Blockchain-based Internet of Things-Networks in environmental data pipelines - exploring opportunities and a use case

Hanna Fiegenbaum[a], Bradley Azegele[b] and Stephan Seider[b]

[a]*Leipzig University, Institute for Medical Informatics, Statistics, and Epidemiology; Gefion/WoodenValley gGmbH*
Email: hanna.fiegenbaum@gmail.com, hanna.fiegenbaum@uni-leipzig.de
[b]*BLCK IOT, Berlin/Nairobi*
Email: hello@blck-iot.com

Abstract: Blockchain-based IoT-Networks are part of an evolving field termed decentralized physical infrastructure networks (DePIN), encompassing ways of decentralizing, incentivizing, and rewarding operation and maintenance of technical infrastructure and networks. This paper examines the features by which the integration of blockchain and IoT networks could address challenges in the design and governance of environmental data pipelines. It further reports on the findings from deploying IoT devices on the blockchain-based Helium Network in a pilot use case for measuring regulating urban ecosystem services in a community-based urban green space restoration project in Nairobi, Kenya.

Introduction

To assess drivers of climate change, pollution and nature loss as well as for monitoring the state and functioning of ecosystems, increasingly large amounts of data and monitoring efforts from different sources are needed at temporal and spatial scale (TNFD et al., 2023). Not only governments and public organizations monitor pollution, environmental services and ecosystems. Also the private sector is encouraged to acquire more climate- and nature-related data for reasons of reporting obligations, for tracking targets and changes in state of nature, biodiversity and ecosystem services and to manage impacts on climate and biodiversity (Addison et al., 2018; zu Ermgassen et al., 2022). New technologies such as eDNA, remote sensing, IoT networks, bioacoustic data, are increasingly used to collect and combine various types of climate- and nature-related data and for monitoring specific parameters.

Blockchain-based IoT-monitoring networks are part of an evolving field termed decentralized physical infrastructure networks (DePIN), encompassing ways of decentralizing, incentivizing, and rewarding operation and maintenance of technical infrastructure and networks. This paper examines the features by which the integration of blockchain and IoT networks could address challenges in the design and governance of environmental data pipelines. It further reports on the findings from deploying IoT devices on the blockchain-based Helium Network in a pilot use case for measuring

regulating urban ecosystem services in a community-based urban green space restoration project in Nairobi, Kenya.

IoT

The Internet of Things (IoT) refers to the network of physical objects that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems through a communication technology that provides connectivity to the internet. Using the IoT for environmental monitoring involves the deployment of interconnected devices and sensors to collect, transmit, and analyze data about the environment. Functions of IoT devices can be broadly categorized into two types: sensing and actuating. Sensing devices collect data from their environment, such as temperature, humidity, light levels, motion, air quality, to gather information and transmit it for analysis, monitoring, or alerting purposes. Actuators in IoT devices are used to perform a physical action in response to a command, which can be triggered manually by a user or implemented automatically. Real-time monitoring ensures that changes and anomalies in the environment can be detected immediately, allowing for quick responses to potential environmental threats or changes. IoT enables remote monitoring of environmental conditions, without the need for human presence. This is particularly valuable in inaccessible or hazardous areas. IoT-enabled environmental monitoring can inform decision-making, support with optimization of resource use and planning, help enforce environmental regulations, and provide the database for evaluating conservation strategies.

Communication protocols - LP-WAN

Depending on the conditions of the specific use case, IoT deployment solutions have distinct requirements regarding radio coverage, scalability, and power consumption. Operational requirements to use IoT at a large temporal and spatial scale include conditions such as low data rate, long-range transmission, low energy consumption and low cost. Meeting these requirements is dependent on the communication protocol that is used. While several wireless communication protocols are available, only Low Power Wide Area Networks (LP-WAN) (Raza et al., 2017) meet all of these requirements. LP-WAN are wireless technologies that provide large coverage areas, low bandwidth, support small packet sizes, application layer data sizes, long battery life operation and low power consumption (Anastasiou et al., 2023). Among the different LP-WAN, LoRaWan protocol is increasingly used in IoT environmental monitoring. LoRaWAN (Long Range Wide Area Network) is a protocol for wireless, battery-operated devices which exceeds other protocols in terms of long transmission range, low power consumption and low operational costs (Table 1):

Low Power Consumption: LoRa is the physical layer protocol used in LoRaWAN and it features ‘low power operation, which enables certain devices to last approximately 10

years on a single charge' (Reyneke et al., 2023). Together with the low energy consumption of LoRaWAN communication protocol, this makes LoRaWAN particularly suitable for use cases where devices need to be deployed over a long time period and where electricity is not available.

Long Range: LoRaWAN is a communication protocol specification built on top of the LoRa (Long Range) modulation technique. Due to its Chirp Spread Spectrum modulation technique, LoRa is able to achieve longer transmission ranges than other wireless networks. While stating exact measures for ranges varies, Reyneke et al. (2023) admit ranges from 3-5km in urban areas and up to 20km in rural areas.

Low Data Rate: Low data rates enable signals to travel longer distances, making LoRaWAN suitable for rural and remote monitoring applications where other types of connectivity may not be feasible. Devices designed for low data rate transmission can be simpler and cheaper to manufacture and maintain, reducing the overall cost of IoT deployments. Further, they consume less power when transmitting small amounts of data, leading to extended battery life, which is ideal for remote or hard-to-reach sensor deployments.Transmitting small amounts of data also uses less bandwidth, contributing to reduced network congestion, which is beneficial in densely deployed sensor networks. Low data rate signals can better penetrate obstacles like walls and buildings, improving indoor coverage and connectivity in urban environments. However, LoRaWAN is hence not suitable for handling types of data that need high data rates such as video streaming or any type of high-resolution data. Low data rate furthermore can lead to higher latency, which means there can be a delay in the transmission and reception of data, which may not be ideal for time-sensitive applications. This can however be balanced by higher redundancy of signal transmission.

Network Structure: LoRaWAN employs a star-of-stars network architecture, where end-devices communicate with gateways as points of presence to the network server. LoRaWAN networks are designed for devices to communicate with multiple gateways simultaneously. This increases redundancy because the same message can be captured by more than one point, enhancing the reliability of data transmission.

Open Protocol: LoRaWAN is an open protocol. Its specification (LoRa Alliance, 2017) is publicly available and it is developed by the LoRa Alliance®, a non-profit association of members. Its open nature promotes interoperability and standardization among hardware and software providers.[1]

Spectrum and Regulation: LoRa devices and the LoRaWAN protocol operate in unlicensed ISM (Industrial, Scientific and Medical) bands, which vary by region. Addabo et al. (2019) state unlicensed ISM bands of 868MHz in Europe and 915MHz in North America. Using unlicensed bands allows for flexible deployment, however it also requires compliance with regional regulations.

[1] https://lora-alliance.org/about-lora-alliance/

Low Cost: The use of unlicensed bands implies that anyone can use the frequency without the need to acquire licenses, making it a cost-effective option for wide area IoT deployments (Reyneke et al., 2023). Besides low energy consumption and long battery life, this adds to its low operating costs.

Security: The importance of security in a communication system is on a par with its availability and reliability. The LoRaWAN standard incorporates several security features to ensure secure communications between end devices and the network server.[2] These features include unique network keys for network authentication and application keys for end-to-end encryption, providing a secure method for transmitting sensitive data over the network. LoRaWAN ensures the security of its messages through origin authentication, integrity, replay protection, and uses AES-128 for end-to-end encryption and adds a frame counter to the packets for verification (Blenn and Fernando, 2017). For a device to join the LoRaWAN network, it must undergo mutual authentication, ensuring a secure connection. However, the security effectiveness can be compromised through physical access by an unauthorized user. In such cases, encryption keys are safeguarded in a Secure Element, a tamper-resistant hardware, making key extraction highly challenging (Coman et al., 2019).

