Sharing is (S)caring: Security and Privacy Issues in Decentralized Physical Infrastructure Networks (DePIN)

Maurantonio Caprolu[1], Simone Raponi[2], and Roberto Di Pietro[1]

[1] King Abdullah University of Science and Technology (KAUST)
Thuwal 23955, Saudi Arabia
{maurantonio.caprolu, roberto.dipietro}@kaust.edu.sa
[2] Equixly S.r.l. Firenze, 50124, Italy
simone.raponi@equixly.com

Abstract. Decentralized Physical Infrastructure Networks (DePIN) have emerged as a promising paradigm, offering numerous benefits across various domains. For instance, DePIN allows to share (and monetize) excess resources, such as computing capacity and network bandwidth, enabling the provisioning of a wide range of services, including anonymous navigation, data acquisition, and computation, in exchange for cryptocurrency. The above examples are just the tip of the iceberg of the dematerialization, distribution, and democratization capabilities of the DePIN paradigm. However, in addition to their potential advantages, the decentralized nature of DePIN applications also introduces significant security and privacy concerns that must be carefully addressed.

In this paper, we analyze the security and privacy implications of the DePIN infrastructure focusing on two domains: *Network Services* and *Computation for AI-based Tasks*. By examining the major active projects within each domain, we identify common security and privacy issues that require urgent attention from the community. Specifically, vulnerabilities related to the sharing of resources with unknown entities pose significant risks to the integrity and reliability of DePIN networks. In addition, concerns related to the handling of sensitive data, such as personal information and financial transactions, underscore the importance of robust security measures. Furthermore, inherited cybersecurity challenges from the underlying blockchain technology, including Sybil attacks and consensus vulnerabilities, exacerbate the security landscape of DePIN networks. To bridge this gap, we propose several directions for future research aimed at addressing security issues common to the DePIN paradigm.

Keywords: DePIN · Security · Privacy · Blockchain · IoT · Tokenomics.

1 Introduction

The emergence of the DePIN sector marks a significant variation from the traditional Web2-based online service model. To fully grasp the innovation introduced by this new paradigm, it is useful to recall the evolution of Internet technologies and service models, as illustrated in Fig. 1. Although Web2 enabled end-users to generate and share content, its centralized architecture granted major tech companies full control over users' data and identities. In contrast, the user-centric Web3 model, on which the DePIN architecture is implemented, allowed users to share physical resources, e.g., bandwidth, storage, and computation, in a zero-trust environment, giving them ownership of their data [8]. In Web2, dominant big tech companies, such as Facebook, Google, and Amazon, exercise significant control over user data and interactions [7]. These platforms act as intermediaries, collecting large amounts of user data to fuel targeted advertising and other monetization strategies. In this model, users often sacrifice privacy and autonomy in exchange for access to free services. For example, social media platforms track users' online activities, preferences, and interactions to deliver personalized content and advertisements in exchange for free access to their platforms and services [6,13]. On the contrary, Web3 embraces decentralization with the aim of allowing users to regain control over their data. Blockchain technology plays a central role in Web3, enabling decentralized applications (DApps), which operate without centralized servers. Users retain ownership of their data and can interact with DApps in a peer-to-peer manner without relying on intermediaries. For example, decentralized social media platforms, such as Steemit and Minds, reward users for their contributions and allow them to monetize their content directly, bypassing traditional intermediaries [7]. The concept of value exchange is, in fact, one of the key differences between Web2 and Web3. In Web2, a few big companies extract value from users' data and attention, often without adequately compensating them. On the contrary, Web3 leverages tokenomics methodologies and decentralized finance (DeFi) protocols, where users can earn and exchange tokens for their contributions. For example, platforms like Uniswap and Compound enable users to participate in decentralized exchanges and lending/borrowing protocols, earning tokens in exchange for liquidity or borrowing assets [19]. Following the Web3 revolution, the DePIN model emerged as a response to the limitations and drawbacks of centralized infrastructure and services in traditional Internet of Things (IoT) and networking architectures. Historically, IoT frameworks have operated primarily in two modes: cloud-centric, where data from physical devices is routed through IoT gateways to centralized cloud servers for processing and storage, or edge-centric, which involves processing data closer to the source by specialized edge servers [14]. Although these approaches have been prevalent in IoT applications, they tend to be centralized or hybrid in nature. In contrast, DePIN introduces a pioneering approach by integrating three core concepts: Blockchain, IoT, and Tokenomics, following the Web3 model. This integration enables the creation of decentralized systems that are not only efficient but also transparent and economically incentivized, enabling community-driven development and resource management. In the last

few years, several common use cases have risen for DePIN, showcasing the versatility and potentialities of this model. Some of the most common DePIN use cases include decentralized Internet access, supply chain management, energy grid, and finance, just to name a few.

Although DePIN applications offer numerous benefits, they also pose several security concerns that need to be addressed. Unfortunately, as usually happens during the development of new technologies, both academic and industrial research focus more on designing and implementing new platforms that enable innovative use cases, often neglecting crucial security considerations.

