SoK: DePIN Data Layer for Modular Blockchain

***Abstract*—Blockchain Layer 2 solutions share the goal of moving computational processes and data off-chain. Along with modular design they become the new norm for blockchain scalability solution. These approach provide additional layers built on top of Layer 1 to process transactions more efficiently, relieving congestion on the Layer 1. However, within the modular architecture of Layer 2, the data layer introduces trade-offs. One of these trade-offs involves the reliance on third-party decentralized storage services for data availability. These third-party decentralized storage services, while providing benefits data availability, also introduce potential risks and dependencies. Users may have concerns about data availability, reliability, and security when relying on external storage providers. DePIN leverages blockchain rewards to incentives the development of physical infrastructure networks. These networks could potentially provide data availability services for blockchain networks. By integrating physical infrastructure with blockchain technology, DePINs can offer reliable and secure data storage solutions that are decentralized and resistant to censorship or manipulation. This paper introduces the concept of using DePIN for the data availability layer in modular blockchain systems. It begins by reviewing the layer 2 ecosystem and its limitations. The proposed concept could serve as motivation for further research into DePIN-based data layers for blockchain systems.**

***Index Terms*—blockchain, layer 2 solutions, scalability, modular design, Decentralized Physical Infrastructure Network**

I. Introduction

In the realm of blockchain technology, Layer 2 ($L2$) scaling solutions have emerged as a compelling answer for its scalability limitation. In the context of blockchain, scalability refers to the system's ability to maintain performance as it grows and expands (1). Scalability is widely recognized as a significant technical limitation hindering widespread adoption of blockchain (2). Several methods are currently in development or practice aimed at improving the scalability of blockchain networks. These include optimization of block size (3); adopting alternative consensus architectures (4; 5; 6; 7; 8) which replaces the computationally intensive consensus process to increase the network's transactions per second (TPS) capability; sharding (9; 10; 11), a concept from distributed databases that breaks data into smaller datasets, known as *shards* and recent development of $L2$'s and rollups work by maintaining transaction execution and state off-chain (12). Rollups specialize in offloading specific tasks from the primary blockchain ($L1$) to secondary blockchains ($L2$) to enhance performance.

$L2$, despite being proposed as an effective scaling solution for blockchains, can face data availability problems (13; 14). This issue arises because rollups rely on a $L2$ to process and store transactions off-chain, and then submit a compressed summary of those transactions to the $L1$. However, if the data on the $L2$ becomes unavailable or inaccessible, it can lead to challenges in verifying the validity of transactions and accessing the full transaction history. This data availability problem can potentially undermine the security and trustworthiness of the rollup solution (15). Therefore, ensuring robust data availability mechanisms and maintaining accessibility to the $L2$'s data are crucial aspects in mitigating this challenge.

DePIN, short for Decentralized Physical Infrastructure Network, is a revolutionary concept connecting physical deceives in a decentralised manner utilizing tokenization to incentivize empowered by blockchain technology (16). In this model, individuals contribute to building up the infrastructure in a decentralized manner and receive token rewards as incentives. The fundamental idea is build decentralised infrastructure by incentives participation through token rewards. DePIN has the potential to address the data availability problem for blockchain rollups (17; 18). By leveraging physical infrastructure networks, DePIN can potently provide a reliable decentralized data availability layer for rollups (19).

In this paper, we delve into the current state of blockchain L2 solutions and DePIN, exploring their respective roles in addressing scalability limitations and data availability challenges within the realm of blockchain technology. Identify its use case and propose some future research direction.

II. Layer 2 networks

Layer 2's are blockchain scaling solution which are secondary protocols or networks built on top of a primary blockchain that aim to extend the capabilities of that primary blockchain (12). Within this architecture, we define $L1$ as the primary blockchain, guaranteeing security through decentralisation or asset locking within it and $L2$'s aid in scaling the $L1$ by handling processes such as computations that would traditionally run on the $L1$. As of first quarter of 2024, most common $L2$ solutions are state channels, sidechains and rollups.