Scalability: The protocol is designed to support a wide range of applications. It is able to handle large number of connections, making it suitable for wide-scale IoT deployments, like smart city projects, agricultural monitoring, and industrial IoT applications.

Feature/Protocol	LoRaWAN	WiFi	ZigBee	Bluetooth	4G Cellular	5G Cellular
Bandwidth	Narrow	Wide	Narrow	Narrow to Moderate	Wide	Very Wide
Frequencies	Sub-GHz (e.g., 868 MHz, 915 MHz)	2.4 GHz, 5 GHz, 6GHz	2.4 GHz, 868 MHz, 915 MHz	2.4 GHz	Multiple bands from 700 MHz to 2.5 GHz+	Sub-6 GHz, mmWave (24 GHz and up)
Modulation	LoRa (Chirp Spread Spectrum)	OFDM, DSSS	DSSS, O-QPSK	GFSK, π/4 DQPSK, 8DPSK	QPSK, 16QAM, 64QAM	QPSK, 16QAM, 64QAM, 256QAM
Max Data Rate	<50 kbps	Up to 600 Mbps (802.11n),	250 kbps	1-3 Mbps (Classic), up to 2	Up to 1 Gbps	Up to 10 Gbps and beyond

[2] https://lora-alliance.org/security/

		higher for newer standards		Mbps (BLE)		
Range (Urban)	~2-5 km	~50 m	~10-100 m	~10 m	~1-2 km	~100-500 m (varies greatly with deployment)
Range (Rural)	>10 km	~100 m	~100-200 m	~100 m	~10 km	~10 km+ (varies with deployment)
Transmit Current (Max)	Low	Moderate to High	Low to Moderate	Low	High	High
Transmit Power (Max)	<30 dBm	~20 dBm (100 mW)	~20 dBm	~10 dBm	Up to 200 mW (23 dBm)	Up to 200 mW (23 dBm)
Receiver Sensitivity	Very High (-130 to -148 dBm)	Moderate (-65 to -90 dBm)	Moderate to High (-100 to -102 dBm)	Moderate (-82 to -92 dBm)	High (-94 to -109 dBm)	High (-94 to -109 dBm)
Latency	High (>1s possible)	Low (~1-10 ms)	Moderate (~15-30 ms)	Low (~6 ms for BLE)	10-30 ms	<1 ms (target)
Power Consumption	Very Low	High	Low	Low	Moderate to High	Moderate to High

Table 1: Wireless Network Features

Application areas of IoT for environmental monitoring

IoT environmental monitoring is a well-studied field with contributions from research on various use cases. A combination of IoT and LoRaWAN architecture has been deployed in urban environmental monitoring, ‘exploiting public transport (..) to pervasively collect data’ of polluting substances (Addabo et al., 2019) and for assessing air quality by measuring concentrations of particulate matter PM10, PM2.5 and other parameters

such as NOx (Johnson et al., 2019; Wang et al., 2018). It is used at scale in smart and sustainable farming with ‘the ultimate goal (..) to collect, monitor, and effectively employ relevant data for agricultural processes, with the purpose of achieving an optimized and more environmentally sustainable agriculture’ (Codeluppi et al., 2020; see also Ahmed et al., 2022). Combining real-time monitoring with actuators that act on received signals enables immediate reaction to potential environmental hazards. IoT sensors on LoRaWAN have therefore been used in settings that require immediate responses such as in forest fire detection (Sharma et al., 2023) and forest fire prevention in Indonesia (Kadir et al., 2018) and for designing real-time Flood Early Warning Systems (Yoeseph et al., 2022; Devaraj Sheshu et al., 2018). IoT-enabled tracking of wildlife in conservation projects covers use cases of monitoring animal movement (Abd-Elrady et al., 2022), supporting ‘virtual fencing’ (Sree et al., 2023), monitoring terrestrial wildlife migration corridors (Kučas et al., 2023), mitigating human-wildlife conflicts (Thangavel et al., 2021, Nandutu et al., 2022) or combining all these data points into an ‘Internet of Animals’ (Kays and Wikelski, 2023).

Challenges in IoT deployment for environmental monitoring

Musaddiq et al. (2022) report that installing IoT sensors and LoRaWAN gateways, maintaining the network and covering the operational costs still remains operationally, technically and financially demanding in many use cases. Organizations, especially smaller ones or in low-resource regions, may lack access to the necessary expertise or find it challenging to retain skilled personnel and technical capacities for monitoring tasks. Furthermore, monitoring environmental efforts can be expensive. It requires purchasing specific equipment, compensating trained personnel, and it demands for the technical resources to integrate continuous data collection, and analysis over extended periods. The initial setup cost and ongoing operational expenses can be prohibitive, especially for long-term projects. This conflicts with the fact that monitoring efforts may be insufficiently covered within budgets for environmental interventions as they might not be perceived as necessary or are not enforced by policies. Stakeholders may focus on the implementation of environmental actions without recognizing that monitoring is crucial for assessing the effectiveness of these actions, for identifying areas for their improvement, and ensuring accountability. Ecosystems are dynamic, and requirements for environmental interventions may change over time which can only be accounted for when deploying continuous monitoring. Yet, where environmental projects are funded by grants, donations, or government budgets, these might prioritize implementation of environmental actions or immediately tangible results, such as tree planting, over long-term continuous monitoring to track SMART (specific, measurable, achievable, relevant, time-bound) targets and results.

Challenges in designing environmental data pipelines

In addition to these challenges of acquiring and deploying IoT solutions, there exist requirements for environmental monitoring solutions that originate from cases in which environmental data pipelines are multi-actor efforts. Often, the actors carrying out environmental measurements are not the ones who make use of these data. Furthermore, actors responsible for environmental interventions and the data collection to assess their impact are also not the ones financing these interventions. Lastly, environmental data needs to be findable, accessible, interoperable and reusable across platforms complying with FAIR data principles (Wilkinson et al., 2016).

White et al. (2022) state with a specific focus on conservation budgets that 'biodiversity conservation is chronically underfunded'. The authors call for improving cost reporting (White et al., 2022) to provide a more detailed and comprehensive view of financial aspects. Underfunding environmental restoration and protection and the implied monitoring efforts contrasts with the stated demand for more data in better quality, complying with FAIR data standards, and taking into consideration the rights of the data originators. Comparing eight global and regional agricultural monitoring systems, Fritz et al. (2019) contend that there exist gaps in methods as well as in data. Accordingly, the authors recommend 'addressing these gaps through ongoing improvements in remote sensing, harnessing new and innovative data streams and the continued sharing of more and more data' (Fritz et al., 2019).

Distributed and collaborative approaches to environmental monitoring already exist. Multi-actor initiatives and associations have been formed for the purpose of making a collective effort to enhance environmental monitoring on various levels, in the form of high-level or sector-specific institutions to citizen science. The eDNA Collaborative[3] or the TNFD Data Initiatives[4] are collaborative efforts to advance nature-related data acquisition[5] for institutions and the private sector. On the level of citizen science, the concept of 'crowdsensing' (Diviacco et al., 2023) has been introduced to describe distributed monitoring efforts. Diviacco et al. (2023) suggest a design and implementation of collective IoT-monitoring of air quality in an urban environment through measuring particulate matter that 'allows for drastically reduced costs and considerably improves the coverage of measurements'. Besides economic distribution of costs and benefits, the authors highlight social and educational benefits of collective environmental action: 'Crowdsensing and open access to air quality data can provide very useful data to the scientific community but also have great potential in fostering environmental awareness and the adoption of correct practices by the general public'. Such distributed monitoring efforts, however, require mechanisms to clean data and build traceable data streams where data origin is independently verified in order to fulfill data integrity requirements. Furthermore, distributed monitoring efforts may face challenges of standardization to make data accessible, interoperable and reusable.