Contributions. To address the cited gaps, in this paper we analyze the novel DePIN infrastructure from both the security and privacy perspectives. In this regard, we first selected two domains, based on the popularity and capitalization of their prominent projects. Then, for each of the two domains, we discuss the major active projects and identify security and privacy concerns that need to be addressed by the community. Finally, we present several security issues that are horizontal to DePIN use cases and propose several directions for future research on possible countermeasures. In more detail, the main contributions of this paper can be summarized as follows:

- After discussing the DePIN technological pillars, we summarize and synthesize the general DePIN architecture providing a unified reference framework—contrary to the partial and scattered information available in the literature.
- We analyze two different DePIN domains, *Network Services* and *Computation for AI-based tasks*, identify the major related active projects, and discuss their peculiar security and privacy issues.
- We outline several security challenges idiosyncratic to the DePIN paradigm, while also suggesting potential directions for future research aimed at developing effective countermeasures.

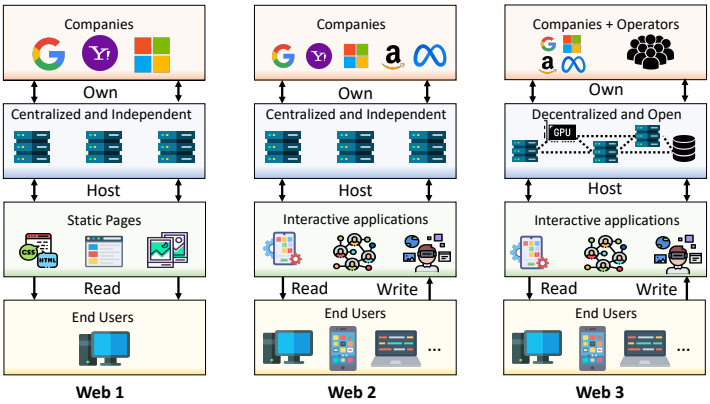

Fig. 1. Evolution of Internet technologies, from Web1 to Web3.

2 Related Work

Research into Decentralized Physical Infrastructure Networks (DePIN) is still in its infancy, with a few key studies setting the initial groundwork for understanding and developing these complex systems. This section reviews some of the seminal works that address the architecture, classification, and foundational protocols of DePIN, focusing on how these studies frame the current landscape and identify the primary challenges of these networks. Fan et al. position paper [5] discusses the potential to scale DePIN through the use of rollup-centric architectures. They propose the integration of off-chain transaction aggregation and on-chain data commitment as a solution to the scalability limitations of traditional blockchain systems. This approach is suggested to significantly improve transaction throughput, which is essential for DePIN applications that demand high transaction volumes and swift processing. The insights from the paper provide a preliminary look at how DePIN systems can be made more efficient and scalable. Ballandies et al. [2] offer one of the first categorizations of the emerging field of DePIN through a comprehensive taxonomy. Their work organizes DePIN systems based on the underlying technologies, operational mechanisms, and applications. This taxonomy is valuable for systematically identifying and understanding the diverse aspects of DePIN systems.Sarkar [15] has introduced a generalized protocol framework aimed at standardizing the core functionalities of DePIN. His framework outlines the critical components and interactions within DePIN systems, aiming to support the development of modular and interoperable applications across different sectors. Sarkar's framework contributes to the foundational efforts in promoting a cohesive approach to DePIN development, highlighting the need for standards and consistency in these decentralized systems.

These early studies are pivotal in shaping the initial conceptual and technical understanding of DePIN. However, they also reveal a significant gap in the literature, particularly in addressing security and privacy challenges that are critical to the robust and safe deployment of DePIN systems. Our research builds upon these preliminary findings, focusing specifically on enhancing security and privacy mechanisms, key elements for the broader adoption of DePIN technologies.

3 DePIN Architecture

The concept of DePIN is strictly related to Decentralized Applications (DApps), a novel software paradigm that leverages blockchain technology to run applications on decentralized networks rather than centralized servers. The architecture and implementation details of a DePIN application strictly depend on the underlying blockchain environment. In the following, we generalize an architectural design, common to any DePIN project, which consists of technologies and methods combined to enable decentralized infrastructure management and operations.

The core technological pillars include blockchain, which implements smart contracts and powers *DApps* technologies, as well as IoT, *tokenization*, and novel methodologies like *tokenomics*.

DePIN applications leverage blockchain technology to establish a decentralized and tamper-proof public ledger to record data exchanges within the system. This decentralized infrastructure eliminates the need for centralized intermediaries, enabling transactions between participants in a trustless environment. The blockchain infrastructure also provides smart contracts, a crucial component in DePIN applications. Smart contracts are self-executing pieces of code that implement agreements between parties with predefined rules and conditions. Directly deployed on the blockchain platform, smart contracts enable efficient and transparent operations within the network, implementing several functions, such as asset management, data sharing, incentive mechanisms, and many others.

DePIN applications, typically built as *DApps* on top of a blockchain infrastructure, leverage a Layer 1 blockchain to facilitate seamless interactions with the underlying system. This enables users to manage shared resources, view real-time data, and participate in network governance. Once deployed, these applications operate autonomously through smart contracts, executing tasks according to predefined rules without human intervention. Their decentralized nature ensures that no single entity controls them, relying instead on distributed consensus mechanisms to maintain transparency and security.

Another crucial concept for DePIN is *tokenization*, that is, the process of converting assets into digital tokens on a blockchain. These tokens can represent different types of assets, including physical assets, e.g., real estate or commodities [12], financial assets [3], e.g., stocks or bonds, or digital assets, e.g., cryptocurrency or digital collectibles. A critical feature provided by *tokenization* is to enable *fractional ownership* by dividing assets into smaller, tradable units usually managed by smart contracts within DePIN applications. In the context of *DApps*, and particularly in the *DeFi* and DePIN domains, *tokenization* plays a crucial role in creating fungible or non-fungible tokens that represent ownership or rights to specific assets or utilities within the ecosystem.

