applied sciences

MDPI

Article

Internet of Things Aware Secure Dew Computing Architecture for Distributed Hotspot Network: A Conceptual Study

Partha Pratim Ray [1,*,†] **and Karolj Skala** [2,†]

[1] Department of Computer Applications, Sikkim University, Gangtok 737102, India
[2] Center for Informatics and Computing Science, Ruđer Bošković Institute, 10000 Zagreb, Croatia
* Correspondence: parthapratimray1986@gmail.com or ppray@cus.ac.in
† The authors are IEEE Dew Computing STC members.

Abstract: Building a widely distributed hotspot network is a very tedious task due to its complexity. Providing security, fully distributed network services, and a cost-conscious impact are the major challenges behind this goal. To overcome these issues, we have presented a novel distributed hotspot network architecture with five layers that can provide large-scale hotspot coverage as an assimilated result. Our contributions to this new architecture highlight important aspects. First, scalability can be increased by including many Internet of Things (IoT) devices with sensors and Wi-Fi and/or LoraWAN connectivity modules. Second, hotspot owners can rent out their hotspots to create a distributed hotspot network in which the hotspots can act as an ordinary data gateway, a full-fledged hotspot miner, and a light-weight hotspot miner to earn crypto tokens as rewards for certain activities. Third, the advantages of Wi-Fi and LoraWAN can be seamlessly leveraged to achieve optimal coverage, higher network security, and suitable data transmission rate for transferring sensor data from IoT devices to remote application servers and users. Fourth, blockchain is used to enhance the decentralized behavior of the architecture that is presented here by providing immutability and independence from a centralized regulator and making the network architecture more reliable and transparent. The main feature of our paper is the use of the dew-computing paradigm along with hotspots to improve availability, Internet backhaul-agnostic network coverage, and synchronous update capability, and dew-aware leasing to strengthen and improve coverage. We also discuss the key challenges and future roadmap that require further investment and deployment.

Keywords: dew computing; Internet of Things; blockchain; hotspot network

Citation: Ray, P.P.; Skala, K. Internet of Things Aware Secure Dew Computing Architecture for Distributed Hotspot Network: A Conceptual Study. *Appl. Sci.* **2022**, *12*, 8963. https://doi.org/10.3390/app12188963

Academic Editor: Fabio La Foresta

Received: 3 August 2022
Accepted: 3 September 2022
Published: 6 September 2022

1. Introduction

The world has witnessed several technological advances, especially in the areas of pervasive computing, ubiquitous computing, security, and open-source hardware (OSH) development [1–3]. Since its inception, IoT has experienced tremendous growth in all application areas such as agriculture, industry, automation, smart city, and healthcare [1,4–6]. Every time an IoT device collects sensor data from a physical entity, it requires a gateway or Internet connection to transmit this data to the remote applications and users. This results in huge network traffic and a degradation of the network's backhaul dependency. Apart from this, the extensive use of IoT sensor data for transmission over long distances incurs costs and is associated with significant power consumption [7–9]. In the absence of a suitable network technology, IoT sensor data might be limited to the near periphery from which it originates. As a result, the quality of service is minimized, and the reliability is neglected. As a result, the entire IoT ecosystem evolves into an unstable concept where IoT sensor data is not always available to remote applications. Existing Internet backhaul and cloud computing-centric approaches are mainly responsible for such obstacles.

Standalone hotspots are regularly used in our daily life [10,11]. Normally, a cell phone with subscriber network connectivity and available data packets can be seamlessly used as a

mobile hotspot for other interested devices that are nearby to access the Internet. It becomes problematic when the hotspot that an interested user's device is trying to connect to has no network coverage or is out of subscription, limiting the ability to break the coverage of the hotspot for the interested device [12,13]. This calls into question the usability, quality of service, and reliability of such hotspots.

Dew computing is a recent development in computing that aims to leverage in-network dependencies and collaborative approaches for remote cloud servers [14–16]. Dew servers are such devices that follow the dew computing idea and perform needed activities such as data access to local machines that are independent of network availability [17]. Dew computing is based on the principles of the synchronization function, which allows such dew devices to operate locally and require very little Internet connection to synchronize with their cloud replica [18–20]. In dew computing, each user has a cloud replica with a local clone of the same content. At the time of writing, dew computing is still in its early stages and thus focuses mainly on services that are related to network data access for its end devices [21]. However, the long-term goal of dew computing is to provide higher reliability, better availability, and user-centric data access, as well as a provider that is primarily independent of Internet connectivity.

Distributed hotspot networks are an idea that has been discussed for a long time and has received increasing attention in both the industry and in academia in recent years. However, to date, no such fully self-organizing distributed hotspot network exists, either in research or in practice [22]. The idea of using Wi-Fi as an enabler for hotspot deployment is currently under investigation [23]. However, Wi-Fi struggles with limited range, signal interference, bandwidth usage, and security [24]. Using Wi-Fi on a large number of IoT devices may pose various challenges in terms of power consumption, which may shorten the battery life of IoT devices [25]. On the other hand, LoraWAN can be considered as an alternative to Wi-Fi to provide wide-area connectivity with improved security and battery life for IoT devices [25,26]. However, it faces problems such as having a low data rate, a small packet size, and an unsuitability for real-time applications. In addition, it is believed that a person who wants to provide their hotspot as a gateway for IoT devices may face the challenge presented by paid subscriptions, which may prevent them from providing their hotspot device to an unknown IoT device. When an IoT device wants to connect to the hotspot of an unknown person in a nearby coverage area, authentication and security become the most important factors. Security and authentication issues can be solved by incorporating blockchain and appropriate crypto tokens that perform as incentives for hotspot owners. Blockchain is an immutable, decentralized technology that aims to provide inherent security for the stored data and access by nodes (miners and validators) that are with or without authorization [27,28]. In this way, a complete business model can be formulated where a distributed hotspot network can be developed that operates in a fully decentralized manner and offers incentives to hotspot owners to rent out their hotspots to serve IoT devices in the vicinity [29–31].

In this paper, we present a novel idea for an IoT-based, secure, distributed hotspot network to solve the existing problems in creating and deploying a hotspot network that has the potential to succeed as a business model. The main contributions of this work can be summarized as follows:

- Using IoT devices as sensor data generators under the supervision of nearby hotspots that may be unknown to these IoT devices.
- The architecture presented here is a distributed hotspot architecture that can be assimilated with many IoT devices to scale the data generation process.
- The presented architecture can leverage highly secure and authenticated hotspot network coverage by using blockchain.
- The whole concept behind the architecture is to use a decentralized approach for the connected hotspot devices that can act as distributed gateways.
- Such hotspots can earn crypto tokens as rewards for certain activities such as data transmission, coverage stability, validation, and mining.

- Authentication and security-enabled hotspot networks can span several miles without requiring existing cellular networks.
- Dew computing is integrated into hotspot devices to provide increased computing power and capacity that are independent of the Internet backhaul.
- By deploying dew servers in the hotspots, they can be configured to become full-fledged, lightweight, data-only hotspots.
- The hotspots that are presented here can perform mining, validation, IoT data coverage, and crypto token collection from the blockchain.
- Remote users and application servers can be connected to such secure, authentication-enabled incentive hotspot networks, through which distributed IoT devices can transmit sensor data over long distances.
- In this design, IoT devices can be equipped with Wi-Fi and/or LoraWAN antenna modules that can be reasonably deployed according to the data transmission needs (low or high) and distance requirements.
- The presented architecture can open a new business model where hotspot owners can earn crypto tokens from their hotspots to reduce subscription and operational costs and make the whole network ecosystem sustainable.

The concept paper is organized as follows. Section 2 discusses the related work. Section 3 presents the background idea on various technologies that are used to develop a secure and distributed hotspot network. Section 3 provides a detailed description of the novel architecture. Section 4 concludes this paper with a discussion, the important challenges, future work, and a conclusion.

2. Related Work

We performed an extensive literature search to find the related work that is relevant to our work. We searched IEEE Xplore and Google Scholar to find most of the related articles in this section. We note that none of the works relate to the dew computing paradigm for solving the new dimensions of the distributed hotspot network formation. The majority of the articles do not consider IoT devices as part of their models. None of the articles discuss the integration of LoraWAN into the hotspot network. For example, Zha et al. [32] discuss blockchain-based energy distribution with detailed policies, but this discussion lacks a detailed process for forming a distributed hotspot network. Zhao et al. [33] do not address the hotspot aspects in the design of blockchain-based distributed networks. Messié et al. [34] use blockchain with hotspots to build the BALAdIN framework for multi-actor access network formation without providing clear guidance for designing the distributed hotspot networks.

Lopez et al. [35] discuss choice-based modeling of a distributed network on top of the federated learning, but the way is paved for the distributed nature of hotspots. Janiesch et al. [36] show a Wi-Fi sharing architecture with a payment channel formation, but this does not show the distributed behavior of the underlying hotspots. Yang et al. [37] use a pricing mode for paving the wireless caching reward with a cache content dispersion mechanism. Zhao et al. [38] show the energy transaction mechanism with an energy trading facility, however no study is performed for the hotspot distributed network creation. Kim et al. [39] present a Wi-Fi security model by using smart contract to safeguard it from Wi-Fi vulnerability. Ivanov et al. [40] design a smart Wi-Fi architecture by using a Hansa handshaking procedure and perform payments via crypto token. However, it does not consider the dew computing aspects. Pustišek et al. [41] present a low-bandwidth distributed application framework where a LoraWAN-aware inclusion scheme is not discussed. Ma et al. [42] perform a security analysis on top of Android data cloning, where an evaluation is made, without involving the blockchain. Table 1 presents the comparison of related works.

Table 1. Comparative analysis of related works.

Paper	Blockchain	IoT	Hotspot	Wi-Fi	LoraWAN	Dew Computing	Key Contributions	Limitations
Zha et al. [32]	Yes	No	Yes	Partial	Partial	No	Blockchain aware energy, review, policy recommendations, applications;	Lacks hotspot network design approach
Zhao et al. [33]	Yes	Partial	No	No	No	No	Blockchain distributed network design aspects, traceable, tamper-proof design;	Hotspot discussion is minimal
Messié et al. [34]	Yes	No	Yes	Partial	No	No	BALAdIN framework, multi-actor access network;	No clear direction on distributed hotspot
Lopez et al. [35]	Yes	No	No	Partial	No	No	Choice modeling, federated learning, distributed privacy-aware design;	No analysis about distributed model is made
Janiesch et al. [36]	Yes	No	Yes	Yes	No	No	Wi-Fi sharing architecture, payment channel networking, evaluation of architecture;	Distributed behavior not analyzed
Yang et al. [37]	Yes	No	Partial	Partial	No	No	Pricing mode, wireless caching reward, cache quality, cache content dispersion;	Hotspot distributed network not covered
Zhao et al. [38]	Yes	No	Partial	No	No	No	Energy transaction, multi-microgrid, energy trading;	Hotspot aware design lacks
Kim et al. [39]	Yes	No	Partial	Yes	No	No	Wi-Fi security model, secure models using smart contracts to safeguard Wi-Fi vulnerability;	Distributed hotspot discussion missing
Ivanov et al. [40]	Yes	Partial	Yes	Yes	No	No	Smart Wi-Fi architecture, Hansa handshake/service, smart contract, payment, refunds, security analysis;	Hotspot distributed-ness lacks
Pustišek et al. [41]	Yes	Yes	Yes	Yes	No	No	Low-bandwidth distributed applications framework (LDAF) architecture, distributed model;	Consensus algorithm no specified, no scalability
Ma et al. [42]	No	No	Yes	Yes	No	No	Security risk analysis, android data cloning, Evaluation;	No blockchain involved
Our Model	Yes	Yes	Yes	Yes	Yes	Yes	Distributed hotspot architecture design, blockchain aware secure IoT device data transmission, dew computing inclusion, scalable, incentive.	Implementation needed

Our Key Contributions

Our contributions are new with respect to the related works that are presented in this section, as follows.