[3] https://www.ednacollab.org/
[4] https://tnfd.global/engage/data-initiatives/
[5] https://tnfd.global/engage/data-initiatives/

They require a robust integration of these various data sources as well as their verification and traceability to provide data integrity. These challenges can persist even when complementing data from centralized data streams with those from distributed monitoring efforts.

The objective of considering the needs of data originators is supported by a study with a focus on forest data collection, conducted by De Lima et al. (2022), which stresses and reports that data collection of forest data benefits data users more than data collectors. According to the authors, costs and benefits of data collection are unfairly distributed. They argue that 'ground forest measurements are hard to sustain and the people who make them are extremely disadvantaged compared to those who use them'. Therefore, the authors propose that a new approach to forest data has to focus on the needs of data originators such as Indigenous People and Local Communities whose contributions have to be considered and compensated, which calls for a more and fairly distributed form of monitoring efforts and benefits.

Specifying requirements for the design and governance of environmental data pipelines

Specificities of requirements for the design and governance of environmental data pipelines are certainly dependent on the type of actors and stakeholders involved, the types of data collected, the regulatory, technical and social features of the data value chain, and the purposes for which the data is acquired and used. More research could be conducted to define a typology of challenges and their likelihood to occur under certain conditions, context and use case. However, there are requirements that already emerge from the challenges discussed above. Besides closing funding gaps for monitoring efforts and providing the required scientific and technical expertise, responding to an increasing demand for better data and closing data gaps, there are social and equity considerations to be addressed. Consideration of needs of data originators, fairness of distribution of costs and benefits of data collection and participatory governance in designing environmental data pipelines call for improved solutions that respond to these concerns. In addition, environmental data pipelines need to be able to comply with data integrity requirements, providing traceable data trails and independent verification mechanisms, while ensuring secure data transmission and compliance with data privacy regulations. Best practices and appropriate governance policies could be specified further following already defined principles such as the FAIR data principles and CARE data principles for use of Indigenous Peoples' and Local Communities' rights to control their data (Carroll et al., 2021; GIDA, 2019[6]). In order to facilitate standardization and compliance with FAIR data principles in environmental data, the concept of Essential Variables for Earth System Science has been developed (Sansone et al., 2019; Pereira et al., 2013; Navarro et al., 2017; Poisot et al., 2019;

[6] https://www.gida-global.org/care

Michener et al., 2015; Crystal-Ornelas et al., 2022). This concept encompasses a wide range of variables for collecting environmental and Earth system data, which include essential variables for climate (ECV), biodiversity (EBV), ecosystem services (EESV) and other environmental factors. Further, in ecology, the Darwin Core Standard (DwC) is a body of standards intended to facilitate the sharing of information about biological diversity (Wieczorek et al., 2012).

Integration of IoT and blockchain - DePIN

The integration of IoT with blockchain has been addressed in the academic literature (Reyna et al., 2018; Minoli et al., 2018; Wang et al., 2020), citing the advantages of such an integration related to enhancing data integrity, reliability, security, and collaboration. Blockchain-based IoT-networks are part of an emerging field seeking to address design and governance challenges in data pipelines that occur related to centralization - of control, operation, governance, or benefits. Decentralized Physical Infrastructure Networks (DePIN) introduce a new approach to constructing and managing distributed physical infrastructure on blockchain and incentivizing its adoption and rewarding its maintenance through cryptocurrencies.[7] DePIN refers to systems of interconnected physical devices that operate without a central point of control or authority but are instead maintained by its nodes. Different DePIN business models exist covering services ranging from distributed energy grids, waste management, water supply to telecommunication networks (cf. DePIN Landscape by Andrew Law 2023[8]).

Blockchain

Blockchains are digital ledgers that are stored and maintained in a distributed way across a network of nodes. A blockchain integrates peer-to-peer networks with cryptographic techniques, including public key messaging and hash functions, to form a secure, immutable, and publicly verifiable ledger (Swan, 2015; Pilkington, 2016). A block on a blockchain can contain various types of data. Consensus is established among validator nodes in order to add a new block, making it impossible for a single entity to control or tamper with the information. A consensus protocol consists of a set of rules written in computer code that allow network participants (nodes) to agree on the accurate status of a ledger—which can contain transactions, contracts, ownership, identities, and other data (see for instance Rajagopalan, 2018). Consensus algorithms are designed to facilitate agreement among distributed systems or nodes on updates of the ledger even under challenging conditions like malicious intent, network delays, faults, or asynchronicity (Fischer et al., 1985). Transactions on a blockchain are visible to all participants and can be verified by any party, enhancing transparency among users. A blockchain can be public, where everyone can join and participate in the

[7] https://messari.io/report/state-of-depin-2023
[8] https://iotex.io/blog/depin-landscape-map/

network, view its ledger, and participate in the consensus process, given the reputation and, in the case of Proof-of-Stake protocols, a required locked-up stake. A blockchain can also be private, where the participation in a network is restricted to one organization or a few invited organizations or institutions such as in a blockchain consortium. Despite its decentralized nature, the distributed data storage and consensus mechanism, blockchain ecosystems can exhibit varying degrees of centralization, depending on their specific implementation. Blockchains were first implemented (under the alias Satoshi Nakamoto, 2008) as the technology underpinning bitcoin, a cryptocurrency. However, as Davidson et al. (2018) argue, cryptocurrencies were only the first instantiation of what is otherwise a decentralized data infrastructure that can host any possible data. Not only data is stored in a distributed way, but also smart contracts can be executed on blockchain, a set of rules or programs that execute autonomously, when certain predefined conditions are met (Szabo, 1994). According to Davidson et al. (2018) blockchain ecosystems and their governance are best described as a (techno-)institutional innovation for economic coordination and governance that 'competes with other economic institutions of capitalism, namely firms, markets, networks, and even governments'.

Blockchain for climate and nature

Blockchain technology has found adoption for various use cases in the environmental field. It is moreover promoted as a technology to be used to build decentralized applications to fight climate change by the European Commission[9]. Esmaeilian et al. (2020) list capabilities of Blockchain applications to increase sustainability with regard to four main areas: '(1) design of incentive mechanisms and tokenization to promote consumer green behavior; (2) enhance visibility across the entire product lifecycle; (3) increase systems efficiency while decreasing development and operational costs; and (4) foster sustainability monitoring and reporting performance across supply chain networks.' Beside its use in supply chain tracking (Munir et al., 2022), the technology has been implemented to facilitate payment for ecosystem service projects by enabling direct automated payments between parties through smart contracts, by decreasing transaction costs, enabling transparency and an auditable data pipeline for environmental monitoring, as well as its secure and independent verification (cf. Oberhauser, 2019; Granados and Schlüter, 2023). Apart from underpinning exchanges for tokenized ecological assets or blockchain-based marketplaces, a further development is the use of blockchain technology as a decentralized database or data-exchange for ecological data in research specifically (Marstein et al., 2024). Such a data exchange suggests to provide data originators with more control over their data and reward them for their data provision (Lewis et al., 2023) through the use of smart-contract automated payments. In the field of biodiversity and climate finance,

[9]https://digital-strategy.ec.europa.eu/en/policies/blockchain-climate-action

nature- or climate-backed tokens (see, for instance, Wunder et al 2024, preprint) and various environmental assets are implemented on blockchain.

Integration of IoT networks with Blockchain to address challenges in design and governance of environmental data pipelines

The integration of IoT networks and blockchain is yet another area for a use of blockchain that could support nature and climate mitigation actions. This combination can respond to technical requirements of providing robust, traceable and independently verified data pipelines for environmental monitoring, while it could also help addressing social and economic issues. The following features of a blockchain and IoT combination can contribute to technical requirements such as reliability and security of IoT operation, while also address social and economic challenges to enhance monitoring, reporting, and verification processes and leverage fairer distribution of benefits, respect data ownership, and increase community participation.

Transparency: Every data exchange or transaction between IoT devices can be recorded on a blockchain, creating an immutable history of interactions. Consensus mechanism ensures that data recorded on the blockchain has been verified by multiple parties, ensures its accuracy and reliability.