Providing end-users with economic incentives to boost active participation and maintain adherence to the protocol is imperative for the security and success of any decentralized project. In this context, *tokenomics*, which studies the economic incentives that make a crypto-based project valuable, assumes a pivotal role in DePIN applications. Typically, *DApps* use either the native token of the underlying blockchain network or a customized one to encourage participation, reward contributions, and facilitate value exchange. These tokens may represent ownership rights, access to network resources, or voting power within the governance framework of the system. A popular component of tokenomics, relevant but not exclusive to DePIN, are airdrops: quantities of tokens distributed to active users (typically, if some conditions are verified) in order to start aggregating a community that could possibly foster interest in the project [9].

[3] https://www.coindesk.com/markets/2024/03/20/blackrock-enters-asset-tokenization-race-with-new-fund-on-the-ethereum-network/

A general DePIN infrastructure is shown in Fig. 2. At the core of the network are physical devices, owned by users participating in the protocol, often called *operators*. This layer can include any device, ranging from personal computers to small sensors embedded with IoT capabilities, shared by operators to end-users. Physical devices are deployed across the infrastructure network to provide particular services related to the main goal of the implemented application, such as collecting, processing, or storing data, handling network packets, and managing green energy production and distribution, just to name a few [3]. Operators connect their physical resources to the DePIN application, which leverages smart contracts, tokenization, and tokenomics to create the market. End-users make an offer according to their needs, use the resources, and pay a rental fee. Finally, the transaction is stored on a Layer 1 blockchain, and the operator receives the benefit according to the platform rules and conditions.

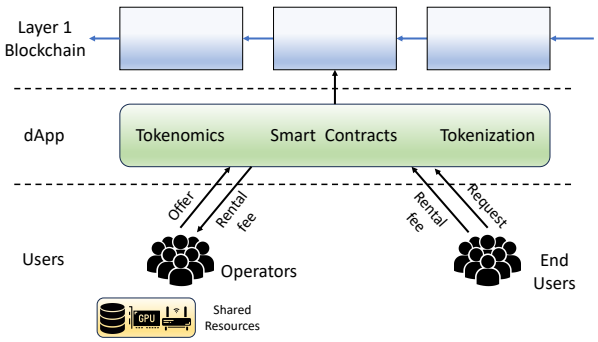

Fig. 2. A generic high-level DePIN architecture

4 Decentralization of Network Services

DePIN technologies have introduced novel approaches to the provision and management of network services, offering distinct advantages in terms of resilience, scalability, and economic efficiency. Wireless connectivity and VPN services stand out as domains that are undergoing a substantive transformation thanks to the DePIN paradigm, generating use cases that, other than being interesting on their own, also epitomize the added value of DePIN and show further possible applications in different domains as well. In this section, we discuss the most popular projects related to *decentralized VPN* (dVPN) and *decentralized wireless* (deWI). Then, we analyze the security and privacy aspects of these two use cases from the perspective of both the users participating in the protocol, i.e., the ones who share their resources, and the end-users, i.e., the ones who utilize the shared resource.

4.1 Decentralized VPN (dVPN)

Virtual Private Networks (VPNs) play a crucial role in ensuring secure and private communications over the Internet, especially in particular contexts, such as public networks and areas under censorship. Traditional VPN services are centralized and operated by commercial providers, raising concerns about data privacy, software vulnerabilities, and potential regulatory restrictions. In this scenario, DePIN applications seek to address these limitations by offering decentralized alternatives to traditional VPN services, leveraging blockchain technology and distributed infrastructure to improve security, privacy, and user control.

In a DePIN-based VPN ecosystem, participants deploy decentralized VPN nodes (dVPNs), creating a distributed network of exit points for the VPN service. Using blockchain-based identity management and encryption protocols, dVPNs ensure secure and private communication, protecting user data from surveillance, censorship, and unauthorized access. These applications leverage tokenomics to incentivize node operators and users. The system rewards operators with native tokens for providing bandwidth and maintaining infrastructure, while users access services by staking tokens or paying fees.

dVPNs offer several advantages over centralized VPN providers. First, dVPNs encrypt user packets and mix them with network traffic of other users, making online activities harder to trace. Without centralized servers, dVPNs reduce the risk of data breaches, logging, and surveillance, making censorship and blocking difficult. These advantages make dVPNs particularly suitable for regions with restricted internet access. Additionally, dVPNs leverage residential IP addresses, since exit nodes are operated by retail users, unlike centralized VPNs that use data center IPs. Residential IPs usually have better reputations, resulting in fewer restrictions, and provide greater access to geo-restricted content. They also reduce the risk of IP blocking, offering a smoother browsing experience and enhanced online freedom.

It is worth noting that dVPN is not a novel concept. One of the first proposals for a fully distributed VPN system over P2P networks, called Everywhere Local Area network (ELA) [1], dates back to 2005. Although the rationale is the same, the lack of incentives for participants, as well as a reliable underlying technology layer, prevented the wide diffusion of this technology. However, the advent of the DePIN paradigm, that is, blockchain and smart contracts combined with novel tokenomics methodologies, fueled the revival and rapid spread of dVPN services, demonstrating the power of DePIN infrastructures. Although dVPN is still in its infancy, the provided solution is attracting numerous operators and end-users, also fueling research into optimal monetization strategies [18] and novel architectures [16, 17].