- We use a dew computing paradigm that can provide independence on the integrated hotspot nodes. Doing so, our architecture can work on a rental basis where an actual hotspot network can be formed in a purely distributed manner. Dew computing uses high reliable synchronization techniques that help the connected devices to use the network even when a given dew system is not able to process the connected device's

request. Dew computing can form *dewlets* that support the rental facility of the network coverage from nearby hotspots to enrich the availability and overall quality of the service.
- Dew server-based hotspots can act as miner and validators to facilitate the generation of the reliability factors of the blockchain network. Based on the PoC challenge, once a hotspot miner or validator solves the challenge, it can establish the reliability. The hotspot miner, upon completion of certain PoC and data transmission activities, can earn crypto token which can be reflected in the wallets of the respective hotspot owners.
- Our architecture uses IoT-based devices as the data collecting nodes that are able to send the data to remote application servers or users to facilitate the visualization and monitoring of related tasks. Millions of IoT devices can be integrated with the presented architecture to improve their scalability.
- Our architecture is able to cope up with standard IEEE 802.1X authentication, which works on top of the IEEE 802.11u standard. This ensures a secure and more effective authentication process.

3. Background

In this section, we discuss the IoT, dew computing, blockchain, and hotspot technologies to understand how they work and their existing issues.

3.1. Internet of Thing (IoT)

IoT describes a set of physical or digital objects that communicate via the Internet or similar communication technologies [43–45]. Such objects are referred to as "things", which are usually equipped with sensors, actuators, processing power, memory, and software to perform the required tasks [46–48]. The applications of IoT are very diverse and range from smart heating, smart agriculture, smart automation, smart military, smart industry, smart city, smart horticulture, smart building, smart consumer applications, smart health monitoring, and smart supply chain management [49,50]. As the number of IoT devices is rapidly increasing, several governmental and international agencies are involved in developing policies, regulatory guidelines, and related standards [51].

IoT ecosystems are enabled by various communication and networking technologies: (i) short-range: e.g., Bluetooth, near-field communication, Wi-Fi, Z-Wave, and radio frequency identification (RFID); (ii) medium-range: e.g., ZigBee and LTE-advanced; (iii) long-range: e.g., cellular, satellite communication, and low-power wide-area networks. Wired alternatives such as Ethernet, fiber, and powerline communications (PLC) can be complemented with existing IoT infrastructure [52,53]. The IoT also supports heterogeneity and addressability. Despite the tremendous prospects, IoT suffers from the problems of platform fragmentation, privacy, autonomy, data storage, security, design, a negative environmental impact, and control mechanisms.

3.2. Blockchain

A blockchain refers to a growing list of blocks that are cryptographically linked together. Typically, a block consists of transaction data (in the form of a Merkle tree), block height, timestamp, cryptographic hash of the associated block, and nonce [54]. Other key components such as the threshold signature of an existing consensus group may be included in each of the blocks. Blockchains are managed by a peer-to-peer network, and typically, each node of the blockchain contains a distributed ledger [55]. These nodes adhere to the same network protocol for communicating with other nodes in the blockchain and for validating new blocks. Blockchains are inherently immutable and decentralized, and have very high fault tolerance [56,57]. Mining is the most important task of a blockchain. In general, a mining node can solve a puzzle (mathematical problem) to get a chance to add a new block as the next block to the blockchain. Thus, a miner can earn crypto tokens as a reward. They can also get a certain amount from the transaction fee for all transactions in that block [58]. The main goal of a mining node is to ensure the reliability of the work that is performed on the blockchain network by using a consensual protocol such as Proof

of Work (PoW) and Proof of Stake (PoS) [59]. The mining process can be performed in the form of a pool of miners, and in pool mining, the chance of crypto reward is higher than it is in single mining. On the other hand, the validation task is performed by a validator node in the blockchain network, which is involved in disseminating messages to almost all nodes. Sometimes, the validators can take over the mining task seamlessly [60]. Usually, an epoch is set in which a certain group of validators is selected to act as a consensus group. At the end of each epoch, a new group of validators is selected to act as a new consensus group for validating the new blocks. Generally, rewards are distributed per block or per epoch via a specific reward transaction. Various types of transactions are possible in a blockchain, some of which are: Gateway addition, location confirmation, chain variable, data credit, multiple payment, rotation, consensus algorithm execution, opening or closing state channels, and security exchange [61,62].

There are four types of blockchains: (i) public: here there are no access restrictions, a node following a standard blockchain communication protocol can act as a validator and send transactions to other such nodes with Internet connectivity; (ii) private; (iii) hybrid: this is a combination of public and private blockchain functions; (iv) sidechains: this is an independent blockchain that can run in parallel with the main blockchain by connecting sidechains in both directions and by communicating with the main blockchain [63,64]. Major applications of blockchain include cryptocurrencies, smart contracts, financial services, online games, supply chain management, domain names, and voting. Blockchains can interact with other blockchain systems to transfer digital assets.

3.3. Dew Computing

Dew computing provides a new way for end users (dew users) to connect to cloud-based content without relying on the Internet backhaul [65]. It enables an exciting idea where a dew user can access cloud-based data using their own dew device without requiring minimal intervention from the Internet connection. Dew users can access the same content as a local copy of the cloud content [66,67]. Once the Internet connection is restored, the changes are homogenized between the local and cloud content. This minimizes the dependency that is on the cloud, where an end user needs an Internet connection every time they want to access the cloud data. Actually, dew computing aims to solve the problems of offline access to data in the existing cloud computing paradigm [68]. Traditional cloud content and configurations are far from user self-control, as such services are provided exclusively at the enterprise level. Dew computing enables users to match endpoint capabilities with cloud services in a more reliable approach [69]. It depends on two aspects: (i) independence: a local dew device can operate independently of cloud services, and (ii) collaboration: a local dew device can communicate with cloud services when Internet connectivity is available, or when synchronization is desired. A dew virtual machine (DVM) is required on the user's dew device, which can take the help of a dew server, a data analytics server, and a dew device decision-making approach [70]. Dew computing can provide multiple services that are equivalent to cloud computing, such as data in dew, platform in dew, infrastructure in dew, web in dew, software in dew, storage in dew, and database in dew [71]. Studies show that dew computing-assisted drones [72] and a federated learning-based blockchain can be useful in IoT-aware drone employments [73].

The main advantages of dew computing over Cloud, Fog, or Edge computing paradigms can be summarized as follows: (i) negligible latency, (ii) negligible jittering effects, (iii) highly location-aware behavior, (iv) highly distributed geolocated services, (v) very low probability of data redirection attacks, (vi) targets mobile users, (vii) requires limited resources or hardware capacity, (viii) very high-quality user experience, (ix) very low Internet dependency, (x) high delay tolerance, and (xi) very high computing power [74,75].

The dew computing paradigm is seen as an extension of the cloud computing scenario, but at the extreme edge of the network, the end users can directly access the Internet [76]. It follows a strict computing hierarchy when it cannot provide the required services to the end users. A dew image for the user-owned cloud repository can be used in the user-owned

dew system [77]. Therefore, synchronization plays an important role in dew computing. Process synchronization with a timestamp can be very useful for dew computing users. The functions of data replication and distribution-oriented transparency can be easily complemented by Internet access to dew computing data. In case of local data loss, there is a great chance to recover the same data from the cloud storage. In addition, rule-based data collection, scalability, and high reliability are important aspects of dew computing that provide a minimalist approach to the Internet backhaul, so that the user experience can be greatly improved [78]. Dew data rental services can be offered between dew devices that are in close proximity, allowing a dew user to access Internet data even if their personal Internet data is unavailable or restricted for some reason. In this way, dew computing can serve as a hotspot network entity.

3.4. Hotspot

In general, a hotspot is a physical location where users can access the Internet. Typically, Wi-Fi technology is used to connect a Wi-Fi router that is connected to an Internet service provider (ISP) via an Ethernet or a wireless local area network (WLAN) to a device. Hotspots can be both public and private [79–81]. Public hotspots are established and maintained by businesses or government agencies for use by the public, especially at bus stops, train stations, libraries, hospitals, supermarkets, and university buildings. Private hotspots are usually set up in hotels, restaurants or cafés. Public hotspots are usually served by wireless access points (WAPs) that are configured for Internet access. These WAPs are controlled and managed by local authorities. A facility that has broadband or fibre Internet access can provide wireless Internet access through the WAPs [82–84]. These WAPs are connected to routers or gateways that provide seamless Internet connectivity. Figure 1 presents generic structure of Wi-Fi hotspots.

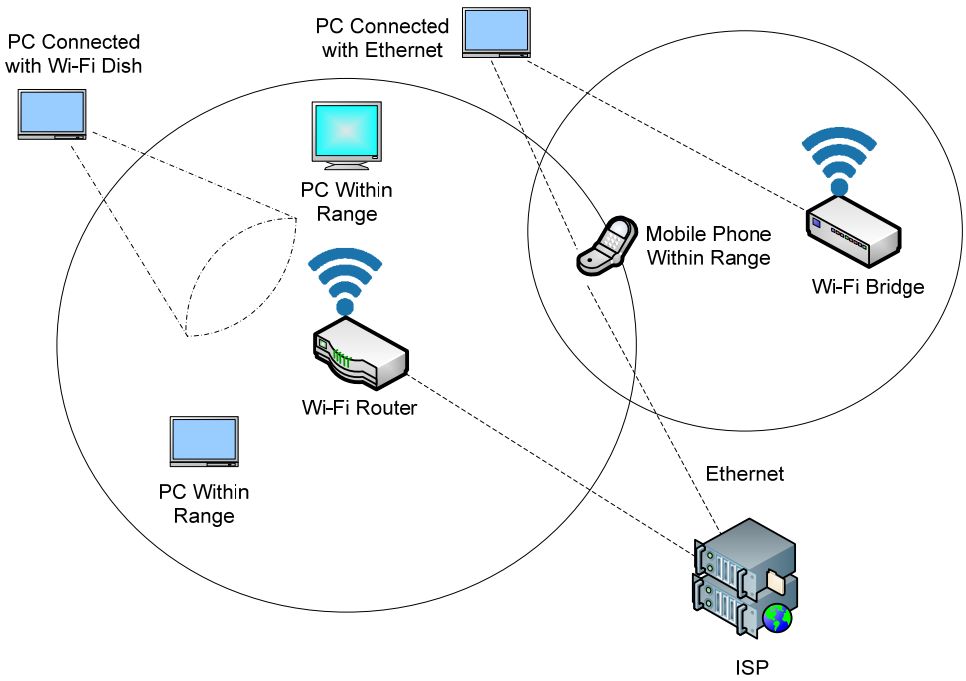

Figure 1. Generic structure of Wi-Fi hotspots.