State channels enable two participants to conduct off-chain transactions through a dedicated channel after locking a segment of account state on the main chain. Participants update the account state among themselves and temporarily holding it until a agreed time and updated state back to the primary blockchain. This off-chain process facilitates rapid updates without constant the primary blockchain involvement is a key strength of state channels (20; 21). On the other hand, sidechains operate as separate blockchains linked to a primary blockchain, usually the main chain. They handle specific tasks or operations independently, alleviating the primary blockchain from processing every transaction. Users can transfer assets or data between the primary blockchain and the

sidechain, allowing flexibility while preserving a connection to the primary blockchain's security.

Rollups are a type of off-chain solution that specialize in execution component of blockchain system. Rollups, as execution solutions, offload computation from the primary blockchain $L1$ to $L2$ to enhance performance. As of 2024 there are two primary types of rollups exist: Optimistic rollups and Zero-Knowledge (ZK) rollups (22).

With rollups, the main chain, such as Ethereum, serves as the primary layer for securing the network and settling disputes. Off-chain transactions occur within the rollup layer, where they are processed quickly and cost-effectively. Rollups leverage techniques to aggregate and compress transaction data, allowing multiple transactions to be bundled into a single batch. Validators or operators execute and validate these transactions off-chain, utilizing optimized execution environments. After processing, a succinct summary of the transaction data, known as a rollup block, is generated and submitted to the main chain along with cryptographic proofs for verification and anchoring. Validators or users are incentivized to ensure data availability and honesty through fraud proofs or challenges. Once confirmed on-chain, the rollup block finalizes the corresponding transactions, updating state changes or balances. Rollups typically support various settlement periods, allowing users to withdraw funds back to the main chain after a waiting period (23).

III. Decentralized physical networks

DePINs, are networks that use token incentives to motivate individuals to share their physical resources and services. DePIN are been projected as new way of building and operating decentralised infrastructure such as wireless networks, cloud services, mobility networks, and power grids which are mostly dominated by large companies due to high capital requirements (24; 25; 26). Centralized entities successfully in establishing digital platforms leverage the power of the community to develop web applications. For instance, platform service such as Uber and Airbnb utilize individuals to offer physical resources and services to the platform and make these services accessible to a broad user base. In return, the resource and services providers receive payment for their services.

Centralized corporations have historically dominated the deployment and management of physical infrastructure, resulting in limited competition. These corporations dictate pricing and conditions for end-users, effectively monopolizing the market. DePIN project seeks to counter these issues by decentralization and democratization of infrastructure deployment and management. Unlike traditional centralized systems, DePIN distributes control, decision-making, and resources across a network of nodes, fostering autonomy and decentralization. Token incentives within DePIN ecosystems drive the creation of real-world infrastructure, incentivizing builders to develop applications.

A. Operation of DePIN

A DePIN system consists of a set of network nodes coordinated in a peer-to-peer manner, forming an ecosystem that builds, maintains, and operates system infrastructure in an open and decentralized manner. These node integrate physical devices to provide services such as generate data using IoT sensor devices, provide services such as hotpot for wireless connectivity, data storage network. These network participants receive rewards for contributing to the network services through a blockchain token rewards schema.

Through incentivized rewards, DePin aims to enhance engagement and promote active participation. Individuals contributing to the network will receive rewards, fostering a sense of ownership and deeper investment in the network's success. DePINs enable anyone with appropriate hardware to become an infrastructure provider, thereby lowering barriers to entry for new players, reducing capital investment for projects, democratizing access and ownership of infrastructure, and decreasing reliance on centralized monopolies. As participants take specific actions and witness the direct impact of their contributions, they are motivated to continue their involvement, thereby strengthening the overall network ecosystem.