Identity: By adopting a unified blockchain system, it is possible to identify each Hotspot and IoT device uniquely. Blockchain enables reliable distributed device authentication and decentralized authorization of network access for IoT applications.

Security: Blockchain can handle exchanges of messages between IoT devices as transactions, which are secured through validation and traceable on chain. Moreover, the integration of blockchain can refine the effectiveness of existing secure standard protocols utilized in the IoT. Encryption mechanisms such as zero-knowledge proof or homomorphic encryption can further secure data transmission and data access.

Autonomy: Combining IoT with blockchain supports autonomous systems which are, once they are set up, not in need of further human intervention. Smart contracts on blockchain can further automate transactions and device actions without the need for centralized authority or manual intervention. This allows for automated processes that can respond to specific conditions without human oversight, reducing the potential for error and increasing efficiency. Data from IoT devices can, for instance, trigger payments through smart contract operation in PES schemes.

Robustness: A distributed system architecture eliminates single points of failure and bottlenecks, which increases the robustness of system operation. Decentralization of transactions on blockchain through a consensus mechanism further enhances fault tolerance. Distributed storage of data and transactions on an immutable ledger such that each node has a copy of the entire ledger makes it resistant to malicious attacks or data loss.

Scalability: Distributed network operation and data storage reduces IoT data silos. A decentralized IoT network can grow to include even more participants that are at the same time its operators.

Decentralization of control over data and network operation: Transitioning from a centralized to a peer-to-peer distributed architecture contrasts with a scenario in which a few organizations have control over the data transmission, processing and storage for a vast number of users. Instead, in a decentralized architecture, data providers and network operators are placed at the center of decentralized systems, responsible for their operation and maintenance.

Lower costs and cost distribution: The decentralized nature of blockchain implies that the infrastructure costs, such as for maintaining the network and validating transactions, are shared among participants. By leveraging blockchain, IoT networks can achieve higher levels of security and data privacy, which are critical for legal compliance. This indirectly benefits all stakeholders by reducing potential costs associated with data breaches and privacy violations. As blockchain operates on a decentralized network, which eliminates or reduces the need for central intermediaries, like cloud service providers, this eliminates transaction costs between nodes who provide IoT network coverage and its users. Here, blockchain can further streamline transactions through smart contracts, which automatically execute agreements upon meeting predefined conditions.

Funding and distribution of benefits: By distributing rewards for network operation between nodes participating in its maintenance, further revenue streams for these participants are created. Moreover, blockchain can accelerate the creation of an IoT ecosystem of services and data marketplaces (Reyna et al., 2018), where data can be tokenized and traded. While the assetization of data and applications has long been leveraged yet centralized by a few organizations, blockchain-based data exchanges seek to decentralize the data economy (Davidson et al., 2016; Davidson et al., 2018).

Community Participation: Distributing data and consensus among nodes makes blockchain a ‘participatory’ technology in technical terms in the first place. This technical distribution among nodes leads to their involvement not only in the systems operation, but also in its governance. Public blockchains and their ecosystem, the applications around use cases built with them, are in a process of continuous development. In contrast to traditional technology that is designed, developed and governed in a centralized way, around centralized data storage and centralized network operation, decentralizing steps of designing, planning, implementation and governance of a technology and its operation implies participation of the blockchain community in the technical development and rule-making of a blockchain ecosystem. Community participants vote on proposals to develop the blockchain system and its governance further.

This does, however, not necessarily imply that this technical participation is fairly distributed. But other than centralized systems, blockchain ecosystems entail the possibility of it. In order to fully realize this potential, technological governance and distributed operation is in need to be complemented by social and community participation, and regulation, which integrates blockchain ecosystems within a broader institutional landscape and is able to leverage other forms of participation (Hart et al., 2024)[10].

How requirements of the design and governance in IoT data streams can be addressed eventually by a specific integration of blockchain with monitoring infrastructures such as IoT depends on the specific technological architecture, business or operational model, including choice of blockchain, governance model, token model, and community participation policies. While the integration of IoT networks with blockchain has already established itself as a research field (Reyna et al., 2018, Minoli et al., 2018, Wang et al., 2020), reports on specific use cases with specific networks remain scarce (Reyneke et al., 2023, Musaddiq et al., 2022). In the following section, a pilot use case of IoT operation on the blockchain-based IoT-subnetwork of Helium Network is presented that was installed and tested in the context of a community-based urban green space restoration project in Nairobi, Kenya.

Pilot use case of the blockchain-based IoT Helium Network in a community-based urban green space restoration project in Kamukunji Park in Nairobi, Kenya

The Kamukunji Environmental Conservation Champions (KECC) are a volunteering-based community initiative of urban green space stewards that emerged from a local community of 25 different groups from the neighborhood around Kamukunji Park in Nairobi, Kenya. The Kamukunji Park is owned by the city but maintained by the community initiative. The KECC have been actively engaging in park maintenance and restoration actions such as cleaning of the dump sites of the park, of removing waste from the Nairobi river and the urban green site, installing a children's playground, starting to plant trees, introducing sites for urban farming and establishing proper waste management in the area with partners to enhance the use of the park for festive occasions and educational and recreational purposes. In the context of these community-based restoration activities, IoT sensors were installed in Kamukunji Park, Nairobi, Kenya, for the purpose of enabling environmental monitoring of regulating urban ecosystem services. The purpose of environmental monitoring was to provide the community initiative with data to enable further restoration planning, monitor progress and include data in grants applications. IoT devices were registered on the blockchain-based IoT subnetwork of Helium Network and LoRaWAN Hotspots were installed in the city to provide network coverage for data transmission of sensor packets.

[10] https://otherinter.net/research/three-body-problem/

Project Partners: In December 2022, the community initiative KECC formed a partnership with de_plan, a spatial planning initiative from Philadelphia/US and Nairobi, Kenya, and BLCK IOT, a project based in Nairobi, Kenya, and Berlin, Germany, that is deploying IoT-solutions to enable monitoring with integration on blockchain, and with support in research from Leipzig University.