3.4.1. Tethering

A private hotspot can be created, configured, and managed using tethering. Tethering uses a phone as a modem (PAM) that shares the phone's (device's) Internet connection with authorized (by password or pin number) nearby devices such as computers, smartphones, tablets, and notebooks. The connection in tethering is established via a physical cable connection (e.g., a USB cable), Bluetooth, or WLAN-based Wi-Fi technologies. Nowadays,

tethering is done via WLAN, which is called a mobile hotspot. Such mobile hotspots can serve as both dynamic and portable routers for Internet access. Most operating systems for mobile devices (Windows 6.5 or higher, Android 2.2 or higher, iOS 3.0 or higher) support this feature. These smart devices are equipped with the necessary software and hardware to enable wireless Internet access [85,86]. Tethering over Wi-Fi is also referred to as a personal hotspot. Tethering can also be done via Network Address Translation (NAT) that is based on the existing Internet connection of the mobile device. Such NAT is used for IPv4 networks where the mobile device has a single IPv4 address, but multiple devices can be identified with such a network address.

3.4.2. Hotspot Varieties

Hotspots may be operated in open, public network spaces as free or closed public networks with a central hotspot management system that is operated by a local authority. Hotspots can be operated commercially, requiring users to authenticate or pay before using the Internet data [87]. Software-enabled access points (SoftAP) are one such type of hotspot that can be used in a computer or cell phone to turn it into a virtual router. SoftAP can be used to configure Wi-Fi enabled devices (e.g., IoT devices) that do not have a display or other inputs. There are two major challenges in doing this: (i) manually connecting to the SoftAP network, and (ii) if the passkey is lost or one is given the wrong passkey, the disconnected device is almost irretrievably unavailable for further use of the SoftAP network.

3.4.3. Hotspot 2.0

Hotspot 2.0 is also known as Passpoint (Wi-Fi certified), which can be used to access Wi-Fi and Wi-Fi Alliance. The purpose of Hotspot 2.0 is to allow the Wi-Fi-enabled mobile device to automatically connect to a Wi-Fi subscriber when the mobile device moves into the Hotspot 2.0 region [88,89]. In this way, a better on-demand service is provided to the mobile devices. In addition, a scenario for better bandwidth utilization can be developed, where the load on the network operator's infrastructure is reduced to minimize network traffic. Hotspot 2.0 is based on the IEEE 802.11u standard to enable cellular-like roaming. A mobile device that is supported by IEEE 802.11u and subscribed to Hotspot 2.0 can automatically join the network and roam accordingly [90]. A dynamic fairness model is used to charge for the use of the Internet connection in this context. A user priority list is recommended to charge for Internet usage based on time criticality and network traffic types (e.g., audio, video, and data). Hotspot 2.0 is deployed, based on the IEEE 802.11u standard, which defines a formulation for a terminal device to receive WLAN-related information. Hotspot 2.0 consists of some key elements, such as: (i) a terminal device (STA) that supports WPA2, Hotspot 2.0, 802.1X, and Access Network Query Protocol (ANQP); (ii) an access point (AP): the Hotspot 2.0 supports WPA2-801.1X and acts as an ANQP server, and it can send Hotspot 2.0 network information to the connected STAs; (iii) an access controller (AC) that supports 802.1X configuration between the Aps in stacks; (iv) an AAA server: it supports various encryptions such as the Extensible Authentication Protocol (EAP) authentication and key agreement (AKA)/subscriber identification module (SIM), Transport Layer Security (LTS), Tunneled Transport Layer Security (TTLS), and it can also obtain authentication vectors from the Home Location Register (HLR); (vi) BOSS: it provides important operational support as an end-to-end business provider to perform regular customer-facing tasks such as billing, rating, and general service.

Network discovery and selection is an important job of Hotspot 2.0. It is formulated as follows. The network discovery service needs the packet exchange between the end STA module and the access point. An end STA module can perform active and passive scans. Both scans can take place parallelly. The STA device must have pre-registration with a home network, with pre-configured network cards, certificates, a username, and a password. An organization identifier (OI) is very important for the working of the STA module. An STA module can communicate with roaming WLAN, however, in that case,

the roaming WLAN must have been pre-registered and configured with the home network where which, the STA is located [91]. Figure 2 presents the generic structure of Hotspot 2.0.

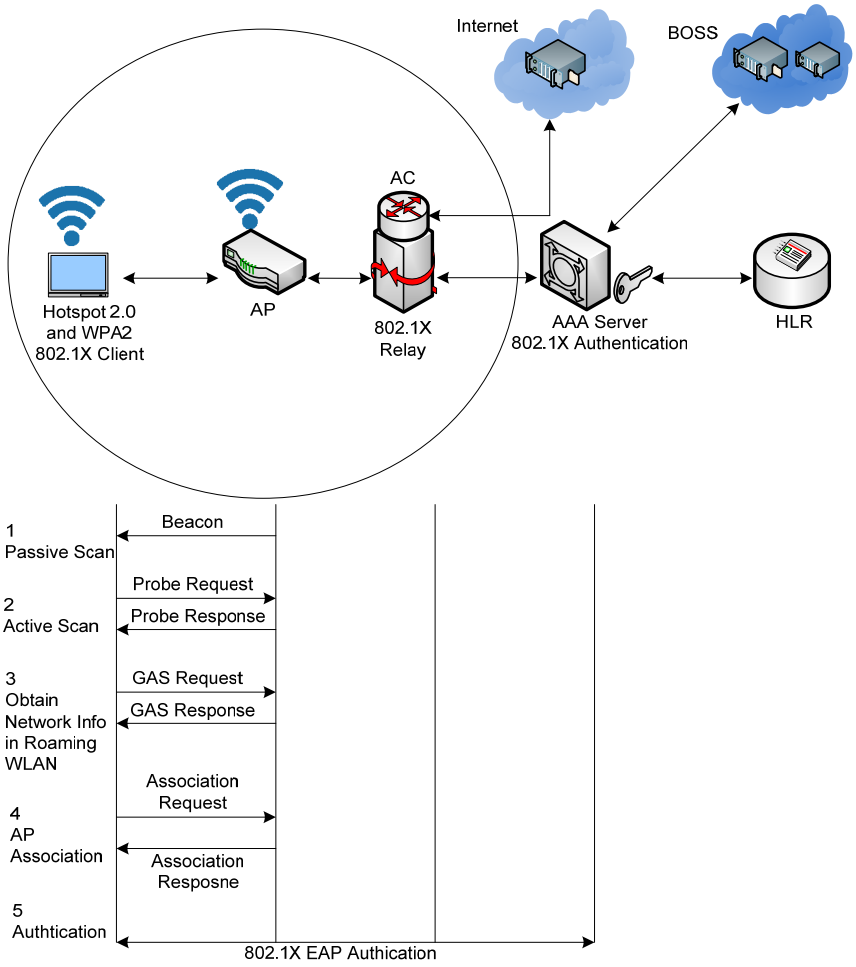

Figure 2. Generic structure of Hotspot 2.0.

- STA passive scan: The Hotspot 2.0 access point sends a Beacon frame to the STA module that comprises of network type, Hotspot 2.0 indication, and related network information. Upon receipt of the Beacon frame, the STA module checks the Hotspot 2.0 indication into it. The STA module can learn about basic service set (BSS) load prior to establishing a connection with the access point. If all works correctly, the STA module performs the parsing of the roaming consortium field in the Beacon frame to get details about the OI of the WLAN service provider.
- STA active scan: During this scan, the STA module sends a Probe Request frame to the access point along with the network type information. Upon receipt of this frame, the access point matches with the network type of the frame with its own network type. If the network type is matched, it sends the Probe Response frame to the STA module with the necessary BSS load, the internet connectivity flag, and other network details. After receipt of the Probe Response frame at the STA module, the STA module checks the hotspot indication. If everything works correctly, then the STA module assumes that the access point has the Hotspot 2.0 facility and the other activities are performed as in active scan procedure.
- The STA gathers roaming WLAN information: The generic advertisement service (GAS) is a mechanism that allows an STA module to exchange requests and response packets with the WLAN side. Firstly, the STA sends a GAS Initial Request to the access point along with supported authentication types, Hotspot 2.0 operators, and

related details. Upon the receipt of such a packet, the access point responds with GAS Initial Response packet that contains the ANQP-structured contents such as, the roaming consortium list, domain name, venue name, venue info, operator friendly name, IP address type availability, connection capacity, network authentication type information, access network type field, internet available field, BSS load information, Hotspot 2.0 indication, operating class indication, network access identifier (NAI) realm, 3GPP cellular public land mobile network (PLMN), and the homogeneous extended service set (HESSID).

- The STA association with the access point: Upon the detection of a target WLAN, the STA module sends an association request to the access point with the NAI realm, network type, authentication types, and Hotspot 2.0 indication. If all works correctly, the access point responds back with an association response frame to the STA module where the advanced encryption standard (AES)-aware 802.1X authentication procedure is embedded.
- STA authentication: An STA module sends an 802.1X authentication request to the access point, which then forwards it to the 802.1X authentication server (AAA) via an 802.1X relay (access controller) along with the NAI reports. A home authentication server (AAA) then communicates with the remote AAA server for the requisite authentication approval. If all works correctly, remote AAA server then grants access of the WLAN to the STA module.

In [92], a strong authentication scheme was proposed that is able to find the federated identities without tamper-resistant hardware. The study shows the password-based credential (PBC) to resist offline attacks by using a randomize-then-prove approach. This work shows how the PBC can be assessed as publicly verifiable for a federated identity application. In [93], a quantum-safe password authentication scheme was elaborated for its use in mobile devices. In this method, the password-authenticated key exchange (PAKE) system is deployed between two peer devices. Asymmetric-PAKE protocols can be used in this ecosystem to lower the remote server-aware plain text compromise that is posed by an attacker by storing the hash of the user's password. It is guaranteed that the user's password is never transmitted to the remote server. To improve the security of the system, smooth projectile hash functions (SPHF) and commitment-based password-hashing schemes (PHS) are introduced in the study. We believe that such schemes can be considered as alternatives to the generic hotspot architecture.

3.4.4. Hotspot Gateway

It is a network device that is responsible for providing authentication, authorization, and accounting (AAA) for a given wireless network infrastructure. Despite a possible intrusion by an eavesdropper, such a gateway can prevent malicious users from accessing a private network [94]. It helps users access the Internet instantly, without requiring any changes to the configuration of the user's mobile device or its internal client-side network software. With the existing network settings, a user can easily access different Internet networks through hotspot gateways. The location of the gateway can be identified by integrating the GPS-based antenna.

3.4.5. Hotspot Security Issues

The hotspot faces several challenges which can hinder the user experience, as follows:

- It does not solve interference problems.
- It faces an installed base hurdle because old access point replacement is a tedious task.
- Possible eavesdropping may be induced in terms of a man-in-the-middle attack.
- WLAN encryption is performed at the surface or interface level, later the message travels via the underlying network stack in an unencrypted manner to the remote service provider (ISP), thus causing risk.
- Public hotspots are prone to collect the users' metadata and related content, which require more secure access methods such as HTTPS and SSH.

- Despite authenticating the users, users may be able to peek into the network traffic by using a packet sniffer mechanism.
- Some business vendors provide a download option for Wi-Fi protected access (WPA) which may cause conflict with enterprise configurations which match with their own WLAN specifications.

4. Distributed Hotspot Network Architecture

It is a network device that is responsible for providing authentication, authorization, and accounting (AAA) for a given wireless network infrastructure. Despite the possible intrusion of an eavesdropper, such a gateway can prevent malicious users from accessing a private network [94]. It helps users to access the Internet instantly without requiring any changes to the configuration of the user's mobile device or its internal client-side network software. With the existing network settings, a user can easily access different Internet networks through hotspot gateways. The location of the gateway can be identified by integrating the GPS-based antenna. Figure 3 presents the conceptual design of IoT-dew aware blockchain assisted distributed hotspot network.