B. DePIN Projects

Several DePIN projects have transformed infrastructure provision by centralized enterprises into a form of crowdsourcing that involves users worldwide. The concept of DePin is now a hot topic among crypto enthusiasts, promising a revolution in decentralized physical infrastructure.

a) : Filecoin (27) is revolutionizing data storage with its decentralized network, where independent miners a providing storage space and earn tokens rewards for their contributions. Users can store files which will be stored across multiple miners for redundancy and security. Clients can retrieve their data at any time by paying retrieval fees to the miners. Since its main launch in 2020, *Filecoin* has experienced substantial growth, boasting a raw storage capacity of 7.6 XB bytes. *Filecoin* offers a decentralized alternative to traditional cloud storage services, leveraging blockchain technology to provide secure, reliable, and efficient data storage solutions.

b) : WiFi Maps is decentralized Wifi platform that aims to provide internet access through a DePIN infracture. *WiFi Maps* offers opportunities for users to connect, earn rewards, receive cashback, redeem points, and engage in various activities (28).

c) : Helium (29) exemplifies the essence of a DePIN system, representing a decentralized wireless infrastructure revolution. Users set up hardware units to establish a network that offers 5G Wi-Fi coverage. Praised for its extensive hardware deployment, *Helium* provides practical solutions for decentralized connectivity. Much like *Helium*, other DePINs address various infrastructure requirements, including solar power, cloud storage, and computing power.

d) : IoTeX (30) is dedicated to the Internet of Things (IoT) and developing security and privacy solutions via decentralized hardware. Positioned as a platform for DePIN de-

velopers, *IoTeX* seeks to enable billions of devices and dApps across both physical and digital realms. Utilizing *IoTeX*'s decentralized devices enhances security and privacy for users, who are rewarded with *IOTX* tokens in exchange.

e) : Hivemapper[1] a decentralized version of Google Maps through a DePIN project functions by integrating real-world physical devices of dash cams installed by users in their cars) that generate and share data via live footage (31).

DePIN emerges as a solution to address many critical challenges and limitations within the decentralized ecosystem. In this paper, we particularly focus on the scalability bottleneck associated with data storage within the $L2$ solutions. This decentralized infrastructure model has the potential to provide reliable decentralized data storage infrastructure for the modular architecture.

IV. $L2$ MODULAR LANDSCAPE

Modularity refers to a design principle where different functions of a system are separated into discrete modules or layers often referees as level in a modular design (32; 33). A modular architecture is designed to separate a system's functions into layers compared to monolithic architecture, which handles all its function activities in a single layer. For example a monolithic blockchain is a blockchain that performs all its essential tasks in to a single foundational layer and a blockchain that manages select tasks in its base layer and delegates the remainder to additional layers (refers as layer 2) is defined as a modular blockchain.

In a monolithic architecture all system operations occur within a single cohesive environment, represented as $M = f(x, x', x'')$, with M denoting the monolithic architecture and x, x', x'' as operations. And a modular system, denoted as $M' = f(x \parallel x' \perp\!\!\!\perp x'')$, is constructed around distinct, parallel, or independent execution operations. Each operation addresses specific tasks, where tasks are specific operations. A monolithic architecture is constrained by its operation capability confined to a single layer where all operations are executed within a single cohesive environment. A modular architecture is built around distinct modules. Each module in such an architecture addresses specific tasks. Furthermore, these tasks can be managed by multiple $L2$ networks layered over a foundational multi-purpose $L1$. By compartmentalizing these functions across distinct layers, modular blockchains endeavor to elevate overall performance through the mechanism of vertical scaling.

The terms layer and module describe different elements within a system. This has been interchangeable used therefor we make dissected definition in the contest of information system.

Definition 1 (Layer)**.** A layer is a logical division or abstract section within a system, serving a distinct purpose or encapsulating specific functionalities.

In software design, layers act to compartmentalize functions, fostering modularity. Each layer manages designated tasks or operations and engages with other layers in a predefined manner.

Definition 2 (Module)**.** A module refers to a self-contained unit of code or functionality that serves as a foundational element within a system.

Typically, modules encapsulate a specific set of related functions or operations. They are crafted to be modular and reusable, facilitating the organization and control of code complexity. Consider modules as independent units capable of effortless integration into various parts of a system.