Major Active Projects

Deeper Network This project aims to integrate cybersecurity, network sharing, and blockchain technology to create an innovative internet infrastructure inspired by the Web3 paradigm, adhering to the principle "Of the Users, By the Users, For the Users," which aims to return internet infrastructure ownership

to end-users. Deeper Network operates a decentralized infrastructure powered by proprietary hardware devices running an open-source operating system, *atomOS*. Users connect these plug-and-play devices to their home routers, becoming network exit nodes and gaining free access to Deeper Network's dVPN service in exchange for sharing their bandwidth. The network is governed by a Proof-of-Credit (PoCr) consensus algorithm. In addition, users can stake the native token, Deeper Network (DPR), to participate in mining and earn rewards. The underlying blockchain, Deeper-chain, is built on the Substrate framework to support essential network functionalities. A key advantage of this project is the versatility and user-friendliness of its devices. Although traditional dVPNs are often complex and suited only for tech-savvy users, Deeper Network's devices simplify setup, making the network accessible to users regardless of their technical expertise.

Mysterium Network Mysterium Network is an open-source ecosystem offering several privacy-focused tools and services, including a dVPN. Participants join by running the free MystNodes software, which connects their device to the network as an exit node. In return for sharing bandwidth and routing other users' traffic, node owners earn the native token, MYST, based on connection time and data volume. The network's tokenomics model allows node runners and token holders to stake MYST in the delegation pool, participate in the consensus protocol, and earn additional tokens. Networking functionalities are built on the WireGuard protocol, and the micropayment system uses *Hermes*, a proprietary protocol that allows pay-as-you-go transactions. *Hermes* operates on a Layer 2 solution backed by the Ethereum blockchain. One major advantage of Mysterium Network is its purely software-based approach, allowing users worldwide to join without setup costs; in contrast, Deeper Network requires purchasing proprietary hardware. MystNodes is lightweight and can run on budget devices, such as the Raspberry Pi, enabling continuous operation with minimal hardware and energy costs. The Mysterium network boasts over 22,000 nodes in 155+ countries, routing 1.83 PB of traffic monthly, according to the official website.

Security and Privacy Issues of dVPN

While dVPNs offer unique advantages in terms of architecture, provided services, and monetization model, they also present certain challenges and limitations that users and operators should carefully consider before adopting them as their preferred VPN solution. Some disadvantages stem from technical aspects, e.g., potential speed reduction due to routing through many different heterogeneous nodes, and setup complexity. Although these challenges can be addressed by developing and implementing more robust and user-friendly protocols, others arise from the distributed and permissionless nature of the network, posing risks to the security and privacy of both users and operators. In fact, the volunteer-based model of any DePIN application means trusting nodes operated by unknown entities, as well as sharing resources with unknown users. Furthermore, in the particular case of dVPNs, regulatory ambiguity is also a big concern. In fact,

the legal status of these services can be unclear or vary by region, potentially putting operators at risk of unknowingly violating local laws. In the following, we discuss some potential security and privacy issues peculiar to dVPN applications that involve both operators, who serve as exit nodes, and end-users, who utilize dVPN services (the attack target is reported within the squared bracket).

Privacy attacks [end-users]. By design, dVPN end-users route their traffic through exit nodes operated by the community. For this reason, they may be exposed to various privacy attacks, with one particularly concerning issue being the threat posed by malicious exit nodes. These attacks can compromise user privacy in several ways. First, malicious nodes could try to analyze network traffic, monitoring the patterns and volume of data that passes through the network. By analyzing traffic patterns, attackers can infer sensitive information about users' browsing habits, interests, and online activities, even if the content of the data packets is encrypted. This kind of attack is particularly difficult to detect, as the attacker passively analyzes the traffic without further interaction with the victim. With the same goal and methodology, malicious nodes may log and retain user internet traffic and meta-data, compromising their privacy and trying to infer their identities.

Among active attacks, we can cite DNS spoofing, where the malicious node redirects users' DNS requests to malicious servers controlled by the attacker. This allows the attacker to control the resolution of domain names, redirect users to any external website, possibly containing phishing software, or intercept sensitive information transmitted over insecure connections. Similarly, malicious end nodes may attempt to intercept and manipulate users' Internet traffic, acting as intermediaries between the user and their intended destination, i.e., man-in-the-middle attack. In this case, the attacker can intercept communications, modify or inject malicious content into data packets, and impersonate legitimate websites or services, leading to data theft, phishing, or malware infection.