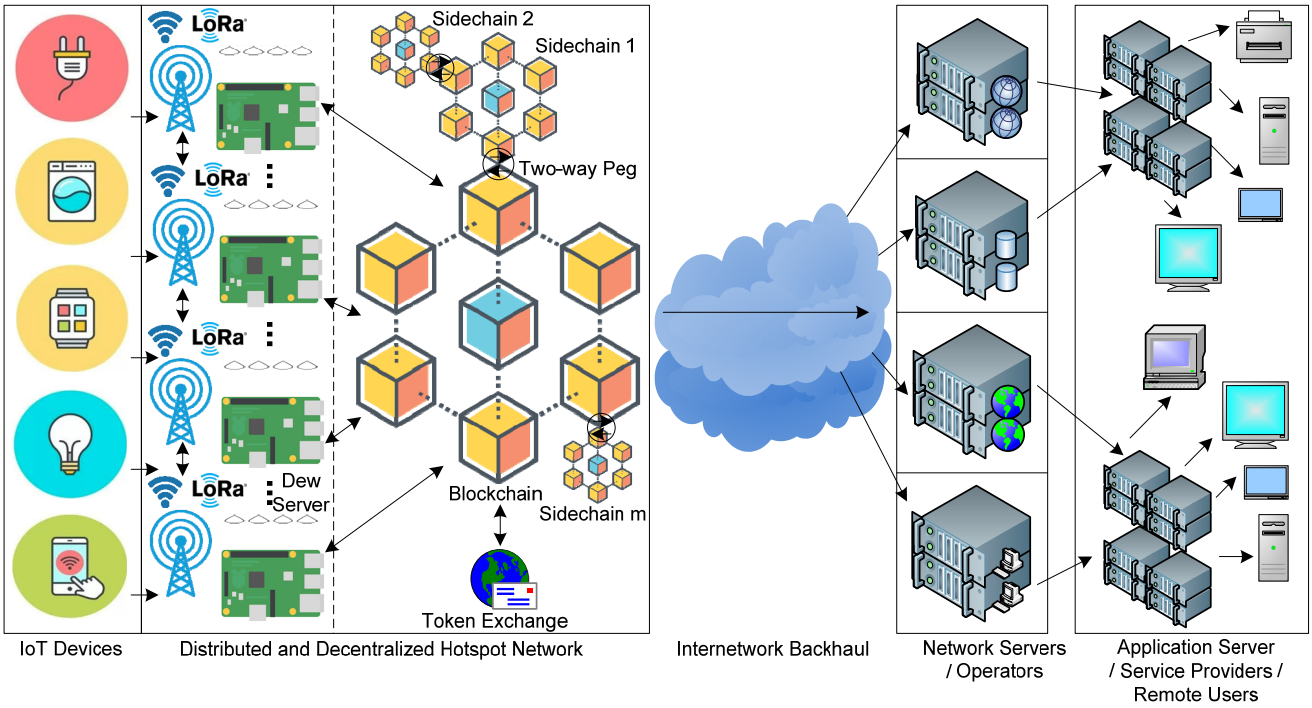

Figure 3. IoT-aware dew computing enabling blockchain-assisted, distributed hotspot network architecture.

4.1. IoT Device Layer

This layer includes various IoT devices from smart home, smart health, smart transportation, smart agriculture, and smart industry. All types of IoT devices along with sensors can participate in this layer. Standard 8-bit, 16-bit. and 32-bit microcontrollers and microprocessor-based IoT hardware pools can be used in this layer. The main role of this layer is to transmit data packets through intermediate layers to remote application servers/service providers/users. For example, a farmer is a remote end user who can visualize, monitor, or analyze the status of his farm through this architecture. They can place many devices that are equipped with IoT sensors at different locations on his farmland. These IoT devices are equipped with Wi-Fi and/or LoraWAN, depending on the data transmission capacities that are required (see above). However, it must be assumed that such IoT devices should be placed near a hotspot so that the sensor data can be easily transmitted. The farmer can set up his own dew server-centric hotspots (Wi-Fi or

LoraWAN) or rent the hotspot services of others who have already set up their hotspots in the geographical coverage area of the farmer's IoT devices. In this way, the farmer's IoT devices can communicate with the remote application layer by either using the hotspot services of their own hotspots or renting the network access services of other hotspots that have been systematically placed in the nearby coverage areas of such IoT devices.

4.2. Distributed and Decentralized Hotspot Network Layer

This layer is the most important layer of this architecture. The idea behind this layer is related to the commonly known People Powered Network (PPN), which is similar to that which the Helium Society has developed. The goal of this layer is to enable secure IoT data transmission over the distributed hotspot network access mechanism [95,96]. The term "people" is used here because the hotspots can be used by any person who wants to provide IoT data transmissions in their hotspot coverage area. Typically, the range of IEEE 802.11n (2.4 GHz) Wi-Fi is about 50 m. However, some long-range Wi-Fi devices are becoming available, which can operate on higher GHz bands (3.6/4.9/5/5.9/60 GHz) and multiple channels. For example, Wi-Fi 6 (IEEE 802.11ax) has 600–9608 Mbps and a longer range. LoraWAN can also be used as an alternative to Wi-Fi when data transmission over very long distances at minimum data rates is required. LoraWAN is a software communication protocol, and it is architecture that is based on the Lora-based Chirp Spread Spectrum (CSS) modulation scheme. Its range can be easily extended to 10–15 km, which is far more than Wi-Fi with a data capacity of 0.3–50 kbps per channel. LoraWAN has an additional advantage over cellular or other LPWAN techniques: it offers AES protection with end-to-end encrypted messaging with lower power consumption and thus a better battery life. LoraWAN operates in a bandwidth of 415/868/915 MHz in a license-free spectrum.

4.2.1. Hotspot Gateway

We can use Wi-Fi or LoraWAN as a promising hotspot provider technology because they have their own advantages over other cellular and LPWAN alternatives. All hotspots that are equipped with Wi-Fi or LoraWAN can be configured as gateways for IoT device data. Standard, off-the-shelf hardware platforms such as Raspberry Pi 4 or higher, Beaglebone black or higher, ASUS Tinker board, Libra Computer board AML-S905X-CC, Odroid N2+, UDOO Blot v3, and other related boards can be used as hotspot gateways. Such gateways must be equipped with a high-gain Wi-Fi or LoraWAN antenna. Anyone can use such hotspot gateways to provide IoT devices in the vicinity with the network.

4.2.2. 802.1X Authentication

Authentication is a very important part in this architecture. IEEE 802.11u-aware IEEE 802.1X authentication can be useful in the underlying scenario. IEEE 802.11u can support network discovery and selection by using GAS, ANQP, and quality of service (QoS) map distribution facilities. Upon a client-side X.509 certification, EAP-TLS can be used to allow such clients to become securely connected with the server side (AAA server). On the other hand, IEEE 802.1X authentication needs the components, supplicant (STA-a IoT device), authenticator (acts as bridge between the supplicant and access point), and authentication server (AAA server), which is a trusted server. The authenticator server informs the authenticator about the possibility that the supplicant is allowed to connect the network. Such an AAA server can run protocols such as the EAP or remote authentication dial-in user service (RADIUS) in their local machines. Sometimes, it can be integrated with the authenticator device itself. The whole process of authentication involves four procedures, such as, (i) initialization: at this stage, the supplicant is allowed for 801.1X traffic and other data such as the internet protocol, and the allied TCP and UDP services are dropped; (ii) initiation: in this stage, the authentication process begins where the authenticator transmits the EAP-Request/Identity frame to the local network segment at the 01:80:C2:00:00:03 address, and, upon receipt of such a frame, the supplicant responds with an EAP-Response frame to the authenticator with its own user identity, and

the authenticator then transmits this frame in the form of a RADIUS Access Request packet to the AAA server; (iii) EAP negotiation: in this phase, the AAA servers send a RADIUS Access-Challenge packet to the authenticator with an embedded EAP method, and the same is forwarded to the supplicant by the authenticator, then the supplicant can start with the mentioned EAP method, or it can respond with a non-acknowledgement frame to the authenticator; (iv) authentication: this is the final phase where both the AAA server and supplicant agree on a given EAP method, wherein the EAP Request and EAP Response packets are transmitted between the supplicant and AAA server via the authenticator, and this process continues until the AAA server responds with an EAP-Success message inside the RADIUS Access-Accept packet to the supplicant, otherwise, a RADIUS Access-Reject message is sent to the supplicant. Finally, upon the successful completion of the authentication process, the supplicant sets the post to an authorized state and normal data traffic is allowed, and upon logging off by the supplicant, the authenticator sets the post to an unauthorized state.

4.2.3. Dew Server Computation

Dew servers can be used to host such hotspot gateways. We can use a hotspot gateway and dew server separately to achieve higher effectiveness and a better user experience. We can also integrate both into a single system, where both activities can be performed simultaneously. The main goal of using a dew server is to leverage the dew computing paradigm in the periphery of the distributed hotspot network. Another idea behind the use of dew computing-enabled servers is to provide better performance capabilities in a way that is independent of Internet network services (cloud), so that the hotspot can operate seamlessly in a scenario with limited Internet access. For example, hotspots can enable nearby IoT devices to share sensor data with remote applications. Dew servers can also help IoT devices transmit sensor data when they are in rental mode. In lease mode, a dew server that is overloaded or performing other work can allocate its nearby hotspots to act as a gateway for said IoT device. In this way, an IoT device gains better access. If a dew hotspot is unable to serve the purpose of its nearby IoT device, it can forward the coverage to the nearest dew hotspot system, which will handle the message delivery for the IoT device. Another important aspect of using dew computing in this layer is the security of IoT-based messages. Such secure transmission can be ensured by incorporating a peer-to-peer (P2P) network technology, i.e., blockchain.

4.2.4. Dew Server as Hotspots

Ordinary hotspot gateways can function in two ways: (i) as a light-weight hotspot miner, and (ii) as a data-only hotspot. It may not be advisable to configure an ordinary hotspot gateway as a full-fledged hotspot miner, due to the following problem: It is well known that as a blockchain grows after its inception, the full nodes experience a huge burden of processing and storing distributed ledgers on the local machine. Gradually, such full nodes tend to be out of sync with the main blockchain. Due to the very high computational requirements, one can think about using moderately resilient miner nodes in the presented architecture. Instead of using ordinary hotspot gateways as full miners, we can consider them as light-weight hotspot miners or data-only hotspots. It is possible to turn a hotspot device into a lightweight miner with a hotspot provisioning tool or configure it as a data-only hotspot (that is without mining functionality). In our architecture, each person can deploy their dew server to act as either a light-weight hotspot miner or a data-only hotspot broker. Dew servers can solve the synchronization problem that usually occurs with full miners. Thus, a dew server can solve this problem and opens a new way to mitigate the synchronization problems that are normally encountered with traditional network computers.