A. Modular Design

The modular thesis proposes a distinct strategy for scaling blockchains compared to the layered approach: rather than stacking solutions on top of each other, it advocates for abstracting specific functions into separate systems. In a modular blockchain framework, functions like execution, consensus, and data availability could operate across distinct networks. This approach holds the potential to enhance system scalability and efficiency significantly. Additionally, it facilitates easier expansion or modification of module functions without disrupting the entire framework. Moreover, it enables the reusability of modules across different systems, leading to substantial savings in development time and resources.

A recent survey conducted on distributed ledger technology (DLT) by Bellaj et al. (34) delineated four fundamental layers within the DLT stack: data, consensus, execution, and application. These layers respectively govern the recording of system state, the establishment of agreement among participants via a software-defined ruleset, computational processes, and the facilitation of APIs for decentralized application (DApp) development. Building upon current research (35; 36), this paper highlights *execution*, *data*, and *consensus* as the primary functional components that can be modularized within a blockchain system. Depending on the system configuration, each of these modules may be distributed across different nodes or systems.

Definition 3 (Consensus)**.** The consensus module facilitates the mechanism for reaching *consensus*, a collective agreement on the global state.

Consensus in the context of blockchains refers to an ordered sequence of blocks on a $L1$ network. The module provides network security where the proof of state transaction is anchored. In the modular design a consensus module may not keep data related to state transaction on $L2$. Instead, keep the account state and its balance on $L1$. In order for validators to verify the state transaction on $L2$ the proposer must post the relevant data with the block proposal. After other validators validate and approve the state change, the data associated with that state change form $L2$ will be part of a separate data module.

Definition 4 (Execution)**.** This module handles the computation aspect.

Execution module is where the application's business functional logic will be deployed. The application primarily inter-

[1]https://www.hivemapper.com/explorer

acts with this module to process transactions. This module may utilize $L2$ network, rollups system, external data sources or other blockchain sources to perform the business logic. Once the business process is completed, the final results, such as the state of an account, are updated on the $L1$ chain. Importantly, $L1$ does not need to process the business logic; it only verifies whether the data provided for the state change is valid.

Definition 5 (Data)**.** The data module is meant to providing data for all the primitives necessary for validation, verification or execution of state transaction.

The term data module in the context of blockchain refers to a data availability infrastructure or service for the blockchain ecosystem. This infrastructure is designed to provide data related to state changes from other modules. The data module acts as a crucial component that ensures data availability. Otherwise, it might suffer from inadequate data availability problem.

B. Data Availability

Data availability in blockchain is to do with the assurance that all necessary data for verifying a state transaction is available when and where they needed (37; 38). In the context of the $L2$ ecosystem, data availability relates to ensuring that the data necessary to verify a $L2$ state transaction is accessible to $L1$ or any other network participants.

For a $L2$ system, the data availability requirement aims to demonstrate to network participants that all necessary data to verify transaction execution is accessible. Technically, this approach creates bottlenecks with data storage and availability when all nodes are required to keep a copy of the data for validation. To address this limitation, $L2$ solutions use forms of data availability layer (39).

C. Problem Definition

$L2$ solutions, aimed at offloading computational processing and data off-chain, have become the new standard for addressing blockchain scalability issues. They add supplementary layers on top of $L1$ to facilitate more efficient transaction processing, thus alleviating congestion on the $L1$ network. However, within the modular architecture of $L2$, the data layer introduces certain trade-offs.

One such trade-off involves relying on third-party decentralized storage services for data availability. While these services offer benefits in terms of data availability, they also bring about potential risks and dependencies. Users may have concerns regarding the reliability, security, and availability of data when depending on external storage providers.

This is where DePIN enters the picture. DePIN utilizes blockchain incentives to encourage the development of physical infrastructure networks. These networks have the potential to provide data availability services for blockchain networks. By integrating physical infrastructure with blockchain technology, DePINs can offer decentralized and resilient data storage solutions, mitigating concerns related to censorship or manipulation.