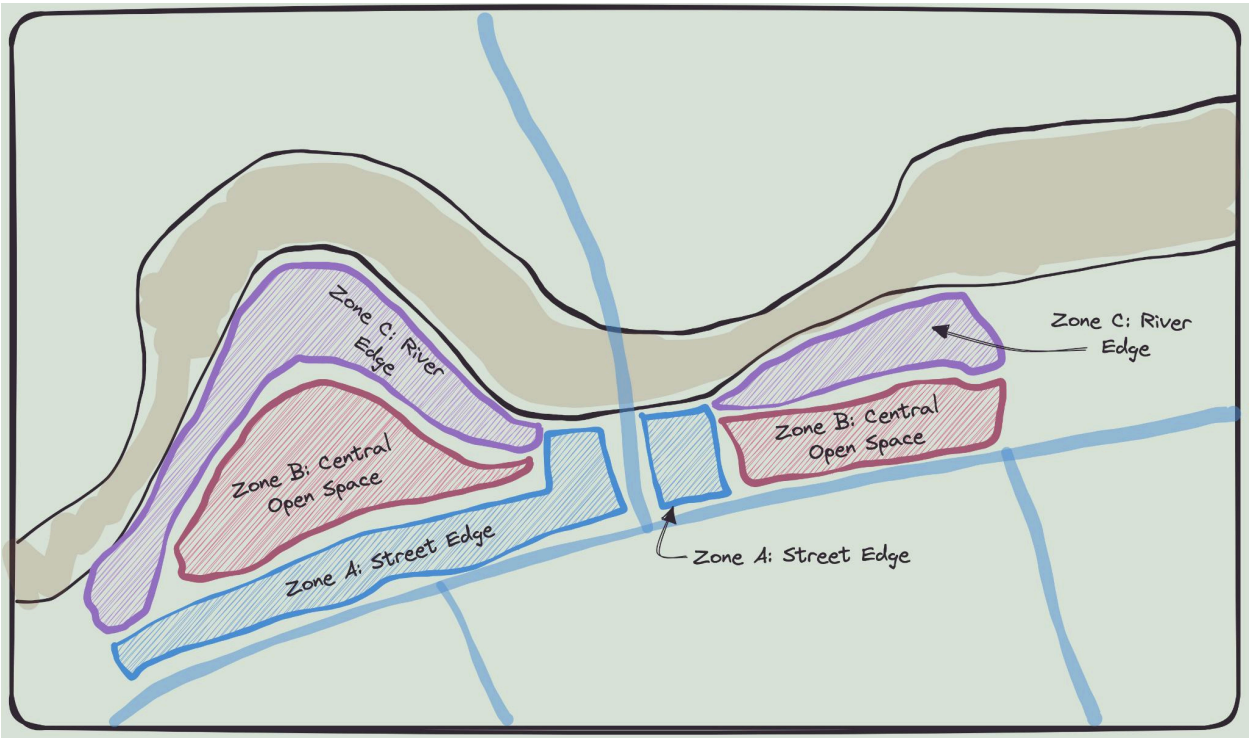

Figure 1: Layout of Kamukunji Park, Nairobi, Kenya.

Monitoring Purpose: The aim of this partnership was to provide the community initiative KECC with environmental monitoring data of regulating urban ecosystem services to include in future grant or funding applications. The KECC are part of the Public Space Network[11], an umbrella organization of community-based initiatives around open spaces in Nairobi. Further objectives were to enable baselining and continuous environmental monitoring of the impact of the initiative's restoration actions in Kamukunji Park to be used for planning and to enable urban green space valuation according to the TEEB urban metric[12] (2011). Installing environmental monitoring devices in Kamukunji Park was intended to contribute to citizen science, with the collected data to benefit not only the community of urban green space stewards but potentially a wider range of stakeholders, including researchers, environmental protection agencies, meteorological organizations, and educational institutions.

[11] https://www.publicspacenetwork.org/
[12] https://teebweb.org/publications/other/teeb-cities/

Accordingly, nature education activities took place repetitively. During one weekend, these included a group of children identifying tree species and their abundance.

Data assessment: Regulating urban ecosystem services were monitored through IoT sensors that were installed in the Park. This data was complemented by satellite data and GIS analysis conducted by project partner de_plan, as well as data about tree diversity, both in tree species richness and abundance, which was assessed on the ground through community field work. Further, use and use values of the park for the community were assessed through a survey. Tools that were tested for further assessments included UrbanInVest, and iTree Eco, and the development of a habitat grid for the park was considered. Urban InVest is a data and modeling platform which is part of the Stanford Natural Capital project[13]. It features spatially explicit biophysical and socio-economic models that enable users to quantify and map the impacts of alternative urban designs on multiple urban ecosystem services. ITree Eco is a software application developed as part of the i-Tree suite of tools, which are designed to allow users to analyze the ecosystem services that trees provide[14].

IoT sensor deployment and measurements: Project partner BLCK IOT deployed an array of sensors in Kamukunji Park, including one particulate matter sensor to measure particulate matter concentration levels of PM10, PM1 and PM2.5, one weather station, five soil sensors to assess humidity, temperature, and electrical conductivity of soil, one leaf moisture sensor, and two water level sensors in the Nairobi River, totaling ten sensors (Figure 1). These sensors were procured through the project, with KECC being responsible for their hosting and maintenance. Data points per sensor assessed are presented in Table (2). With a primary focus on data collection and basic visualization through Datacake, during the testing period, the project established a routine where sensors transmitted data every four hours.

Sensor	Parameter: Unit	Parameter: Unit	Parameter: Unit	Parameter: Unit	Parameter: Unit	Parameter: Unit	Parameter: Unit	Parameter: Unit
Particulate Matter	PM1: µg/m3	PM2.5: µg/m3	PM10: µg/m3					
Weather Station	Temperature: °C	Humidity: %RH	Pressure: Pa	Rainfall: mm/h	Light Intensity: Lux	UV Index: 0-12	Wind Direction: degrees	Wind Speed: m/s

[13] https://naturalcapitalproject.stanford.edu/invest/urban-invest
[14] https://www.itreetools.org/tools/i-tree-eco

Leaf Moisture	Moisture: 0-1	Temperature: °C						
River Level	Distance: mm							
Soil sensors	Temperature:°C	Moisture: %VWC	Electrical conductivity: dS/m					

Table 2 : Measured units by sensor

Figure 2 Dragino LDDS75 a LoRaWAN Distance Detection Sensor in Kamukunji Park

LoRaWAN Helium Network Hotspot Deployment: At the time of the pilot project, the community initiative had no funding available. Traceable data streams for future monitoring were seen as favorable to ensure transparency for various stakeholders. Given these requirements, a blockchain-based IoT solution was regarded as suitable.

Hotspots and IoT sensors were deployed on the Helium Network, which is recognized globally as the largest blockchain-based IoT network with the highest number of nodes.

Helium Network

Helium Network is a decentralized blockchain-based network designed to facilitate wireless communication for the Internet of Things, and recently also mobile devices. Its IoT subnetwork combines a Proof of Coverage (PoC) mechanism to independently verify network coverage of Hotspots as well as data transmission with rewards in the form of cryptocurrency (IOT) tokens to incentivize participants to build and maintain the network's infrastructure. Participants host network gateways, which provide LoRaWAN network coverage, and perform data transmission for IoT devices. Helium Network has emerged to support adopting, scaling and decentralizing IoT monitoring infrastructure and operation (Haleem et al., 2018). It operates a decentralized LoRaWAN network globally and recently also launched 5G networks for mobile devices in the US and Mexico. The Helium IoT subnetwork currently consists of 1.024.647 Hotspots in 195 countries.[15] It has a wide-area wireless networking system, blockchain, and a token economy as its core components. On April 18th in 2023, after a community vote was passed on proposal “HIP70 - Scaling Helium Network”[16] by network participants, Helium Network, which first was its own layer 1 blockchain, migrated to a layer 1 DAO on the blockchain Solana[17]. Hotspots are now ‘a rewardable entity’ on the Helium Network and are represented on Solana as a compressed NFT (Non-Fungible Token)[18]. NFTs are uniquely identified by their identifying ECC Compact Public Keys.

[15] https://explorer.helium.com/
[16] https://github.com/helium/HIP/blob/main/0070-scaling-helium.md
[17] https://docs.helium.com/solana/migration/
[18] https://docs.helium.com/solana/rewardable-entites