4.2.5. Types of Hotspots

Based on the earlier discussion, we can state that the dew servers can act as: (i) full hotspot miners, (ii) light-weight hotspot miners, and (iii) data-only hotspots. Anyone can deploy the dew servers to act as one of three hotspots in the aforementioned architecture. In doing so, the range of the hotspot network coverage can be expanded to several hundreds of miles which can transmit IoT data in a fraction of the cost and energy with respect to standard cellular networks. All types of miners should follow the same software and packet format so that homogeneity is perceived [97,98]. Besides acting as a hotspot facilitator, dew severs can act as miners too. Such miners can also earn a given cryptocurrency standard (e.g., bitcoin, Ethereum, tether, USD, XRP, terra, Binance, etc.) or one that is indigenously (newly) developed from the network. Here, we discuss the three types of hotspots:

- Full hotspot: Dew servers, which can be configured as full hotspots, can be eligible to perform coverage facility to the IoT devices that are in their vicinity and also participate in all types of potential crypto reward scenarios inside the network. The Proof-of-Coverage (PoC) can be seen as a dominant algorithm in such an aspect as this. However, it should be maintained that such full hotspots should have prior approval from the underlying network authority, with high-standard and failure-proof subjunctives. We apprehend that the higher specification of servers with a complex processor design and memory capacity are mandatory for such type of hotspots.
- Light-weight hotspot: Such hotspots can be configured to replace full hotspots when moderate-load and moderate computations are needed, seamlessly. Dew servers have great potential to become converted into light-weight hotspots. They can perform regular hotspot coverage and perform header-wise synchronization with the associated blockchain. In this context, when overloading is perceived on the light-weight hotspots, they can transfer some consensus work to the full hotspots which are then expected to act as the validator of the light-weight hotspot. The use of light-weight hotspots can simplify the network structure and it enables the network ecosystem to grow rapidly.
- Data-only hotspot: This type of hotspot can only perform network data transfer. The transfer of data that are related to crypto awards may be earned by the use of such hotspots. We do not expect that the data-only hotspot would participate in the PoC-aware reward. Thus, a permissionless approach may be incorporated in the blockchain. users start earning crypto tokens as and when they are allowed to add blocks to the blockchain.

4.2.6. Proof of Coverage

The PoC is used to verify that the hotspots are actually in the locations that they claim to be [99]. The PoC aims to verify that hotspots are in their original locations and perform IoT device-related wireless network coverage from their specified locations. Any network that can be created using our architecture should be a physical wireless network. The success of such a physical wireless network depends on the reliability and availability of the network coverage for the IoT devices in the environment. The PoC algorithm uses the key properties of some radio frequencies (RF) as evidence that the hotspots are operating as smoothly as they claim to be. The properties of the radio frequencies are as follows:

- The radio frequency has a limited range for propagation.
- The radio frequency signal that is received at a terminal can be used to measure the signal strength by applying the proportional squared distance law.
- Radio frequencies have a minimum latency because they propagate at the speed of light.

The associated blockchain periodically polls all the connected hotspots using the PoC algorithm to verify that they provide a stable and reliable coverage for the IoT devices. In this way, the PoC confirms that the hotspots are constantly transmitting IoT data and storing it as blocks in the blockchain. Such a policy can be seen as proof that the hotspots are working, while their coverage is being used for the IoT devices.

The PoC essentially poses a challenge to all the hotspots as a discrete unit of work of the algorithm. Several million such challenges can be issued to the hotspots and processed simultaneously by the associated blockchain [99]. With each new challenge, the PoC confirms that the hotspot network is functioning as desired. The main goal of the PoC is to minimize the PoC interval to a certain limited number of α-blocks or less. At any point in time, a hotspot has one of the following three main roles:

- Interrogator: Usually, such nodes are full hotspot nodes or other designated validators that create the PoC challenge and issue it to the condemned node. It challenges the PoC for a convicted target node.
- Convicted: it is a hotspot node that is the target of the PoC challenge, and it is expected to transmit the challenge packets so that the nearby hotspots can observe its activity.
- Witness: Such hotspots are located in the immediate (geographic) vicinity of the convicted node and also report to the querying system, the status of the challenge packets that is sent by the convicted node (High Performance Remote Procedure Call-gRPC). Such a witness is directly connected to all the light-weight hotspot nodes. Such lightweight nodes, that are PoC challenge witnesses, can use validators to which they are connected so that the entire query validator search process can be managed using the hash of the PoC packet. This routing information is later used by the light-weight hotspot to deliver the witness report directly to the query sender. Once the query sender receives both the convicted receipts and witness reports after a certain time, it transmits them to the blockchain and the PoC challenge is complete.

4.2.7. PoC Challenge Creation and Target Selection

Ordinarily, full hotspots or validators can construct a challenge for every block of the blockchain. However, increasing such a challenge request per block can be disastrous in terms of the computation load. Thus, a variable—β—can be used to control the PoC challenge rate so that the number of PoC challenges per block can be controlled. Increasing β can significantly increase the number of PoC challenges in each block.

Firstly, a full hotspot or validator generates a short-term key pair—(p,q) and a hash—*hash* (*publickey*). Secondly, the (p,q) and *hash* (*publickey*) are included into the validator *txns*. Next, the *privatekey* is stored in a *local_state* (*validator*). Later, while absorbing the *txns*, if the proposed keys do not match to a consensus group member (CGM), such proposed keys are added to local cache—*lcache*. Later, each member of the CGM selects a number of keys—$k \in$ *lcache*—so that the target β can be obtained. If a minimum ($2k + 1$) number of nodes participate in a block, then β can be obtained by following $\frac{\beta}{2(N-1)/3}$ by each of the validators in the group. The value of β may be fixed for any unnecessary changes of α, periodically, in order to reduce the network load. If more than $2k + 1$ number of nodes participate, then the public keys hashes are truncated so that the block metadata can be formed. A number of selected keys are removed from *lcache*, thus resulting in the adjustment and governance by the validators to serve the capacity of the network.

Once, a block is successfully handled, every validator inspects the *publickey* in the given block and finds out whether it matches with them. If a match happens, a new PoC is generated for each of such matching. Later, the *hash* (*publickey*) is used with the *hash* (*block*) to generate an entropy—*e*—for the respective PoC challenge in the *H3* region. Such an entropy—*e*—which is generated from a combination of *hash* (*publickey*) and *hash* (*block*), is used to identify the target node in the *H3* region for generating a PoC challenge. Among all the regions, the PoC challenge and target are locally persistent with each challenger validator.

4.2.8. Crypto Mining and Rewards

Dew servers acting as hotspot miners can earn crypto tokens as rewards for their reliable network coverage service for IoT devices. Such crypto tokens can have any standard form or be developed in-house. The block time can be in μ seconds and the target epoch size is b blocks. Usually, an epoch consists of all the blocks that are processed by the current CG from the end of the last epoch. Let us assume that the blockchain is designed to mint c

crypto tokens per month. Then the following formula can be used to analyze the number of epochs per month, l, and crypto tokens per epoch, m:

$$l = (43{,}200 \text{ min per month})/((\mu \times b)/60 \text{ per epoch})$$

$$m = (\text{c crypto-token per month})/(l \text{ epochs per month})$$

The crypto tokens per epoch, m, can be shared between the PoC interrogator, the PoC-convicted, and the witness nodes in a standardized manner. The reward can also be split between the CG and the network (data-only hotspot) rewards that are associated with the data transmission. Hotspot owners can use multiple crypto wallets to receive or issue crypto tokens. Such wallets may be equipped with the following features: account balance verification, network identity verification, reconciliation, address book support, and support for payments to multiple accounts/recipients.

4.2.9. Network Consensus Protocol Goals

The network consensus protocol can be designed around the following key properties: (i) permission-free: any hotspot that operates reliably can participate in the network architecture; (ii) constraints can be imposed so that there is no additional benefit to complex hardware equipment in the hotspot; (iii) the protocol is Byzantine fault-tolerant; (iv) the consensus system should be based on useful, reliable, and reusable actions; (v) the transaction confirmation rate should be imposed; (vi) the hotspots should behave in a censorship-independent manner (they should not select or deselect any IoT device). In addition, the formation of sidechains can be allowed for conducting micropayments, research, and development, and for publishing betas. A sidechain is a blockchain that is connected to a parent blockchain via a two-way connection. Such sidechains have their own consensus protocols so that privacy and security can be improved. In this way, trust in the main blockchain is minimized. The two-way connection facilitates the transfer of digital assets between blockchains. In addition, such blockchains can enable the exchange of crypto tokens.

4.3. Internetwork Backhaul

Internetworking for incoming messages from IoT devices via various hotspots and the blockchain are transmitted to target application server/remote users. This internetwork backhaul can be optional, if the LoraWAN-aware design is considered where LoraWAN-based platforms can act as the message delivery system. For example, helium channels can be deployed to serve the backhaul connectivity to remote network servers/operators. A standard the things network (TTN) is also capable of performing similar tasks. Otherwise, a regular cellular-based internetwork backhaul may be considered.

4.4. Network Servers/Operators

Network servers/operators are the entities, the standard ISPs, that can be used in this architecture as the domain name servers or the path forwarders. Such providers enable wireless bearer services, especially cellular services for the end applications or users. To accomplish this task, the operators perform radio frequency allocation, end-user support, network process maintenance, and network equipment provisioning. These operators are also able to generate revenue and charge end-applications or customers according to their agreement or network usage policy. In addition, mobile virtual network operators (MVNOs) can be used as leased network service providers under the major network operators.

4.5. Application Servers/Service Providers/Remote Users

Application servers host applications and/or software to provide business applications to their subscribers or end users. Such servers may use the server framework service model through an application programming interface (API) to accomplish the desired task. In general, application servers are built to be fail-safe and can perform load balancing. Mobile

application servers (MAS) can also be used to augment business logic with representative state transfer (REST) so that the bandwidth can be minimized. In addition, MAS can provide authentication services, offline support, security, and data orchestration. Service-oriented architecture (SOA)-oriented infrastructures are capable of connecting to dependent end users, but limited resources and broken connections can cause problems.

5. Discussion

Our architecture is inspired by the design of the helium integration network [100], where IoT devices can transmit sensor data to remote application servers or users. We modified the design of the architecture in a multi-layered manner to achieve more control over the network. Our architecture represents a true hotspot coverage network in which many hotspots can be placed within the coverage area of each hotspot. In this way, IoT devices can transmit messages on a hop-by-hop basis. We used the dew computing paradigm to minimize the Internet dependency and improve accessibility for the end devices. The hotspots can be integrated with dew servers to enhance their ability to act as one of three types of hotspots, such as: (i) full-fledged hotspot miners, (ii) light-weight hotspot miners, and (iii) data-only hotspots. A dew-enabled hotspot can earn crypto tokens, based on its specified activities.

The implicit architecture enables a new type of incentive for hotspot owners to set up hotspots, according to their needs. Dew computing leverages the synchronization aspect, which does not require a direct Internet connection. Dew computing hotspots can communicate with each other to create a distributed ad hoc network that operates independently of the Internet. This provides high reliability and availability for the IoT devices that want to transmit sensor data to remote locations. IoT devices do not need to be directly connected to the Internet, which can dramatically reduce the costs of the network and the traffic on the cellular network. Our architecture provides two types of hotspot technologies: (i) Wi-Fi, and (ii) LoraWAN. Wi-Fi-enabled dew-based hotspot miners can be used when high data speed is required and there is an Internet connection between the hotspot network layer and the remote network service providers or the end users. LoraWAN can be used when a low data rate is required and there may not be an Internet connection. The Things network can be added as an exchange. Various APIs can be integrated into the LoraWAN-enabled network platforms to forward the IoT sensor data to the remote network servers and application processes.

5.1. Threat Model

Threat modeling allows the proactive or reactive measure of a system [100–102]. A proactive measure is applied during the design and development phase, i.e., an early stage reactive measure is performed when a system has already been deployed. In this work, we propose a distributed hotspot network architecture on a conceptual basis [103]. Table 2 presents the list of threats, compromised assets, behavior, and threat agent.