V. The appchain Design

A modular appchain is a tailored solution designed to meet the unique requirements of a decentralized application or Web3 protocol (40). These specialized blockchains have independent application-specific functions and operate on top of other blockchains. What sets them apart is its focus on specific tasks and their efficiency in handling those tasks. Their unique environments, fine-tuned for specific applications, allow for efficient processing and utilisation of resources. Their specialization makes them ideal for applications requiring unique functionality such as high throughput and security. Modular appchain architecture offers a flexible and sovereign solution for many Web3 applications (41).

A. Appchain architecture

Figure 1 outlines a design approach for appchain, incorporating different modules for various functionalities.. The design goals are i) Separate tasks into different layers. ii) Each layer maintain its own state. iii) Facilitating efficient resource sharing, whereby an appchain can utilize multiple layer ($L1$ and $L2$) and resources based on its design requirement. These appchains can bee configured based on its system requirement such as $L1$ for security, $L2$ and rollup for execution and DePIN for data layer.

Let us define the execution layer function denoted as $f()$ by taking two inputs: a prior state, represented as p, and a transaction root hash, represented as $H(Tr)$. For this execution to commence, the data layer provides the required previous state, $p = Data()$ and application interface will provide transaction data to form Tr. When these inputs are processed through the function, the outcome is a new state:

$$f(p, H(Tr)) = p'$$

And finally, at the network level, the consensus layer participants compute p' and validate it. The underlying principle is that after processing, all validating nodes should converge on an identical state, p', which will be regarded as a global state. The data within prior state, p consist of hash of block headers $H(h_0, h_1, ...h_n)$. We purposely omit other fields in the bock for clarity. Each block header h_i contains of Merkle tree root of list of transactions Tx_i given as

$$h_i = (Tx_i^0, Tx_i^1, ...Tx_i^n)$$

A block header h_i is considered valid if any validate node execution function $f(p, h_i)$ return true, such that $h_i \subset p$, but not necessarily $Tx_i \in p$.

For a block to be included in the global state, network nodes employ a consensus function $C()$ distinct from block validation. The validity of a block proposed by a validator is subject to a slashing condition if proven to be incorrect. The entire dataset required to validate a block might not be part of the p but could be available on another network. $C()$ should return true if and only if $f(p, h_i)$ returns true. The validator is responsible for both validating and proposing the block. Other validators can access this off-chain data to validate it, and if

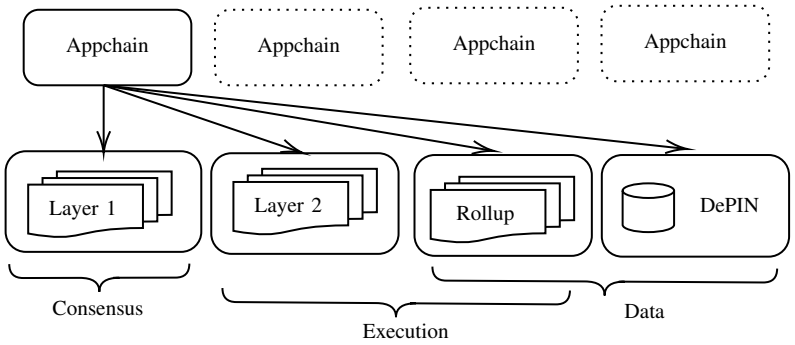

Fig. 1. Blockchain modular application architectures.

the proposed block is found to be invalid, they can claim a penalty bounty.

In a appchain architecture, the state of on-chain data p get extended using a combination of on-chain (p) and off-chain (Tx_i) data. Validates who got access to Tx_i proposed blocks (Tx_i) for global state G. The two distinct functions that are part of the total ecosystem are block validation function $f()$ and global state validation function $g()$.

The differences between a $L2$ and an appchain approach is in he former, the application is deployed either on $L1$ and $L2$ solution is used improve the performance of $L1$ chain or application is deployed on $L2$ and it used $L1$ for security. In many ways $L1$ and $L2$ connected and function within the capability of the weakest chain. Whereas, the appchain proposes a different strategy. let us assume there exist many modular blockchain with different capabilities an appchain can simultaneously utilises both $L1$ and $L2$ networks. In this model, the appchain leverages specific features, such as security from $L1$, computational capabilities from $L2$ and data form DePIN. The key difference is that $L1$ and $L2$ are not dependent on each other in the appchain thesis. Instead, the application interacts with different layers independently, leveraging their respective strengths to optimise performance.