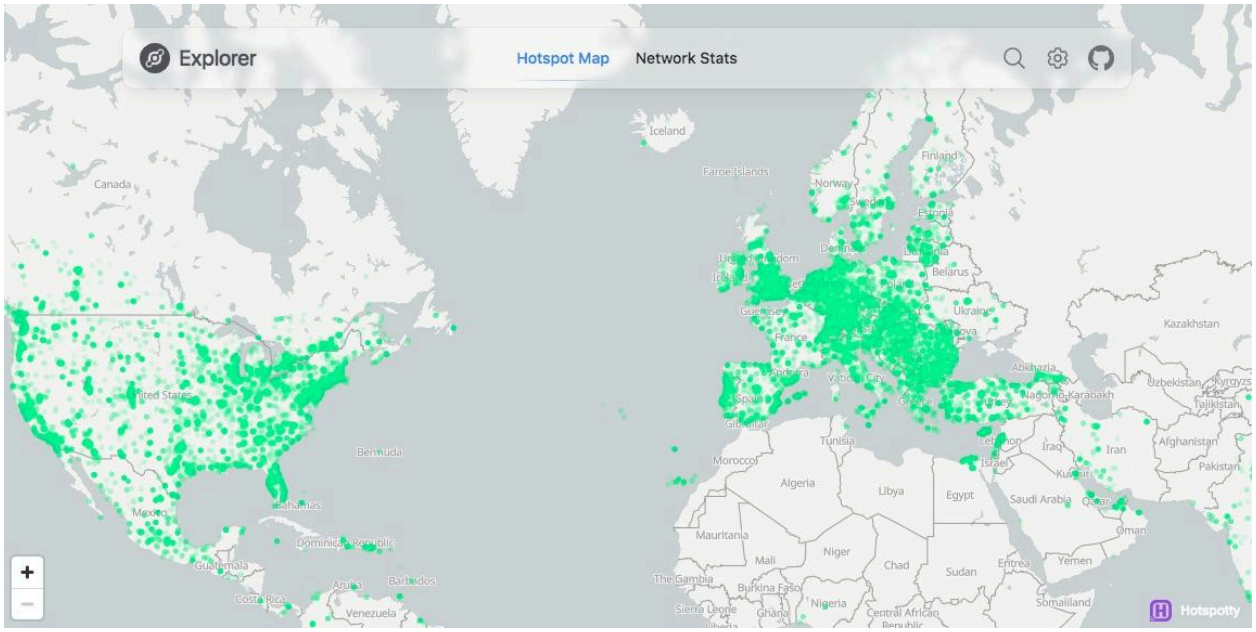

Figure 3: Helium Explorer - Overview of 1.024.647 Hotspots in 195 countries

LoRaWAN on Helium: IoT subnet

Through its IoT subnetwork, Helium Network participants provide LoRaWAN coverage on the Solana blockchain. LoRaWANs key features—long-range coverage, security features such as AES encryption, the open protocol, and low power usage—align with Helium's mission to provide widespread and efficient IoT connectivity. Helium Network establishes a system for bi-directional data transfer between wireless devices and the internet without the need for a centralized coordinator and seeks to further enhance security and reliability of the network. Helium grows through a decentralized model where anyone can participate by setting up a Helium Hotspot. Hotspots are combination devices: they act as wireless gateways providing LoRaWAN network coverage for IoT devices, allowing them to transmit data over long distances, on the one hand, and as nodes of the Helium Network on the other. In return for providing network coverage and for witnessing other Hotspot's location and activity, Hotspot owners earn rewards in the token IOT, which can be converted into Helium tokens (HNT), the native cryptocurrency of the Helium network. Data transmission from IoT devices into the network is paid for in Data Credits (DC), another token which can be derived from burning HNT tokens.

Onboarding a Hotspot to Helium Network

The process for onboarding a new hotspot into the network involves a Hotspot operator purchasing hardware from an authorized Maker and then completing the self-onboarding procedure to connect to the network. At onboarding time, Hotspots sign an onboarding transaction proving physical ownership of their device. A Hotspot can be designated as an IoT Hotspot, a Mobile Hotspot, or serve as both. To qualify for rewards

in both the Mobile and IoT categories, a Hotspot needs to onboard with both the IoT and Mobile networks, including confirming its location for each subnet. After receiving their hardware device, Hotspot operators need to physically set it up in their chosen location. The primary tool for setting up and managing Hotspots on the Helium Network is the Helium mobile app. This app guides users through the process of initializing their Hotspot, connecting it to the network, and registering it on the Helium blockchain. This involves creating a wallet, if the participant doesn't already have one, and performing transactions that establish the Hotspot's presence on the network. The app also allows users to manage their Hotspot's settings and view its performance metrics.

Verification of Node Location and Proof of Coverage (PoC)

When setting up a Helium Hotspot, a node in the network, the owner asserts its geographic location. This is a condition of the Proof-of-Coverage process, by which the network verifies that Hotspots are where they claim to be and are providing wireless coverage. Asserting location and participating in a Proof-of-Coverage mechanism requires a fee to be paid in Data Credit tokens[19], which shall ensure that participants only update their Hotspots' locations when necessary. The asserted location also impacts the distribution of rewards in IOT tokens that Hotspots might earn from participating in the Proof-of-Coverage process. The PoC mechanism is how the Helium Network verifies the actual wireless coverage provided by Hotspots. Following HIP70[20], Hotspots send out Beacons in regular intervals to prove they are providing network coverage which nearby Hotspots witness: receive and acknowledge. These Hotspots, acting as Beacon witnesses, then report to a Proof-of-Coverage ingest farm that they have heard the challenge packet. The Hotspot’s signal has initially a form of entropy or random signal attached to it, to prevent malicious or replay attacks of the signal that could be used by other operators to gain unpermitted access to the network. A Proof-of-Coverage ingest farm is designed to process this signal and it ‘performs basic validation that filters out structurally invalid data and then submits both the beacon [signal] receipt and the witness receipts’ to a storage unit[21]. At last, a PoC Verifier oracle verifies all the data submitted by correlating witnesses to receipts and confirming the series of events[22]. Hotspots earn IOT tokens for their participating in PoC verification, both for sending out signals regularly and for witnessing them. At their launch, the signal interval for a Hotspot is set to six hours. The mechanisms of asserting the location of a Hotspot and Proof-of-Coverage have blockchain transactions attached to them, such that they are recorded on chain and publicly verifiable through the Helium Explorer and its integrated tools such as Hotspotty and Moken. These tools allow other participants

[19] https://github.com/helium/HIP/blob/main/0090-reduce-iot-location-assert-cost-indefinitely.md
[20] https://github.com/helium/HIP/blob/main/0070-scaling-helium.md
[21] https://docs.helium.com/oracles/iot-proof-of-coverage-oracles
[22] https://docs.helium.com/oracles/iot-proof-of-coverage-oracles

and users to explore the geographic distribution of network coverage, which adds transparency to the network.

Setting up IoT Devices and Data Transmission

The Helium Console is another tool that is used to set up IoT devices such as sensors to communicate on the Helium Network. IoT devices are registered through the Helium Console through identifiers (DevEUI, AppEUI, AppKey). The Console is also used to monitor devices activities and data usage through their logs. When an IoT-device such as a sensor transmits data to a Hotspot, the user pays in Data Credits. Data Credits can be allocated to devices in order to be able to send data into the network. Hotspots send these packets into the network. A Hotspot's data transmission is eventually verified by an oracle, triggering rewards in IOT tokens to that Hotspot for transmitting packets through a smart contract. The action of data transmission has a blockchain transaction attached to it as well and is recorded on chain. These transactions can be traced at any time for a specific Hotspot in its activity log through the Helium Explorer and its tool Moken.

Opportunities and challenges

In the context of the pilot project, about 100 Helium Network gateways were deployed in both residential and commercial buildings across the city to offer comprehensive area coverage and to establish reliability through high redundancy of packet delivery. Ten IoT sensor devices were installed on site of Kamukunji Park transmitting data into the network.

Network coverage and operation: The project reported very good network coverage, attributing this success to proper sensor installation. No significant packet loss was noted and packets from different sensors were transmitted successfully during testing. However, another study using the Helium Network in a remote area in Sweden for environmental monitoring in wetlands by Musaddiq et al. (2022) reported packets that would not reach the cloud with a packet drop of 0.1-2%.

The project partners endorsed the use of Helium and LoRaWAN for similar applications, highlighting the range of transmission and low power requirements. Sensor setup was said to be easy, less expensive and more secure compared to more expensive or centralized protocols. However, the project also acknowledged challenges, particularly in establishing network coverage in Kenya. The slow adoption rate in Kenya, in contrast to the rapid adoption seen in regions like the EU and USA, necessitated a more hands-on approach to network setup but also presented an opportunity for piloting work in leveraging these technologies for environmental sustainability.

Accessibility and installation: The onboarding process was found very accessible and easy to use by project participants. They further reported a simple integration of

sensor data with Datacake, a data platform that facilitates visualization and data analysis.