We follow the standard STRIDE classification [104] to model the proposed architectural framework in terms of a threat model. We use triple attributes {*threat agent*, *asset*, *behavior*} to represent the threat model perspectives. The *threat agent* represents a malicious actor who can cause damage to an asset of the proposed architectural framework by invoking a specific *behavior*. The behavior means that, that set of actions that is manual or automated in terms of its interaction with the system.

Two possible threat agents are included, such as, *malicious user* and *malicious service*. A malicious user is an attacker who has no legal nor ethical access to the implied network infrastructure. A malicious service aims to steal assets, cause harm, control the system, and deny the services that it provides. The attacker does not need to be an expert, but a generic technology enthusiast who has the basic knowledge and skills to intercept the operational activities of the system framework. We use various types of compromised assets such as LoRaWAN networks, Wi-Fi networks, IoT devices, dew gateway devices,

dew gateway miner devices, remote users, remote application servers, dew server services, and *dewlet* services.

Table 2. Distributed Hotspot Network Threat Model.

ID	Threat	Compromised Asset	Behavior	Threat Agent
T1	Unauthorized Network Access	LoRaWAN Network	A malicious user aims to associate with malicious IoT device of the user's LoRawan Network	Malicious User
T2	Unauthorized Network Access	Wi-Fi Network	A malicious user aims to associate with malicious IoT device of the user's Wi-Fi Network	Malicious User
T3	Device Hijacking	IoT Device	A malicious user aims to associate with IoT device of the user's periphery without user's knowledge or awareness	Malicious User
T4	Device Hijacking	Dew Gateway Device	A malicious user aims to associate with dew gateway device of the user's periphery without user's knowledge or awareness	Malicious User
T5	Data Leakage	Dew Gateway Device	A malicious user aims to access and retrieve data, i.e., device's location GPS information, user's credentials about dew gateway device	Malicious User
T6	Device Hijacking	Dew Gateway Miner Device	A malicious user aims to associate with dew gateway miner device of the user's periphery without user's knowledge or awareness	Malicious User
T7	Impersonation	LoRaWAN Network	A malicious user aims to associate with a legitimate IoT device to malicious LoRaWAN Network	Malicious User
T8	Impersonation	Wi-Fi Network	A malicious user aims to associate with a legitimate IoT device to malicious Wi-Fi Network	Malicious User
T9	Impersonation	IoT Device	A malicious user aims to associate with force with a malicious IoT device by using other user's credentials	Malicious User
T10	Impersonation	Dew Gateway Device	A malicious user aims to associate with force with a malicious dew gateway device by using other user's credentials	Malicious User
T11	Impersonation	Dew Gateway Miner Device	A malicious user aims to associate, with force, with a malicious dew gateway miner device by using other user's credentials	Malicious User
T12	Jamming	LoRaWAN Network	A malicious user aims to disturb the LoRaWAN Network	Malicious User
T13	Jamming	Wi-Fi Network	A malicious user aims to disturb the Wi-Fi Network	Malicious User
T14	Message Elimination	Dew Gateway Wi-Fi Network	A malicious user aims to delete or eliminate messages of gateway Wi-Fi network	Malicious User
T15	Message Elimination	Dew Gateway LoRaWAN Network	A malicious user aims to delete or eliminate messages of gateway Wi-Fi network	Malicious User
T16	Exhaustion of Power	IoT Device	A malicious user aims to consume excessive power to resist IoT device work to prevent regular activities	Malicious User
T17	Exhaustion of Power	Dew Gateway Device	A malicious user aims to consume excessive power to resist dew gateway device work to prevent regular activities	Malicious User
T18	Exhaustion of Power	Dew Gateway Miner Device	A malicious user aims to consume excessive power to resist dew gateway device work to prevent regular activities	Malicious User

Table 2. *Cont.*

ID	Threat	Compromised Asset	Behavior	Threat Agent
T19	Impersonation	Dewlet Service	A malicious user aims to replace legitimate dewlet service with a malicious service	Malicious User
T20	Impersonation	Dew Server Service	A malicious user aims to replace legitimate dew server-based service with a malicious service	Malicious User
T21	Impersonation	Remote User	A malicious user aims to replace legitimate remote user with a malicious user	Malicious User
T22	Denial of Service	Remote User	A malicious user aims to make legitimate remote user with a malicious service	Malicious User
T23	Denial of Service	Remote Application Server	A malicious user aims to make legitimate remote application server with a malicious service	Malicious User
T24	Eavesdropping	LoRaWAN Network	A malicious user aims to retrieve important packets while transmitted over LoRaWAN network	Malicious User
T25	Eavesdropping	Wi-Fi Network	A malicious user aims to retrieve important packets while transmitted over LoRaWAN network	Malicious User

5.2. Key Challenges

- The architecture is a conceptual model; thus, it needs to be implemented. The implementation of this architecture would require dedicated dew servers and hotspot coverage antennae such as Wi-Fi or LoraWAN. The selection of the Wi-Fi module could be judiciously performed so that long range coverage can be facilitated with a higher bandwidth. However, such antennae should consume a low level of power for providing better sustainability. LoraWAN could be a great choice in this regard, however, the cost of antenna module could be high for very long-range coverage.
- IoT devices should have Wi-Fi or LoraWAN connectivity to communicate to the nearby hotspots. Thus, a serious consideration should be made so that the cost of the IoT device does not go beyond a certain limit and so that the battery consumption can be minimized.
- Hotspots need to be configured as miner nodes that should run on top of dew servers. Synchronization algorithms should be devised for making the internet independency more reliable.
- Several LoraWAN platforms including TTN, Helium, LORIOT, ResIOT, SenRa, and ChirpStack can be considered while one is considering the internetwork backhaul. For Wi-Fi hotspots, a standard cellular backhaul may be used.
- The type of blockchain should be devised. A hybrid approach can be beneficial in this aspect. An owner of a hotspot miner device can place it in their locality, to act as one of three types of hotspots, namely, full, light-weight, or data-only. The design specifications of each type of hotspot are different as their tasks are different. Complex, moderate, and simple hotspot hardware designs should be selected prior to deploying them in the real field of application.
- Concise decisions should be made about the use of a PoC challenging aspect in this architecture. The PoC challenge rate, epoch size, and block time are important parameter that must be resolved a-priori.
- One should consider the wallet type while aiming to connect their hotspot miner node with this network architecture.
- A network consensus algorithm can be revisited to improve the reliability of the hotspot network. Target crypto token production per unit of time (e.g., month, quarter, half-yearly, or yearly) need to be accorded.
- It is important to select a cryptocurrency that will be used in this architecture for rewarding the hotspot owners. It can be selected from existing standard cryptocurrencies or can be devised indigenously for a specific hotspot-distributed network architecture.

- The structure of the block should be designed optimally. The number of transactions per block should be decided before using the blocks in reality. A decision should be made for fixing the transaction fees. The oracles should be carefully decided to specify the data credit conversion rate. The price of the selected crypto oracles must be aligned with the other blockchain networks.
- The interoperability issues should be tackled so that this architecture can talk with other blockchains.
- A trustless packet purchasing features should be formulated in order to allow higher coverage for the hotspot network. State channels and an organizationally unique identifier (OUI) should be implemented with proper care.
- A reward scaling approach must be put in place for each epoch. In this aspect, it becomes important to specify who gets what, i.e., a hotspot shall earn as specific amount, as a reward.
- The selection of a higher-grade Byzantine fault-tolerant protocol becomes inevitable when a blockchain is used. An asynchronous atomic broadcast protocol can be used with a consensus group which has known nodes. The threshold encryption technique may be deployed to improve the async behavior.
- A procedure should be designed to elect a consensus group. It can be performed epoch-wise or in a time/duration manner. The number of members of each consensus group should be judiciously decided.
- The overall governance of the hotspot network must be catered with regular voting and community guidelines.
- The scalability aspects should be investigated for the mass IoT-based dew deployments for the provisioning of the distributed hotspot network.
- The diverse network connectivity of such architecture must be well designed for mitigating a significant amount of channel stabilization. Thus, this issue must be further investigated.
- Dewlet-aware rental services should be invoked with fairness practices. Innovative methods should be investigated to mitigate this issue.
- A detailed threat model analysis is not available for this architecture. Without such a model analysis, it is difficult to state the viability of the proposed system.

5.3. Future Scope

The architecture has the potential to enable a new type of hotspot network deployment in the future. Ordinary mobile and physical network objects should be included in the current hotspot network structure. The security features of hotspots should be considered. The architecture is expected to provide a large area for the distributed coverage of the hotspots. Therefore, it is required that all hotspots follow similar rules and software updates. Edge computing devices need to be evaluated for their suitability as alternative hotspot machines. Third-party cloud service providers can be considered to add value to this architecture.

6. Conclusions

We discuss the possibility of deploying a novel, distributed architecture that provides secure hotspot coverage for IoT devices over long distances. The distributed architecture can open a new business model where the benefits of Wi-Fi and LoraWAN technologies can be leveraged to provide a financial advantage to hotspot owners who wish to lease their hotspots for a user's inclusion in the network. We encourage academics, researchers, and companies to develop new ideas and practical use cases that are based on the proposed architecture.

Author Contributions: P.P.R. wrote the paper, designed the architecture, described the notions of the architecture, and pointed out key challenges and future way outs. K.S. helped with concept and mentoring, screening, and language improvement the paper. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Center of Research Excellence "DATACROSS", Zagreb, Croatia No. EK-KF-KK.01.1.1.01.009 grant number EK-KF-KK.01.1.1.01.009 and the APC was funded by Center of Research Excellence "DATACROSS", Zagreb, Croatia No. EK-KF-KK.01.1.1.01.009.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The paper was partly created in project Center of Research Excellence "DATACROSS", Zagreb, Croatia no. EK-KF-KK.01.1.1.01.009, including payment of APC.