B. Appchain use case

Let us assume a digital asset trading application, tracking property ownership. The ownership title is registered on $L1$ chains, and all secondary details on $L2$ chains. The application's blockchain requirement is to verify property ownership; secondary data is not as important as long as the main chain has proof of ownership. In other words, secondary information may be available to a set of authorities who are part of verifying the deal and facilitate the transfer. Below are the list of assumptions for this application design.

- A $L2$ execution module performed off-chain, and an execution proof as witness then be committed to the execution $L1$.
- The specifics of $L2$ execution data may not available on the $L1$. Instead, a reference is provided, and the data is available on an DePIN system.

In the event of ownership transfer, say through a sale, the sale occurs on a $L2$ chain and once it is finalized on $L2$, the proof of sale and transfer data is posted for verification by proposer to a set of validators on $L1$. It will then be verified and validated by proposers, before changing the ownership. Once the ownership transfer is complete, it will have a reference to the proof of sale and transfer data on DePIN module. Anyone can verify the ownership, but for the proof of sale and transfer data, they would need to obtain it DePIN data layer module.

C. Construction

In this construction, asset ownership is managed through an application interface designed with a modular framework. Participants interact with this interface to manage their digital representations of physical assets. Let us assume a scenario where an existing user, having registered a digital representation of a physical asset within this system, initiates a transaction to transfer ownership of the underlying physical asset to another user. The interface first verifies a user's asset ownership status defined as a function that verifies whether a user has ownership rights for a particular asset on $L1$ chain.

$$O = VerifyOwnership(user, asset)$$

Here, O is a boolean variable representing the result of ownership verification. Once verified, the application proceeds with the asset transfer request. The intricacies of the business transfer logic, involving multiple parties, potential interactions with other chains, and DePIN data sources, are executed on the $L2$ chain.

$$T = ExecuteTransferLogic(O, data(d1, d2...dn))$$

The application interface orchestrates the gathering of essential data for this transaction from various sources. T represents the successful execution of business transfer logic on $L2$. It depends on the ownership verification result O and data gathered from various sources such as $d1, d2..dn$. Upon successful validation and verification of the business process on the $L2$ chain, a request to update the asset ownership information is relayed back to the $L1$ chain.

$$UpdateOwnership(T, asset, newOwner)$$

This update request dependant on successful execution of the business transfer logic on $L2$ ($T = True$), and consensus

requirement set by the application logice for the $L1$ chain to authenticate and facilitate the ownership transfer. $L1$ then conducts the validation process and officially updates the asset ownership to the new address. Notably, the specific data pertaining to this transfer process is not stored on the main chain; instead, it remains accessible on a DePIN data layer, serving as the verification source for the ownership transfer. This approach optimizes the system by leveraging the $L2$ solution for data availability while relying on the main chain's integrity for validating and updating asset ownership records.

VI. Conclusion and future work

Within the blockchain ecosystem the appchain approach harnesses significant potential for scalability by integrating modules architecture. This design approch offers enhanced adaptability compared to a single $L2$ off-chain solutions, empowering blockchain application to flexibly accommodate various functionalities and scalability requirements.

DePIN infrastructure is gaining a lot of traction in the Web3 and blockchain communities. Among many notable physical infrastructure solutions, DePIN has the potential to serve as a data layer for modular blockchains, which is crucial for blockchain applications. The motivation behind this research is to highlight the limitations of scalability solutions and suggest directions for upcoming technologies. Future work in this area involves developing a protocol for the data layer system on DePIN, designing its incentive model, analyzing factors such as security and privacy, and making recommendations on how it can be implemented.