Legal issues [operators]. Participants who agree to serve as exit nodes in a dVPN infrastructure share their Internet connection with unknown and untrusted end-users. As the final exit point from the VPN network to the public internet, the exit node is responsible for decrypting and forwarding end-users' data packets to their intended destinations. This means that the exit node operator's IP address will be tied to end-users internet traffic, making them potentially liable for any illegal activities conducted through their node. Although operators may argue that they are merely providing a technical service and are not responsible for the actions of individual users, legal authorities may hold them accountable as facilitators of illegal activity. Additionally, some jurisdictions impose legal obligations on network operators to monitor and prevent illegal activities, further increasing the potential liability for exit node owners. Potential legal problems may arise from different perspectives, including:

i) *Generic Illegal Activities:* If users engage in illegal activities, such as hacking, distributing malware, or accessing illicit content, through the VPN service, exit node operators may be held responsible for aiding and abetting such activ-

ities. Depending on the jurisdiction, this could result in criminal charges or civil lawsuits against the operator;

ii) *Copyright Infringement:* Exit node operators may face legal liability for copyright infringement if users utilize the VPN service to access copyrighted content without authorization. Although the operator may not be directly responsible for the infringement, they could be held liable for facilitating the transmission of copyrighted material;

iii) *Government Surveillance and Interception Orders:* In some jurisdictions, governments may issue surveillance or interception orders requiring exit node operators to monitor or intercept users' Internet traffic. Compliance with such orders could raise legal and ethical concerns, particularly if they infringe on users' privacy rights or violate the principles of net neutrality. These orders are usually directed at ISPs and centralized VPN providers. However, they could be extended to dVPN operators, as they are performing the same operations.

Illicit use [external targets]. Whenever a platform enables users to share resources in exchange for benefits, such as monetary compensation, malicious actors can exploit third-party resources without authorization to make a personal profit. This behavior, known as sponge attack [4], has been observed across several domains, particularly in crypto mining and residential proxies [4, 10]. In this type of attack, the victim remains unaware that a resource-sharing protocol operates on their infrastructure, resulting in the unauthorized use of resources for the attacker's gain. This attack vector extends to the realm of dVPN in various forms. For instance, malicious users may embed dVPN code within other software, such as Android SDKs or malware, and distribute it to unwilling users. Additionally, unethical employees may stealthily install a dVPN within a company's infrastructure without authorization, making a personal profit while drawing the company's resources.

Some of the above-mentioned problems, such as legal issues for operators and privacy leakage for end-users, are not idiosyncratic of dVPN but shared with similar software, such as centralized VPNs and ToR. However, in the case of centralized VPNs, the problem is slightly different, as end-users know the company name and reputation and are free to decide whether to trust it or not. In the case of ToR, instead, the problem is the same, i.e., exit nodes are operated by unknown and potentially malicious entities [11], but with a smaller impact. In fact, the vast majority of the ToR community is composed of experienced users, with more knowledge on the risks related to the particular technology. In contrast, dVPNs sport fast-growing communities, with all kinds of user joining the protocol attracted by the possibility of monetizing their unused bandwidth, completely unwilling of related threats.

4.2 Decentralized Wireless (DeWI)

Wireless technology is essential in modern communication systems, providing seamless connectivity for a wide range of devices and applications. Decentralized wireless is a novel concept of wireless communication that aims to democratize access to wireless networks while ensuring robustness and reliability. Unlike

the classic centralized architecture, DeWI deploys a decentralized infrastructure of nodes equipped with IoT-enabled devices, such as Wi-Fi routers or mesh networking devices, creating distributed wireless networks that are resilient to single points of failure and more robust to external disruption. As a DePIN application, DeWI leverages blockchain technology to establish transparent and tamper-proof ledgers to manage access rights, bandwidth allocation, and service agreements within the network. Usually, smart contracts govern the automated execution of network transactions, allowing participants to share their Internet access, and end-users to easily access and use wireless connectivity. Additionally, tokenomics mechanisms incentivize users to contribute to the network in exchange for a reward, e.g., native tokens or user rights, fostering community-driven network growth and sustainability.

Major Active Projects

Helium. The Helium project represents a pioneering project in the realm of DePIN, with the ambition of revolutionizing wireless communication and connectivity. At its core, Helium leverages blockchain technology and a peculiar incentive mechanism to create a decentralized network of hotspots that provide wireless connectivity coverage. Hotspot owners are incentivized to contribute to the network by sharing wireless connectivity and routing data, earning the native token of the project, called HNT, in return for their bandwidth. Initially based on a proprietary Layer 1 Helium blockchain, the project migrated to the Solana chain in April 2023, in an attempt to improve the scalability, reliability, and functionality of its ecosystem. The Helium infrastructure employs a distinctive consensus algorithm known as "Proof-of-Coverage" (PoC) to validate the accurate representation of Hotspots' location, configuration, and wireless coverage. This mechanism is designed to facilitate the deployment of hotspot devices in under-served regions and report their installations honestly.

Wicrypt. Wicrypt is an innovative project focusing on providing decentralized Internet access through a peer-to-peer network. Embracing blockchain technology and smart contracts, Wicrypt enables users to share their Internet bandwidth with others in exchange for cryptocurrency rewards. The infrastructure is built on top of *Minima*, a Layer 1 blockchain ecosystem specifically designed to support DePIN applications. The network is powered by operators, who run routers with the custom Wicrypt firmware, and end-users who utilize connectivity services.

Security and Privacy Issues of DeWI

Legal issues [operators]. This issue has been previously addressed within the context of dVPN and holds equal relevance in the DeWI domain.

Security concerns [operators]. Sharing the Internet connection with unknown users promotes the expansion and accessibility of the network. However, it also introduces the risk of malicious users connecting to the operator's local area network (LAN). In fact, unknown users who gain access to the LAN can exploit vulnerabilities in other devices, launch attacks such as malware infections

or unauthorized access attempts, and compromise the integrity and security of the entire network.