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

References

1. Ogonji, M.M.; Okeyo, G.; Wafula, J.M. A survey on privacy and security of Internet of Things. *Comput. Sci. Rev.* **2020**, *38*, 100312. [CrossRef]
2. Lombardi, M.; Pascale, F.; Santaniello, D. Internet of things: A general overview between architectures, protocols and applications. *Information* **2021**, *12*, 87. [CrossRef]
3. Raj, M.; Gupta, S.; Chamola, V.; Elhence, A.; Garg, T.; Atiquzzaman, M.; Niyato, D. A survey on the role of Internet of Things for adopting and promoting Agriculture 4.0. *J. Netw. Comput. Appl.* **2021**, *187*, 103107. [CrossRef]
4. Lee, E.; Seo, Y.D.; Oh, S.R.; Kim, Y.G. A Survey on Standards for Interoperability and Security in the Internet of Things. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 1020–1047. [CrossRef]
5. Ratta, P.; Kaur, A.; Sharma, S.; Shabaz, M.; Dhiman, G. Application of blockchain and internet of things in healthcare and medical sector: Applications, challenges, and future perspectives. *J. Food Qual.* **2021**, *2021*, 7608296. [CrossRef]
6. Misra, N.N.; Dixit, Y.; Al-Mallahi, A.; Bhullar, M.S.; Upadhyay, R.; Martynenko, A. IoT, big data and artificial intelligence in agriculture and food industry. *IEEE Internet Things J.* **2020**, *9*, 6305–6324. [CrossRef]
7. Laghari, A.A.; Wu, K.; Laghari, R.A.; Ali, M.; Khan, A.A. A review and state of art of Internet of Things (IoT). *Arch. Comput. Methods Eng.* **2021**, *29*, 1395–1413. [CrossRef]
8. Sobin, C.C. A survey on architecture, protocols and challenges in IoT. *Wirel. Pers. Commun.* **2020**, *112*, 1383–1429. [CrossRef]
9. Hossein Motlagh, N.; Mohammadrezaei, M.; Hunt, J.; Zakeri, B. Internet of Things (IoT) and the energy sector. *Energies* **2020**, *13*, 494. [CrossRef]
10. Khalaf, O.I.; Romero, C.A.T.; Hassan, S.; Iqbal, M.T. Mitigating hotspot issues in heterogeneous wireless sensor networks. *J. Sens.* **2022**, *2022*, 7909472. [CrossRef]
11. Dolan, E.; Widayanti, R. Implementation Of Authentication Systems On Hotspot Network Users To Improve Computer Network Security. *Int. J. Cyber IT Serv. Manag.* **2022**, *2*, 88–94. [CrossRef]
12. Jiang, Y.; Yang, F.; Yu, B.; Zhou, D.; Zeng, X. Efficient layout hotspot detection via binarized residual neural network ensemble. *IEEE Trans. Comput. -Aided Des. Integr. Circuits Syst.* **2020**, *40*, 1476–1488. [CrossRef]
13. Swedha, S.; Gopi, E.S. LSTM network for hotspot prediction in traffic density of cellular network. In *Machine Learning, Deep Learning and Computational Intelligence for Wireless Communication*; Springer: Singapore, 2021; pp. 35–47.
14. Gushev, M. Dew computing architecture for cyber-physical systems and IoT. *Internet Things* **2020**, *11*, 100186. [CrossRef]
15. Singh, P.; Kaur, A.; Aujla, G.S.; Batth, R.S.; Kanhere, S. Daas: Dew computing as a service for intelligent intrusion detection in edge-of-things ecosystem. *IEEE Internet Things J.* **2020**, *8*, 12569–12577. [CrossRef]
16. Podder, T.; Bhattacharya, D.; Majumdar, A. Dew Computing-Inspired Mental Health Monitoring System Framework Powered by a Lightweight CNN. In *Disruptive Technologies for Big Data and Cloud Applications*; Springer: Singapore, 2022; pp. 309–319.
17. Olabisi, D.; Abubakar, S.K.; Abdullahi, A.T. Demystifying Dew Computing: Concept, Architecture and Research Opportunities. *Int. J. Comput. Trends Technol.* **2022**, *70*, 39–43. [CrossRef]
18. Wang, Y. A blockchain system with lightweight full node based on dew computing. *Internet Things* **2020**, *11*, 100184. [CrossRef]
19. Manocha, A.; Bhatia, M.; Kumar, G. Dew computing-inspired health-meteorological factor analysis for early prediction of bronchial asthma. *J. Netw. Comput. Appl.* **2021**, *179*, 102995. [CrossRef]
20. Hirsch, M.; Mateos, C.; Rodriguez, J.M.; Zunino, A. DewSim: A trace-driven toolkit for simulating mobile device clusters in Dew computing environments. *Softw. Pract. Exp.* **2020**, *50*, 688–718. [CrossRef]
21. Moussa, M.M.; Alazzawi, L. Cyber attacks detection based on deep learning for cloud-dew computing in automotive iot applications. In Proceedings of the 2020 IEEE International Conference on Smart Cloud (SmartCloud), Washington, DC, USA, 6–8 November 2020; pp. 55–61.
22. Draz, U.; Ali, T.; Yasin, S.; Waqas, U.; Rafiq, U. EADSA: Energy-aware distributed sink algorithm for hotspot problem in wireless sensor and actor networks. In Proceedings of the 2019 International Conference on Engineering and Emerging Technologies (ICEET), Lahore, Pakistan, 21–22 February 2019; pp. 1–6.
23. Ye, A.; Li, Q.; Zhang, Q.; Cheng, B. Detection of spoofing attacks in WLAN-based positioning systems using Wi-Fi hotspot tags. *IEEE Access* **2020**, *8*, 39768–39780. [CrossRef]

24. Wang, X.; Lin, F.; Wu, Y. A novel positioning system of potential Wi-Fi hotspots for software defined Wi-Fi network planning. In Proceedings of the 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 11–14 January 2019; pp. 1–6.
25. Noura, H.; Hatoum, T.; Salman, O.; Yaacoub, J.P.; Chehab, A. LoRaWAN security survey: Issues, threats and possible mitigation techniques. *Internet Things* **2020**, *12*, 100303. [CrossRef]
26. Jouhari, M.; Amhoud, E.M.; Saeed, N.; Alouini, M.S. A Survey on Scalable LoRaWAN for Massive IoT: Recent Advances, Potentials, and Challenges. *arXiv* **2022**, arXiv:2202.11082.
27. Zhou, Q.; Huang, H.; Zheng, Z.; Bian, J. Solutions to scalability of blockchain: A survey. *IEEE Access* **2020**, *8*, 16440–16455. [CrossRef]
28. Syed, T.A.; Alzahrani, A.; Jan, S.; Siddiqui, M.S.; Nadeem, A.; Alghamdi, T. A comparative analysis of blockchain architecture and its applications: Problems and recommendations. *IEEE Access* **2019**, *7*, 176838–176869. [CrossRef]
29. Zheng, W.; Zheng, Z.; Chen, X.; Dai, K.; Li, P.; Chen, R. NutBaaS: A blockchain-as-a-service platform. *IEEE Access* **2019**, *7*, 134422–134433. [CrossRef]
30. Wang, Q.; Zhu, X.; Ni, Y.; Gu, L.; Zhu, H. Blockchain for the IoT and industrial IoT: A review. *Internet Things* **2020**, *10*, 100081. [CrossRef]
31. Singh, S.; Hosen, A.S.; Yoon, B. Blockchain security attacks, challenges, and solutions for the future distributed iot network. *IEEE Access* **2021**, *9*, 13938–13959. [CrossRef]
32. Zha, D.S.; Feng, T.T.; Gong, X.L.; Liu, S.Y. When energy meets blockchain: A systematic exposition of policies, research hotspots, applications, and prospects. *Int. J. Energy Res.* **2022**, *46*, 2330–2360. [CrossRef]
33. Zhao, X.; Lei, Z.; Zhang, G.; Zhang, Y.; Xing, C. September. Blockchain and distributed system. In *International Conference on Web Information Systems and Applications*; Springer: Cham, Switzerland, 2020; pp. 629–641.
34. Messié, V.; Fromentoux, G.; Labidurie, N.; Radier, B.; Vaton, S.; Amigo, I. BALAdIN: Truthfulness in collaborative access networks with distributed ledgers. *Ann. Telecommun.* **2022**, *77*, 47–59. [CrossRef]
35. Lopez, D.; Yazdizadeh, A.; Farooq, B.; Patterson, Z. Distributed Privacy-Aware Choice Modelling using Federated Learning over Blockchain. In Proceedings of the International Choice Modelling Conference, Kobe, Japan, 19–21 August 2019.
36. Janiesch, C.; Fischer, M.; Imgrund, F.; Hofmann, A.; Winkelmann, A. An Architecture Using Payment Channel Networks for Blockchain-based Wi-Fi Sharing: An Architecture for Blockchain-based Wi-Fi Sharing. *ACM Trans. Manag. Inf. Syst.* **2022**. [CrossRef]
37. Yang, Y.; Liu, Z.; Liu, Z.; Chan, K.Y.; Guan, X. Joint Optimization of Edge Computing Resource Pricing and Wireless Caching for Blockchain-Driven Networks. *IEEE Trans. Veh. Technol.* **2022**, *71*, 6661–6670. [CrossRef]
38. Zhao, Z.; Guo, J.; Luo, X.; Xue, J.; Lai, C.S.; Xu, Z.; Lai, L.L. Energy transaction for multi-microgrids and internal microgrid based on blockchain. *IEEE Access* **2020**, *8*, 144362–144372. [CrossRef]
39. Kim, S.K.S. Apply Blockchain to Overcome Wi-Fi Vulnerabilities. *J. Multimed. Inf. Syst.* **2019**, *6*, 139–146. [CrossRef]
40. Ivanov, N.; Lou, J.; Yan, Q. Smart Wi-Fi: Universal and secure smart contract-enabled Wi-Fi hotspot. In *International Conference on Security and Privacy in Communication Systems*; Springer: Cham, Switzerland, 2020; pp. 425–445.
41. Pustišek, M.; Dolenc, D.; Kos, A. LDAF: Low-bandwidth distributed applications framework in a use case of blockchain-enabled IoT devices. *Sensors* **2019**, *19*, 2337. [CrossRef]
42. Ma, S.; Li, H.; Yang, W.; Li, J.; Nepal, S.; Bertino, E. Certified Copy? Understanding Security Risks of Wi-Fi Hotspot based Android Data Clone Services. In Proceedings of the Annual Computer Security Applications Conference, Austin, TX, USA, 7–11 December 2020; pp. 320–331.
43. Casado-Vara, R.; Novais, P.; Gil, A.B.; Prieto, J.; Corchado, J.M. Distributed continuous-time fault estimation control for multiple devices in IoT networks. *IEEE Access* **2019**, *7*, 11972–11984. [CrossRef]
44. Babun, L.; Denney, K.; Celik, Z.B.; McDaniel, P.; Uluagac, A.S. A survey on IoT platforms: Communication, security, and privacy perspectives. *Comput. Netw.* **2021**, *192*, 108040. [CrossRef]
45. Boursianis, A.D.; Papadopoulou, M.S.; Diamantoulakis, P.; Liopa-Tsakalidi, A.; Barouchas, P.; Salahas, G.; Karagiannidis, G.; Wan, S.; Goudos, S.K. Internet of things (IoT) and agricultural unmanned aerial vehicles (UAVs) in smart farming: A comprehensive review. *Internet Things* **2022**, *18*, 100187. [CrossRef]
46. Lounis, K.; Zulkernine, M. Attacks and defenses in short-range wireless technologies for IoT. *IEEE Access* **2020**, *8*, 88892–88932. [CrossRef]
47. Balcerzak, A.P.; Nica, E.; Rogalska, E.; Poliak, M.; Klieštik, T.; Sabie, O.M. Blockchain Technology and Smart Contracts in Decentralized Governance Systems. *Adm. Sci.* **2022**, *12*, 96. [CrossRef]
48. Alshehri, F.; Muhammad, G. A comprehensive survey of the Internet of Things (IoT) and AI-based smart healthcare. *IEEE Access* **2020**, *9*, 3660–3678. [CrossRef]
49. Husnoo, M.A.; Anwar, A.; Chakrabortty, R.K.; Doss, R.; Ryan, M.J. Differential privacy for IoT-enabled critical infrastructure: A comprehensive survey. *IEEE Access* **2021**, *9*, 153276–153304. [CrossRef]
50. Mohanta, B.K.; Jena, D.; Satapathy, U.; Patnaik, S. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet Things* **2020**, *11*, 100227. [CrossRef]
51. Nižetić, S.; Šolić, P.; González-de, D.L.D.I.; Patrono, L. Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *J. Clean. Prod.* **2020**, *274*, 122877. [CrossRef] [PubMed]