VII. Acknowledgment

We would like to acknowledge the utilization of advanced AI tools aimed at enhancing the writing quality of this paper.

References

[1] G. Hileman and M. Rauchs, "2017 global blockchain benchmarking study," *Available at SSRN 3040224*, 2017.

[2] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—a systematic review," *PloS one*, vol. 11, no. 10, p. e0163477, 2016.

[3] N. Singh and M. Vardhan, "Computing optimal block size for blockchain based applications with contradictory objectives," *Procedia Computer Science*, vol. 171, pp. 1389–1398, 2020.

[4] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. Gün Sirer *et al.*, "On scaling decentralized blockchains: (a position paper)," in *International conference on financial cryptography and data security*. Springer, 2016, pp. 106–125.

[5] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Annual international cryptology conference*. Springer, 2017, pp. 357–388.

[6] L. Luu, V. Narayanan, K. Baweja, C. Zheng, S. Gilbert, and P. Saxena, "Scp: A computationally-scalable byzantine consensus protocol for blockchains," *Cryptology ePrint Archive*, 2015.

[7] R. Pass and E. Shi, "Hybrid consensus: Efficient consensus in the permissionless model," *Cryptology ePrint Archive*, 2016.

[8] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "{Bitcoin-NG}: A scalable blockchain protocol," in *13th USENIX symposium on networked systems design and implementation (NSDI 16)*, 2016, pp. 45–59.

[9] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 17–30.

[10] M. Zamani, M. Movahedi, and M. Raykova, "Rapidchain: Scaling blockchain via full sharding," in *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*, 2018, pp. 931–948.

[11] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "Omniledger: A secure, scale-out, decentralized ledger via sharding," in *2018 IEEE symposium on security and privacy (SP)*. IEEE, 2018, pp. 583–598.

[12] C. Sguanci, R. Spatafora, and A. M. Vergani, "Layer 2 blockchain scaling: A survey," *arXiv preprint arXiv:2107.10881*, 2021.

[13] R. Neiheiser, G. Inácio, L. Rech, C. Montez, M. Matos, and L. Rodrigues, "Practical limitations of ethereum's layer-2," *IEEE Access*, vol. 11, pp. 8651–8662, 2023.

[14] A. Mustafa, N. Siddique, and M. Zubair, "Data link layer security problems and solutions," 2015.

[15] Oxorio, "Securing layer 2: Unique security concerns and mitigation strategies," 2023, https://blog.oxor.io/securing-layer-2-unique-security-concerns-and-mitigation-strategies- [Accessed: (11/11/2023)].

[16] J. Agbo, "What is the decentralized physical infrastructure (depin) narrative in crypto?" 2024, https://www.coingecko.com/learn/depin-crypto-decentralized-physical-infrastructure-networks [Accessed: (4/3/2023)].

[17] X. Fan and L. Xu, "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*, 2023, pp. 9–12.

[18] J. Finance, "Dismantling the bitcoin/ethereum layer 2 security model and risk indicators," 2024, https://www.coinlive.com/news/dismantling-the-bitcoin-ethereum-layer-2-security-model-and-risk-ir [Accessed: (1/1/2024)].

[19] Crytoray, "Decoding depin: The decentralized future of real-world infrastructure," 2024, https://www.publish0x.com/syntropy-network/decoding-depin-the-decentralized-future-of-real-world-infras-xyqqxr

[Accessed: (1/3/2023)].

[20] D. Tien Tuan Anh, W. Ji, C. Gang, L. Rui, and A. Blockbench, "Framework for analyzing private blockchains," in *Proceedings of the 2017 ACM International Conference on Management of Data, Chicago, IL, USA*, 2017, pp. 14–19.

[21] A. Miller, I. Bentov, R. Kumaresan, and P. McCorry, "Sprites: Payment channels that go faster than lightning," *CoRR, abs/1702.05812*, 2017.

[22] L. T. Thibault, T. Sarry, and A. S. Hafid, "Blockchain scaling using rollups: A comprehensive survey," *IEEE Access*, 2022.