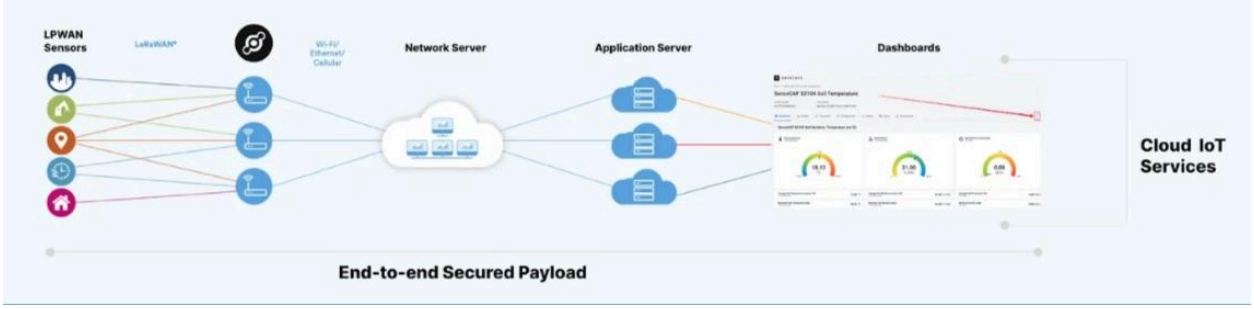

Figure 4: Data stream from sensor to visualization platform

Transparency: Helium Network offers ways to establish transparency for different parties to monitor network interactions. All network interactions and data transmissions are tracked on blockchain as they are coupled with a transaction. A transparent data trail can be established in combining Helium Network's available tools. The Helium Explorer[23] is an online tool to provide overview of the network's activity and its components. Anyone can explore the global distribution of Helium hotspots and see where hotspots are located and the network's coverage area. This is useful for planning where to deploy new hotspots for coverage and participation in Proof-of-Coverage mechanism. Through integration of the Helium Explorer with other tools such as Hotspotty[24] or Moken[25], the information about a specific Hotspot can be investigated in more detail: its location, status (online/offline), its recent activity, and the amount of tokens it has earned. A Hotspot's activity log includes its sending of beacons, its witnessing of other Hotspots, its receiving IOT rewards for witnessing other Hotspots and its data transmission activities. This helps to monitor hotspots' performance. It enables transparency for users to explore a hotspot's activity and to verify transactions on the network, without revealing any of the transmitted data. Network statistics display statistics such as the total number of hotspots, growth over time, and token distribution. In addition, the Helium mapper exists where data on the network's real-world coverage and performance is gathered from the Helium community to visualize how the network provides coverage and how effective it is.
By combining IoT activity logs from Helium Console or from a Visualization Platform with data about transactions from Helium Explorer in integration with other tools such as Moken, it is possible to provide a transparent data trail to track Hotspot activity and data transmission from a specific IoT device. Organizations that use the Helium network for

[23] https://explorer.helium.com/
[24] https://app.hotspotty.net/hotspots/statistics
[25] https://explorer.moken.io/

their IoT applications can use these information for reports showing all transactions related to their devices.

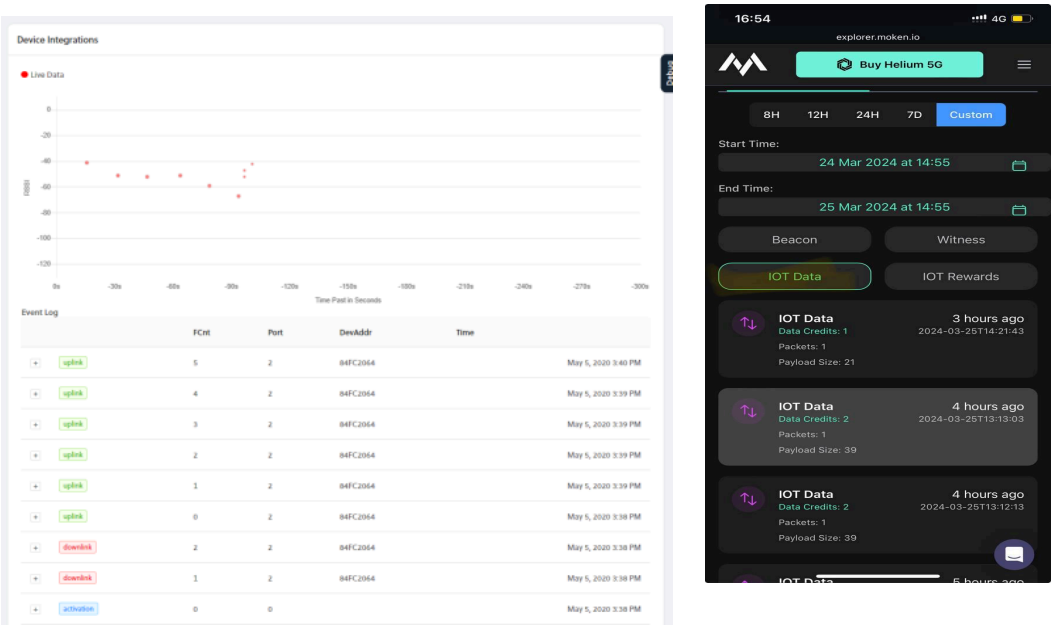

Figure 4: Moken Hotspot activity log and IoT Device activity on Helium Console

Participation in Network development and Governance: Project partners participated in governance of Helium Network through voting on proposals. Helium Network receives Helium Improvement Proposals (HIPs) which are a mechanism for proposing changes or improvements to the Helium network. HIPs allow community members, developers, and stakeholders to formally suggest enhancements, developing features, or policy changes to the existing ecosystem. HIPs are developed and discussed and voted upon by its community to develop the network further. Other blockchain ecosystems have similar processes, for instance Bitcoin's BIPs (Bitcoin Improvement Proposals) or Ethereum's EIPs (Ethereum Improvement Proposals), where proposals undergo community discussion, review, and then a decision - voting - process. All Helium Improvement Proposals can be found on the platform GitHub[26].

Community Participation: The project partners also collaborated with other local members of the Helium network community in Nairobi and other parts of Kenya to fill coverage gaps and create a more robust network through coordinating deployments in underserved areas.

Pay-to-communicate: Network transactions are paid for in Data Credits based on the network use with a pay-to-communicate model. The number of Data Credits that a single sensor consumes per day on the Helium Network depends on several factors. Besides the data packet size, which is the amount of data a sensor transmits in a single

[26] https://github.com/helium/HIP/

message, another factor is the frequency of transmission, how often the sensor sends data. More frequent transmissions as well as larger packet size lead to higher consumption of Data Credits. While the cost to send data on the Helium Network is standardized (1 DC = $0.00001 USD), the actual number of Data Credits consumed per message can vary based on the payload size. During the piloting phase, one sensor transmitted a data packet costing approximately 5 DC every four hours, which equated to 30 DC consumed per sensor per day.

Benefits and rewards: Rewards from Hotspot operations are higher in areas with a high density of IoT devices but with low network coverage, such that a Hotspot can capture more data transfer opportunities. Having a network of Hotspots in high-traffic areas can also indirectly benefit PoC rewards. A well-situated Hotspot in a busy area can better participate in PoC challenges if it is within range of other active Hotspots, which is a common scenario in areas with higher IoT device density. Adoption of use of Helium Network in Nairobi, Kenya, is however rather low, such that there are not many network interactions. Benefits of operating network gateways and IoT sensors on Helium Network in these scenarios can be assessed counterfactually against a baseline of network operations contracting a traditional centralized network provider, where no rewards are earned.

Integration with data marketplaces: The Helium Network records data transmissions on the blockchain without recording the data itself, in compliance with data privacy regulations. Data packets are transmitted in AES-encrypted format. Further revenue can however be generated by connecting IoT device operations with data marketplaces where an IoT operator can tokenize and trade their data. During the pilot project, none of these options were implemented.