Service Level Agreement (SLA) [operators, end users]. Auditing SLA is a critical issue in many systems. In DeWI applications, this problem is particularly difficult to address. In fact, verifying whether operators actually share the promised bandwidth is not trivial, especially in an open-source, permissionless, and trustless environment. Similarly, ensuring that end-users accurately report their resource consumption presents another challenge, as they may attempt to understate usage to reduce costs. For this reason, any DeWI application must implement a mechanism to resolve possible disputes between operators and end-users regarding service quality and resource usage.

Privacy attacks [end-users]. This issue has been previously addressed within the context of dVPN, and holds equal relevance in the DeWI domain.

5 Decentralized Computation for AI-based tasks

As Artificial Intelligence technologies proliferate across various sectors, the demand for computational resources escalates, often surpassing the capabilities of traditional centralized systems. Decentralized computation presents a novel paradigm, harnessing blockchain technology to distribute computational tasks across a network of peer-contribute resources, thus increasing accessibility, reducing costs, and enhancing the scalability of AI applications. This section delves into the evolution and operational dynamics of major active projects in this domain, examining their impact on the AI landscape and their contribution to the advancement of decentralized computing solutions. In addition, it presents some of the security and privacy issues inherent to these decentralized systems, highlighting the challenges and solutions that define their implementation and use.

Major Active Projects

Render. The Render Network emerges as an innovative decentralized platform that leverages blockchain technology to address the growing demand for GPU computing power in the fields of AI. By enabling individuals and organizations to contribute their idle GPU resources, Render enables a distributed ecosystem that significantly enhances and eases the accessibility and efficiency of computational resources for AI-related tasks. This approach, other than democratizing high-performance computing, introduces an economic model wherein contributors are rewarded with cryptocurrency tokens, incentivizing the participation of GPU owners worldwide. For AI computations and intense rendering tasks, Render offers substantial benefits, including (i) scalability, where the network can dynamically adjust resources based on demand; (ii) cost efficiency, achieved through reduced operational and infrastructure expenses; and, (iii) sustainability.

Fetch.ai. Fetch.ai is a decentralized AI-based project that aims to create an open economic framework for autonomous machine-to-machine (M2M) interac-

tions. The Fetch.ai platform is designed to facilitate the creation of autonomous agent systems, with the aim of delivering efficient, secure, and scalable solutions across various industries, including finance, logistics, and energy. By integrating AI and multi-agent systems with distributed ledger technology, Fetch.ai enables the creation of a decentralized network of agents that can perform tasks autonomously, such as data sharing, transactions, and complex decision-making processes without human intervention. This network is built to be adaptive and self-organizing by design, enabling agents to learn and evolve over time through interaction with the environment (and other agents).

SingularityNET. SingularityNET emerges as a pioneering platform in the intersection of AI and blockchain technology, aiming to democratize access to AI services. Its core mission is to facilitate a decentralized marketplace for AI algorithms, enabling developers, businesses, and AI enthusiasts to buy and sell AI services at scale. This innovative approach aims to mitigate a critical bottleneck in the traditional AI industry: the centralization of AI technologies and resources in the hands of a few major corporations, which limits access and reduces innovation. One of SingularityNET's distinctive features is its commitment to interoperability and open standards. The platform is designed to support AI services developed in various programming languages and running on different operating systems, making it an agnostic ecosystem for AI technologies.

Security and Privacy Issues of Decentralized Computation

The innovative integration of blockchain and AI technologies promotes a new era in computing, promising enhanced decentralization, efficiency, and access to computational resources. However, the deployment of such decentralized networks for AI-based tasks, exemplified by platforms like Render, Fetch.ai, and SingularityNET, introduces subtle security and privacy threats. This section explores these challenges, emphasizing the new complexities introduced.

Data Provenance and Integrity Concerns. Data provenance involves tracking the origin, movement, and history of data within the network, ensuring that the information used and generated by AI algorithms can be verified and trusted. Integrity, on the other hand, ensures that data remains genuine, i.e., unaltered, from its source to its destination. The decentralized nature of platforms involving distributed computation, while offering robustness against centralized points of failure, complicates the enforcement of data provenance and integrity. Malicious actors or compromised nodes could potentially inject corrupted, falsified, or malicious data into AI computations, leading to inaccurate and harmful outcomes. For example, a compromised node in the Render network could manipulate computational results or inject malicious data, affecting the reliability and trustworthiness of rendered outputs. Similarly, in Fetch.ai's ecosystem, tampered data could mislead autonomous agents, resulting in erroneous decisions or transactions.

Unverified Contributor Risks. The democratization of computational resources, a key concept in DePIN systems, also poses significant security risks for end-users. By allowing contributions from a broad array of sources, plat-

forms could inadvertently integrate compromised or insecure hardware into their ecosystem. This issue is compounded by the fact that individual contributors' hardware does not undergo rigorous security checks, making the network vulnerable to a range of attacks. For example, an attacker could leverage compromised hardware to perform malicious activities, from snooping on sensitive computational tasks to disrupting network operations through Denial of Service (DoS) attacks.