52. Chettri, L.; Bera, R. A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems. *IEEE Internet Things J.* **2019**, *7*, 16–32. [CrossRef]
53. Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. *Comput. Netw.* **2019**, *148*, 283–294.
54. Wu, M.; Wang, K.; Cai, X.; Guo, S.; Guo, M.; Rong, C. A comprehensive survey of blockchain: From theory to IoT applications and beyond. *IEEE Internet Things J.* **2019**, *6*, 8114–8154. [CrossRef]
55. Pavithran, D.; Shaalan, K.; Al-Karaki, J.N.; Gawanmeh, A. Towards building a blockchain framework for IoT. *Clust. Comput.* **2020**, *23*, 2089–2103. [CrossRef]
56. Gill, S.S.; Tuli, S.; Xu, M.; Singh, I.; Singh, K.V.; Lindsay, D.; Tuli, S.; Smirnova, D.; Singh, M.; Jain, U.; et al. Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges. *Internet Things* **2019**, *8*, 100118. [CrossRef]
57. Dedeoglu, V.; Jurdak, R.; Dorri, A.; Lunardi, R.C.; Michelin, R.A.; Zorzo, A.F.; Kanhere, S.S. Blockchain technologies for iot. In *Advanced Applications of Blockchain Technology*; Springer: Singapore, 2020; pp. 55–89.
58. Shahbazi, Z.; Byun, Y.C. Integration of Blockchain, IoT and machine learning for multistage quality control and enhancing security in smart manufacturing. *Sensors* **2021**, *21*, 1467. [CrossRef]
59. Rane, S.B.; Thakker, S.V. Green procurement process model based on blockchain–IoT integrated architecture for a sustainable business. *Manag. Environ. Qual. Int. J.* **2020**, *31*, 741–763. [CrossRef]
60. Si, H.; Sun, C.; Li, Y.; Qiao, H.; Shi, L. IoT information sharing security mechanism based on blockchain technology. *Future Gener. Comput. Syst.* **2019**, *101*, 1028–1040. [CrossRef]
61. Tseng, L.; Yao, X.; Otoum, S.; Aloqaily, M.; Jararweh, Y. Blockchain-based database in an IoT environment: Challenges, opportunities, and analysis. *Clust. Comput.* **2020**, *23*, 2151–2165. [CrossRef]
62. Alladi, T.; Chamola, V.; Parizi, R.M.; Choo, K.K.R. Blockchain applications for industry 4.0 and industrial IoT: A review. *IEEE Access* **2019**, *7*, 176935–176951. [CrossRef]
63. Sun, S.; Du, R.; Chen, S.; Li, W. Blockchain-based IoT access control system: Towards security, lightweight, and cross-domain. *IEEE Access* **2021**, *9*, 36868–36878. [CrossRef]
64. Sharma, P.K.; Kumar, N.; Park, J.H. Blockchain technology toward green IoT: Opportunities and challenges. *IEEE Netw.* **2020**, *34*, 263–269. [CrossRef]
65. Hirsch, M.; Mateos, C.; Zunino, A.; Majchrzak, T.A.; Grønli, T.M.; Kaindl, H. A task execution scheme for dew computing with state-of-the-art smartphones. *Electronics* **2021**, *10*, 2006. [CrossRef]
66. Ahammad, I.; Khan, A.R.; Salehin, Z.U. A Review on Cloud, Fog, Roof, and Dew Computing: IoT Perspective. *Int. J. Cloud Appl. Comput. (IJCAC)* **2021**, *11*, 14–41. [CrossRef]
67. Gusev, M. Serverless and Deviceless Dew Computing: Founding an Infrastructureless Computing. In Proceedings of the 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 12–16 July 2021; pp. 1814–1818.
68. Gusev, M. What makes Dew computing more than Edge computing for Internet of Things. In Proceedings of the 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 12–16 July 2021; pp. 1795–1800.
69. Javadzadeh, G.; Rahmani, A.M.; Kamarposhti, M.S. Mathematical model for the scheduling of real-time applications in IoT using Dew computing. *J. Supercomput.* **2022**, *78*, 7464–7488. [CrossRef]
70. Sverko, M.; Tankovic, N.; Etinger, D. Dew Computing in Industrial Automation: Applying Machine Learning for Process Control. In Proceedings of the 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 12–16 July 2021; pp. 1789–1794.
71. Braeken, A. Authenticated key agreement protocols for dew-assisted IoT systems. *J. Supercomput.* **2022**, *78*, 12093–12113. [CrossRef]
72. Mukherjee, A.; De, D.; Dey, N. Dewdrone: Dew computing for Internet of Drone Things. *IEEE Consum. Electron. Mag.* **2021**. [CrossRef]
73. Islam, A.; Al Amin, A.; Shin, S.Y. FBI: A federated learning-based blockchain-embedded data accumulation scheme using drones for Internet of Things. *IEEE Wirel. Commun. Lett.* **2022**, *11*, 972–976. [CrossRef]
74. Gusev, M. AI cardiologist at the edge: A use case of a dew computing heart monitoring solution. In *Artificial Intelligence and Machine Learning for EDGE Computing*; Academic Press: Cambridge, UK, 2022; pp. 469–477.
75. Rana, S.; Obaidat, M.S.; Mishra, D.; Mishra, A.; Rao, Y.S. Efficient design of an authenticated key agreement protocol for dew-assisted IoT systems. *J. Supercomput.* **2022**, *78*, 3696–3714. [CrossRef]
76. Medhi, K.; Ahmed, N.; Hussain, M.I. Dew-based offline computing architecture for healthcare IoT. *ICT Express* **2022**, *8*, 371–378. [CrossRef]
77. Guberović, E.; Lipić, T.; Čavrak, I. Dew Intelligence: Federated learning perspective. In Proceedings of the 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 12–16 July 2021; pp. 1819–1824.
78. Aishwarya, M.R.; Mathivanan, G. AI Strategy for Stake Cloud Computing and Edge Computing: A State of the art survey. In Proceedings of the 2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2–4 December 2021; pp. 920–927.
79. Aburukba, R.; Al-Ali, A.R.; Riaz, A.H.; Al Nabulsi, A.; Khan, D.; Khan, S.; Amer, M. Fog Computing Approach for Shared Mobility in Smart Cities. *Energies* **2021**, *14*, 8174. [CrossRef]

80. Escobar-Diaz, F.; Buitrago, C.; Quiñones, L.; Grajales, F.; Mejia, T. Evaluation of particulate matter microsensors to build the low-cost sensors collaborative network of Bogotá. In Proceedings of the 2021 Congreso Colombiano y Conferencia Internacional de Calidad de Aire y Salud Pública (CASAP), Bogota, Colombia, 3–5 November 2021; pp. 1–5.
81. Costa, B.; Bachiega, J., Jr.; de Carvalho, L.R.; Araujo, A.P. Orchestration in fog computing: A comprehensive survey. *ACM Comput. Surv. (CSUR)* **2022**, *55*, 1–34. [CrossRef]
82. Dong, W.; Lv, J.; Chen, G.; Wang, Y.; Li, H.; Gao, Y.; Bharadia, D. TinyNet: A lightweight, modular, and unified network architecture for the internet of things. In Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services, Portland, OR, USA, 27 June–1 July 2022; pp. 248–260.
83. Veloso, A.F.D.S.; Júnior, J.V.R.; Rabelo, R.D.A.L.; Silveira, J.D.F. HyDSMaaS: A Hybrid Communication Infrastructure with LoRaWAN and LoraMesh for the Demand Side Management as a Service. *Future Internet* **2021**, *13*, 271. [CrossRef]
84. Schütz, M. RF Harvesting at 2.4 GHz for Scattering between Battery-less Transponder and Mobile Telephones. In Proceedings of the 2021 IEEE International Conference on RFID Technology and Applications (RFID-TA), Delhi, India, 6–8 October 2021; pp. 93–96.
85. Mishra, V.K.; Swami, B.D.; Kanagarathinam, M.R.; Thorat, P.B.; Das, D. NextGen-MHS: A Novel Architecture for Tethering of Aggregated Licensed and Unlicensed Spectrums. In Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 15–18 April 2019; pp. 1–6.
86. Agyemang, J.O.; Kponyo, J.J.; Klogo, G.S.; Boateng, J.O. Lightweight rogue access point detection algorithm for Wi-Fi-enabled Internet of Things (IoT) devices. *Internet Things* **2020**, *11*, 100200. [CrossRef]
87. Xu, W.; Zhou, H.; Bi, Y.; Cheng, N.; Shen, X.; Thanayankizil, L.; Bai, F. Exploiting hotspot-2.0 for traffic offloading in mobile networks. *IEEE Netw.* **2018**, *32*, 131–137. [CrossRef]
88. Nojima, D.; Yamada, A. Technologies for Interworking Between Cellular and WLAN Systems. *IEICE Commun. Soc. Glob. Newsl.* **2019**, *43*, 3.
89. Bednarczyk, M. IEEE 802.11 ax: Giant leap in WLAN evolution. In Proceedings of the XII Conference on Reconnaissance and Electronic Warfare Systems, Oltarzew, Poland, 19–21 November 2018; Volume 11055, pp. 416–422.
90. Chatzisofroniou, G.; Kotzanikolaou, P. Exploiting WiFi usability features for association attacks in IEEE 802.11: Attack analysis and mitigation controls. *J. Comput. Secur.* **2022**, *30*, 357–380. [CrossRef]
91. Huawei Hotspot 2.0. Available online: https://support.huawei.com/enterprise/en/doc/EDOC1100096325/2010a98b/understanding-hotspot-20 (accessed on 16 July 2022).
92. Zhang, Z.; Wang, Y.; Yang, K. Strong Authentication without Temper-Resistant Hardware and Application to Federated Identities. In Proceedings of the NDSS 2020, San Diego, CA, USA, 23–26 February 2020.
93. Li, Z.; Wang, D.; Morais, E. Quantum-safe round-optimal password authentication for mobile devices. *IEEE Trans. Dependable Secur. Comput.* **2020**, *19*, 1885–1899. [CrossRef]
94. Paolini, A.; Scardaci, D.; Liampotis, N.; Spinoso, V.; Grenier, B.; Chen, Y. Authentication, authorization, and accounting. In *Towards Interoperable Research Infrastructures for Environmental and Earth Sciences*; Springer: Cham, Switzerland, 2020; pp. 247–271.
95. Helium Network. Available online: https://docs.helium.com/ (accessed on 15 July 2022).
96. Helium Mining. Available online: https://www.okdo.com/blog/the-ultimate-guide-to-lora-helium-miners-and-crypto-mining/ (accessed on 16 July 2022).
97. Helium Network Design. Available online: https://create.arduino.cc/projecthub/akarsh98/what-is-helium-network-hnt-mining-hotspots-and-crypto-7a148e (accessed on 16 July 2022).
98. Helium Hotspot Mining. Available online: https://create.arduino.cc/projecthub/akarsh98/tutorial-helium-light-hotspot-with-dragino-lps8-dlos8-miner-b7a39e (accessed on 16 July 2022).
99. Proof of Coverage. Available online: https://docs.helium.com/blockchain/proof-of-coverage (accessed on 15 July 2022).
100. Helium Network White Paper. Available online: http://whitepaper.helium.com/ (accessed on 14 July 2022).
101. Wang, D.; Wang, P. Two birds with one stone: Two-factor authentication with security beyond conventional bound. *IEEE Trans. Dependable Secur. Comput.* **2016**, *15*, 708–722. [CrossRef]
102. NTP Amplified Reflection DDOS Attack Scanning Tutorial, Amplified List Scanning Tutorial. Available online: http://www.aeys.org/thread-3520-1-1.html/ (accessed on 5 August 2022).
103. Granata, D.; Rak, M.; Salzillo, G.; Barbato, U. Security in IoT Pairing & Authentication protocols, a Threat Model, a Case Study Analysis. In Proceedings of the ITASEC 2021, Virtual, 7–9 April 2021; pp. 207–218.
104. The STRIDE Threat Model. Available online: https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN (accessed on 25 August 2022).