; Diogo, P.; Martins, P.; Behravesh, R. Blockchain-based Zero Touch Service Assurance in Cross-domain Network Slicing. In Proceedings of the 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Porto, Portugal, 8–11 June 2021; pp. 395–400.
29. Benzaid, C.; Taleb, T. AI-driven zero touch network and service management in 5G and beyond: Challenges and research directions. *IEEE Netw.* **2020**, *34*, 186–194. [CrossRef]
30. Benzaïd, C.; Taleb, T.; Farooqi, M.Z. Trust in 5G and beyond networks. *IEEE Netw.* **2021**, *35*, 212–222. [CrossRef]
31. Liyanage, M.; Pham, Q.V.; Dev, K.; Bhattacharya, S.; Maddikunta, P.K.R.; Gadekallu, T.R.; Yenduri, G. A survey on Zero touch network and Service (ZSM) Management for 5G and beyond networks. *J. Netw. Comput. Appl.* **2022**, *203*, 103362. [CrossRef]
32. Standish, R.K. Concept and definition of complexity. In *Intelligent Complex Adaptive Systems*; IGI Global: Hershey, PA, USA, 2008; pp. 105–124.
33. Gallego-Madrid, J.; Sanchez-Iborra, R.; Ruiz, P.M.; Skarmeta, A.F. Machine learning-based zero-touch network and service management: A survey. *Digit. Commun. Netw.* **2021**, *8*, 105–123. [CrossRef]
34. ETSI GS ZSM. Reference Architecture. In *Zero-Touch Network and Service Management (ZSM)*; Techical Report; ETSI Industry Specification Group (ISG); Sophia Antipolis Cedex: Valbonne, France, 2019.
35. Siriwardhana, Y.; Porambage, P.; Liyanage, M.; Ylianttila, M. AI and 6G security: Opportunities and challenges. In Proceedings of the 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Porto, Portugal, 8–11 June 2021; pp. 616–621.
36. Zeng, Z.; Zhang, X.; Xia, Z. Intelligent Blockchain-Based Secure Routing for Multidomain SDN-Enabled IoT Networks. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 5693962. [CrossRef]
37. Xevgenis, M.; Kogias, D.G.; Karkazis, P.; Leligou, H.C.; Patrikakis, C. Application of Blockchain Technology in Dynamic Resource Management of Next Generation Networks. *Information* **2020**, *11*, 570. [CrossRef]
38. Xevgenis, M.; Kogias, D.G.; Christidis, I.; Patrikakis, C.; Leligou, H.C. Evaluation of a Blockchain-Enabled Resource Management Mechanism for NGNs. *Int. J. Netw. Secur. Appl.* **2021**, *13*, 1–16. [CrossRef]
39. Yang, G.; Lee, K.; Lee, K.; Yoo, Y.; Lee, H.; Yoo, C. Resource Analysis of Blockchain Consensus Algorithms in Hyperledger Fabric. *IEEE Access* **2022**, *10*, 74902–74920. [CrossRef]
40. Thakkar, P.; Nathan, S.; Viswanathan, B. Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform. In Proceedings of the 2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Tele-communication Systems (MASCOTS), Milwaukee, WI, USA, 25–28 September 2018; pp. 264–276. [CrossRef]
41. Hyperledger Fabric Documentation: Latest Release 25 January 2023. Available online: https://hyperledger-fabric.readthedocs.io/_/downloads/vi/latest/pdf/ (accessed on 28 January 2023).
42. Consensys Quorum. Available online: https://consensys.net/quorum/ (accessed on 10 March 2023).
43. R3 Corda. Available online: https://www.r3.com/products/corda/ (accessed on 1 February 2023).
44. Sealey, N.; Aijaz, A.; Holden, B. IOTA Tangle 2.0: Toward a Scalable, Decentralized, Smart, and Autonomous IoT Ecosystem. In Proceedings of the 2022 International Conference on Smart Applications, Communications and Networking (SmartNets), Palapye, Botswana, 29 November–1 December 2022; pp. 1–8.
45. Hedera How It Works. Available online: https://hedera.com/how-it-works (accessed on 3 February 2023).
46. Gorenflo, C.; Lee, S.; Golab, L.; Keshav, S. FastFabric: Scaling hyperledger fabric to 20,000 transactions per second. *Int. J. Netw. Manag.* **2020**, *30*, e2099. [CrossRef]
47. Baliga, A.; Subhod, I.; Kamat, P.; Chatterjee, S. Performance evaluation of the quorum blockchain platform. *arXiv* **2018**, arXiv:1809.03421.
48. Corda: A Distributed Ledger. Available online: https://www.r3.com/blog/corda-technical-whitepaper/ (accessed on 28 January 2023).
49. IOTA Smart Contracts. Available online: https://wiki.iota.org/shimmer/smart-contracts/overview/ (accessed on 2 February 2023).

50. IOTA Oracles. Available online: https://blog.iota.org/introducing-iota-oracles/ (accessed on 2 February 2023).
51. What Is Chainlink: A Beginner's Guide. Available online: https://blog.chain.link/what-is-chainlink/?_ga=2.209069778.1120344513.1675428709-842934195.1673628852 (accessed on 3 February 2023).