Integrated System Vulnerabilities. In the complex and dynamic ecosystem of DePIN, integration among heterogeneous systems and collaborations between different projects are commonplace. For example, an imminent merge between Fetch.ai, SingularityNET, and Ocean Protocol has recently been announced[4]. The integration of these distinct platforms–each with its architecture, smart contract protocols, and security frameworks–into a single ecosystem amplifies the risk of generating system vulnerabilities. The complexity of harmonizing different technologies can lead to new, unforeseen security loopholes and privacy concerns, especially in areas where their systems overlap. This complexity is compounded by the need to merge potentially divergent governance models, data management protocols, and cryptographic standards. Possible security and privacy concerns that are worth mentioning include cross-platform compatibility and legacy vulnerabilities, data privacy and integrity across merged platforms, as well as governance and smart contract coordination.

6 Common Security and Privacy Issues

In this section, we report the security and privacy issues that, although emerging from the above-explored domains, are shared by any DePIN application, stemming from their reliance on blockchain technology.

Smart Contract Vulnerabilities. Smart contract vulnerabilities arise from flaws in their design or code, which can be exploited by attackers to manipulate contract outcomes, drain funds, or compromise sensitive information. Given the immutable nature of blockchain, once a smart contract is deployed, it can be extremely difficult to rectify any vulnerabilities without consensus mechanisms or hard forks, both of which can be disruptive and contentious within the community. For instance, a vulnerability in a smart contract used by the Render network to handle transactions for GPU resource contributions could potentially allow an attacker to redirect payments or access computational resources without proper compensation. Similarly, in Fetch.ai and SingularityNET, vulnerabilities could compromise the integrity of autonomous agent interactions or AI service transactioned, leading to loss of funds or unauthorized access to proprietary AI technologies.

Governance Complexities The governance of decentralized networks introduces additional layers of complexity in ensuring security and privacy. Effective governance structures are essential for the establishment of security protocols, privacy policies, and compliance with regulatory requirements. However,

[4] https://fetch.ai/blog/superintelligence-alliance-token-merge-asi

the decentralized nature of these networks often means that governance is distributed among a wide array of participants, each with varying interests and levels of commitment to security practices. This can lead to inconsistencies in the application of security measures and difficulties in responding cohesively to security incidents.

Insufficient Contractual Safeguards Service Level Agreements (SLAs) in decentralized networks often fail to provide robust security and privacy protections. The intrinsic challenge lies in the decentralized architecture, which distributes control and authority across a wide network rather than centralizing it. This dispersion complicates the enforcement of SLAs, as ensuring compliance and accountability becomes significantly more difficult. The lack of centralized oversight means that breaches of privacy or security may not be promptly identified or rectified.

7 Countermeasures

In this section, we propose a set of countermeasures and research directions that can be universally applied to mitigate the security issues discussed above. These strategies aim to mitigate the vulnerabilities inherent in decentralized systems, ensure robust defense mechanisms, and enhance user trust.

Smart Contract Vulnerabilities To minimize the risk of smart contract vulnerabilities, it is critical to implement thorough testing and auditing protocols before contracts are deployed on the blockchain. This includes both automated testing, such as static code analysis and dynamic analysis, as well as manual peer reviews by experienced developers. Developing and using formal verification tools can provide mathematical assurances on the correctness of the smart contracts' behavior, ensuring that they act as intended under all foreseeable conditions. These tools help in identifying and eliminating bugs or security loopholes that could be exploited by attackers. Furthermore, adopting a modular approach to smart contract development can improve security. By isolating different functionalities into separate contracts and limiting interactions between them, the potential impact of a vulnerability in one module can be contained, preventing it from compromising the entire system.

Governance Complexities Addressing governance complexities in decentralized networks involves creating inclusive, transparent, and accountable governance structures. These structures should be designed to facilitate equitable participation from all stakeholders, ensuring that no single entity has undue influence over the network. Implementing Decentralized Autonomous Organizations (DAOs) can provide a democratic framework for managing governance, where decisions are made based on consensus among participants rather than centralized power. This approach can help manage the diverse interests and levels of commitment to security practices within the network. Additionally, regular governance audits and the recording and validation of governance actions on-chain can enhance transparency and trust among participants, ensuring that governance practices are consistently applied and maintained across the network.

Insufficient Contractual Safeguards Improving the robustness of Service Level Agreements (SLAs) in decentralized networks requires innovative approaches to contract design, monitoring, and enforcement. Smart contracts can play a crucial role here, automating the enforcement of SLAs and ensuring transparency. These contracts can be programmed to automatically execute agreed-upon terms and conditions, reducing reliance on manual oversight and increasing efficiency. However, any DePIN project must develop a mechanism to verify off-chain events and assess their compliance with SLAs. The "Proof-of-Coverage" developed by Helium to verify whether participants accurately report their shared resources is a good example in this direction, although still in its infancy and far from being an optimal solution.

Unverified Contributor Risks To mitigate the risks associated with unverified contributors, it is essential to establish a rigorous vetting process. This could involve performing security audits on the hardware and software used by contributors before they are approved to join the network. Such audits can be automated to some extent using AI-driven security tools that scan for known vulnerabilities and compliance with security best practices. Additionally, implementing hardware attestation mechanisms can provide further assurance of the integrity of contributing devices. These mechanisms ensure that only hardware configurations that meet specific security criteria are allowed to participate in the network, significantly reducing the risk of introducing compromised devices.