[23] L. Gudgeon, P. Moreno-Sanchez, S. Roos, P. McCorry, and A. Gervais, "Sok: Layer-two blockchain protocols," in *Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers 24*. Springer, 2020, pp. 201–226.

[24] Greythorn, "The rise of depin networks," 2024, https://www.linkedin.com/pulse/rise-depin-networks-greythorn-asset-management-bertf/?trk=article-ssr-frontend-pulse_more-articles_related-content-card [Accessed: (1/3/2023)].

[25] P. D. Hines, S. Blumsack, and M. Schläpfer, "Centralized versus decentralized infrastructure networks," *arXiv preprint arXiv:1510.08792*, 2015.

[26] M. C. Ballandies, H. Wang, A. C. C. Law, J. C. Yang, C. Gösken, and M. Andrew, "A taxonomy for blockchain-based decentralized physical infrastructure networks (depin)," *arXiv preprint arXiv:2309.16707*, 2023.

[27] D. P. Bauer, "Filecoin," in *Getting Started with Ethereum: A Step-by-Step Guide to Becoming a Blockchain Developer*. Springer, 2022, pp. 97–101.

[28] WifiMap, "Wifi map digest: 28 april 2023," 2023, https://medium.com/wifi-map/wifi-map-digest-28-april-2023-2f0e8053d0f1 [Accessed: (11/11/2023)].

[29] V. Rammouz, J. Khoury, . Klisura, M. S. Pour, M. S. Pour, C. Fachkha, and E. Bou-Harb, "Helium-based iot devices: Threat analysis and internet-scale exploitations," in *2023 19th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, 2023, pp. 206–211.

[30] I. Team, "Iotex: a decentralized network for internet of things powered by a privacy-centric blockchain," *IoTeX Team*, 2018.

[31] H. Seth, "Hivemapper," 2024, https://docs.hivemapper.com/welcome/introduction [Accessed: (11/10/2023)].

[32] S. Mittal, Y. Bengio, and G. Lajoie, "Is a modular architecture enough?" *Advances in Neural Information Processing Systems*, vol. 35, pp. 28 747–28 760, 2022.

[33] C. Cachin *et al.*, "Architecture of the hyperledger blockchain fabric," in *Workshop on distributed cryptocurrencies and consensus ledgers*, vol. 310, no. 4. Chicago, IL, 2016, pp. 1–4.

[34] B. Bellaj, A. Ouaddah, E. Bertin, N. Crespi, and A. Mezrioui, "Sok: a comprehensive survey on distributed ledger technologies," in *2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2022, pp. 1–16.

[35] Y. Hao, Y. Li, X. Dong, L. Fang, and P. Chen, "Performance analysis of consensus algorithm in private blockchain," in *2018 IEEE Intelligent Vehicles Symposium (IV)*. IEEE, 2018, pp. 280–285.

[36] M. Kaur and S. Gupta, "Blockchain consensus protocols: state-of-the-art and future directions," in *2021 International conference on technological advancements and innovations (ICTAI)*. IEEE, 2021, pp. 446–453.

[37] H. Si and B. Niu, "Research on blockchain data availability and storage scalability," *Future Internet*, vol. 15, no. 6, p. 212, 2023.

[38] X. Liu, S. Ji, X. Wang, L. Liu, and Y. Ren, "Blockchain data availability scheme with strong data privacy protection," *Information*, vol. 14, no. 2, p. 88, 2023.

[39] A. D. Mas, "Data availability layer: Enabling scalability in blockchain networks," 2023, https://www.linkedin.com/pulse/data-availability-layer-enabling-scalability-networks-andrea-dal-mas/ [Accessed: (1/1/2024)].

[40] J. Surmont, W. Wang, and T. Van Cutsem, "Static application security testing of consensus-critical code in the cosmos network," in *2023 5th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*. IEEE, 2023, pp. 1–8.

[41] D. Berenzon, "Application-specific blockchains: The past, present, and future," 2022, https://medium.com/1kxnetwork/application-specific-blockchains-9a36511c8 [Accessed: (11/1/2024)].