8 Conclusion

In this paper, we provided a comprehensive exploration of the emerging paradigm of Decentralized Physical Infrastructure Networks (DePIN). Starting our analysis from flagship applications, we have focused on the security and privacy challenges inherent in such systems. Through detailed investigation of two major domains–*Network Services* and *Computation for AI-based Tasks*–we have identified key security issues and proposed both remedial and potential directions for future research and development. Our findings highlight that while DePIN offers significant innovations and advantages over traditional centralized models, such as enhanced user autonomy, economic incentivization through tokenomics, and increased resilience against central points of failure, it also introduces complex security vulnerabilities and privacy concerns. These issues range from smart contract vulnerabilities to the risks associated with unverified contributors and the complexities of managing decentralized governance structures. To address these challenges, we presented several research directions and operational guidelines that include developing more robust security protocols, improving smart contract design and verification, and establishing stronger governance frameworks that can effectively enforce security and privacy standards across decentralized networks. In conclusion, our paper underscores DePIN's transformative potential and security challenges, proposing key research directions to drive the development of more secure and resilient decentralized infrastructures.

Acknowledgements

We acknowledge the use of AI-based tools, such as *Grammarly* and *ChatGPT*, to refine the writing and proofread the final draft of this paper.

References

1. Aoyagi, S., Takizawa, M., Saito, M., Aida, H., Tokuda, H.: Ela: a fully distributed vpn system over peer-to-peer network. In: The 2005 Symposium on Applications and the Internet. pp. 89–92 (2005)
2. Ballandies, M.C., Wang, H., Law, A.C.C., Yang, J.C., Gösken, C., Andrew, M.: A taxonomy for blockchain-based decentralized physical infrastructure networks (depin) (2023)
3. Benisi, N.Z., Aminian, M., Javadi, B.: Blockchain-based decentralized storage networks: A survey. Journal of Network and Computer Applications **162**, 102656 (2020)
4. Caprolu, M., Raponi, S., Oligeri, G., Di Pietro, R.: Cryptomining makes noise: Detecting cryptojacking via machine learning. Computer Communications **171**, 126–139 (2021). https://doi.org/https://doi.org/10.1016/j.comcom.2021.02.016, https://www.sciencedirect.com/science/article/pii/S0140366421000797
5. Fan, X., Xu, L.: Towards a rollup-centric scalable architecture for decentralized physical infrastructure networks: A position paper. In: Proceedings of the Fifth ACM International Workshop on Blockchain-Enabled Networked Sensor Systems. p. 9–12. BlockSys '23, Association for Computing Machinery, New York, NY, USA (2024)
6. Johnson, M., Egelman, S., Bellovin, S.M.: Facebook and privacy: it's complicated. In: Proceedings of the Eighth Symposium on Usable Privacy and Security. SOUPS '12, Association for Computing Machinery, New York, NY, USA (2012)
7. Li, C., Palanisamy, B.: Incentivized blockchain-based social media platforms: A case study of steemit. In: Proceedings of the 10th ACM Conference on Web Science. p. 145–154. WebSci '19, Association for Computing Machinery, New York, NY, USA (2019)
8. Liu, W., Cao, B., Peng, M.: Web3 technologies: Challenges and opportunities. IEEE Network pp. 1–1 (2023)
9. Makridis, C.A., Fröwis, M., Sridhar, K., Böhme, R.: The rise of decentralized cryptocurrency exchanges: Evaluating the role of airdrops and governance tokens. Journal of Corporate Finance **79**, 102358 (2023)
10. Mi, X., Tang, S., Li, Z., Liao, X., Qian, F., Wang, X.: Your phone is my proxy: Detecting and understanding mobile proxy networks. In: 28th Annual Network and Distributed System Security Symposium, NDSS 2021, virtually, February 21-25, 2021. The Internet Society (2021)
11. Minárik, T., Osula, A.M.: Tor does not stink: Use and abuse of the tor anonymity network from the perspective of law. Computer Law & Security Review **32**(1), 111–127 (2016)
12. Moriarty, C.: Is realt reality? investigating the use of blockchain technology and tokenization in real estate transactions. Minn. JL Sci. & Tech. **24**, 471 (2022)
13. Rader, E.: Awareness of behavioral tracking and information privacy concern in facebook and google. In: 10th Symposium On Usable Privacy and Security (SOUPS 2014). pp. 51–67. USENIX (2014)

14. Raponi, S., Caprolu, M., Di Pietro, R.: Intrusion detection at the network edge: Solutions, limitations, and future directions. In: Zhang, T., Wei, J., Zhang, L.J. (eds.) Edge Computing – EDGE 2019. pp. 59–75. Springer International Publishing, Cham (2019)
15. Sarkar, D.: Generalised depin protocol: A framework for decentralized physical infrastructure networks (2023)
16. Varvello, M., Azurmendi, I.Q., Nappa, A., Papadopoulos, P., Pestana, G., Livshits, B.: Vpn-zero: A privacy-preserving decentralized virtual private network. In: 2021 IFIP Networking Conference (IFIP Networking). pp. 1–6 (2021)
17. Wolinsky, D.I., Lee, K., Boykin, P.O., Figueiredo, R.: On the design of autonomic, decentralized vpns. In: 6th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2010). pp. 1–10 (2010)
18. Xiao, Y., Varvello, M., Kuzmanovic, A.: Monetizing spare bandwidth: The case of distributed vpns. Proc. ACM Meas. Anal. Comput. Syst. **6**(2) (jun 2022)
19. Xu, J., Paruch, K., Cousaert, S., Feng, Y.: Sok: Decentralized exchanges (dex) with automated market maker (amm) protocols **55**(11) (feb 2023)