Regulation: Kenya is working on new regulations to police trading in cryptocurrencies and has set up a technical working group preparing the draft regulations to be forwarded to the Cabinet for adoption. In Kenya, cryptocurrency is so far regulated by the following acts: (1) The National Payments Systems Act (NPSA); (2) the Capital Markets Act (CMA); and (3) the Kenya Information and Communication Act (KICA). Kenyans are legally allowed to buy and sell cryptocurrencies. [27] The Central Bank of Kenya is responsible for overseeing payment service providers to ensure that platforms are safe for investors.

Conclusion

LoRaWAN is one of the few IoT networks using standardized AES-128 encryption for end-to-end encryption which enables secure data transmission. Its features of low power, low cost, long range and high security operation make it suitable for IoT deployment at any scale for long term environmental monitoring in urban, rural or hazardous areas. Helium Network uses incentives to promote the wider adoption of

[27] https://www.chainalysis.com/blog/africa-cryptocurrency-adoption/

LoRaWAN and leverages blockchain features to reward and further secure IoT operation through unique identification of devices, Proof-of-Coverage and location assertion. Distributed network operation moreover enhances reliability and robustness. By hosting LoRaWAN on blockchain, data transmission is recorded on blockchain which establishes a traceable history of transactions, offering transparency for multi-actor data pipelines and making the transaction record tamper-proof. Deploying blockchain-based IoT networks for environmental monitoring can contribute to addressing design and governance challenges in environmental data streams, not only by enhancing integrity and transparency of data provision, but also by contributing to closing funding gaps of monitoring efforts and distributing costs and benefits of network operation. In addition, in the case of a public network such as Helium Network, Hotspot operators can become active community participants governing system development and operation. However, more research and testing could be conducted to explore possibilities to integrate blockchain-based IoT solutions into existing environmental monitoring efforts and the current project landscape including its regulations, or to assess opportunities of developing customized solutions.

We would like to thank Adrian Clint, Aarti Utwani and Ronald Steyer for providing useful comments on previous versions of this paper. We would like to thank Akshay Aditya, Elzaphan Murage, Nicholas Wahuho and Josephat Karomi (KECC) for collaboration on the urban green space project.

References

Abd-Elrady, E., Abuelkheir, O., & Al-Amer, K. (2022). IoT Technology for Wildlife Conservation Based on Energy Harvesting. *Proceedings of the International Conference on Industrial Engineering and Operations Management*, 1704–1711. https://doi.org/10.46254/EU05.20220332

Abdullahi, U. S., Nyabam, M., Orisekeh, K., Umar, S., Sani, B., David, E., & Umoru, A. A. (n.d.). ORIGINAL RESEARCH ARTICLE. . . *ISSN*, *15*.

Addison, P. F. E., & Bull, J. W. (2018). Conservation accord: Corporate incentives. *Science*, *360*(6394), 1195–1196. https://doi.org/10.1126/science.aau0788

Addison, P. F. E., Bull, J. W., & Milner-Gulland, E. J. (2019). Using conservation science to advance corporate biodiversity accountability. *Conservation Biology*, *33*(2), 307–318. https://doi.org/10.1111/cobi.13190

Ahmed, M. A., Gallardo, J. L., Zuniga, M. D., Pedraza, M. A., Carvajal, G., Jara, N., & Carvajal, R. (2022). LoRa Based IoT Platform for Remote Monitoring of Large-Scale Agriculture Farms in Chile. *Sensors*, *22*(8), 2824. https://doi.org/10.3390/s22082824

Anastasiou, A., Zinonos, Z., & Georgiades, M. (2023). LoRa-Based Environmental Monitoring System for Commercial Farming. *2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT)*, 734–739. https://doi.org/10.1109/DCOSS-IoT58021.2023.00115

Barbier, E. B., Burgess, J. C., & Dean, T. J. (2018). How to pay for saving biodiversity. *Science*, *360*(6388), 486–488. https://doi.org/10.1126/science.aar3454

Bhattacharya, T. R., & Managi, S. (2013). Contributions of the private sector to global biodiversity protection: Case study of the Fortune 500 companies. *International Journal of Biodiversity Science, Ecosystem Services & Management*, *9*(1), 65–86. https://doi.org/10.1080/21513732.2012.710250

Blenn, N., & Kuipers, F. (2017). *LoRaWAN in the Wild: Measurements from The Things Network* (arXiv:1706.03086). arXiv. http://arxiv.org/abs/1706.03086

Buterin, V. (n.d.). *A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM*.

Careja, A.-C., & Tapus, N. (2023). Digital Identity Using Blockchain Technology. *Procedia Computer Science*, *221*, 1074–1082. https://doi.org/10.1016/j.procs.2023.08.090

Carroll, S. R., Herczog, E., Hudson, M., Russell, K., & Stall, S. (2021). Operationalizing the CARE and FAIR Principles for Indigenous data futures. *Scientific Data*, *8*(1), 108. https://doi.org/10.1038/s41597-021-00892-0

Codeluppi, G., Cilfone, A., Davoli, L., & Ferrari, G. (2020). LoRaFarM: A LoRaWAN-Based Smart Farming Modular IoT Architecture. *Sensors*, *20*(7), 2028. https://doi.org/10.3390/s20072028

Coman, F. L., Malarski, K. M., Petersen, M. N., & Ruepp, S. (2019). Security Issues in Internet of Things: Vulnerability Analysis of LoRaWAN, Sigfox and NB-IoT. *2019 Global IoT Summit (GIoTS)*, 1–6. https://doi.org/10.1109/GIOTS.2019.8766430

Crystal-Ornelas, R., Varadharajan, C., O'Ryan, D., Beilsmith, K., Bond-Lamberty, B., Boye, K., Burrus, M., Cholia, S., Christianson, D. S., Crow, M., Damerow, J., Ely, K. S., Goldman, A. E.,

Heinz, S. L., Hendrix, V. C., Kakalia, Z., Mathes, K., O'Brien, F., Pennington, S. C., … Agarwal, D. A. (2022). Enabling FAIR data in Earth and environmental science with community-centric (meta)data reporting formats. *Scientific Data*, *9*(1), 700. https://doi.org/10.1038/s41597-022-01606-w

Davidson, S., De Filippi, P., & Potts, J. (2016). Economics of Blockchain. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2744751

Davidson, S., De Filippi, P., & Potts, J. (2018). Blockchains and the economic institutions of capitalism. *Journal of Institutional Economics*, *14*(4), 639–658. https://doi.org/10.1017/S1744137417000200

De Lima, R. A. F., Phillips, O. L., Duque, A., Tello, J. S., Davies, S. J., De Oliveira, A. A., Muller, S., Honorio Coronado, E. N., Vilanova, E., Cuni-Sanchez, A., Baker, T. R., Ryan, C. M., Malizia, A., Lewis, S. L., Ter Steege, H., Ferreira, J., Marimon, B. S., Luu, H. T., Imani, G., … Vásquez, R. (2022). Making forest data fair and open. *Nature Ecology & Evolution*, *6*(6), 656–658. https://doi.org/10.1038/s41559-022-01738-7

Devaraj Sheshu, E., Manjunath, N., Karthik, S., & Akash, U. (2018). Implementation of Flood Warning System using IoT. *2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT)*. 2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT), Bangalore, India.

Dhanaraju, M., Chenniappan, P., Ramalingam, K., Pazhanivelan, S., & Kaliaperumal, R. (2022). Smart Farming: Internet of Things (IoT)-Based Sustainable Agriculture. *Agriculture*, *12*(10), 1745. https://doi.org/10.3390/agriculture12101745

Diviacco, P., Iurcev, M., Carbajales, R. J., Viola, A., & Potleca, N. (2023). Design and Implementation of a Crowdsensing-Based Air Quality Monitoring Open and FAIR Data Infrastructure. *Processes*, *11*(7), 1881. https://doi.org/10.3390/pr11071881

Esmaeilian, B., Sarkis, J., Lewis, K., & Behdad, S. (2020). Blockchain for the future of sustainable supply chain management in Industry 4.0. *Resources, Conservation and Recycling*, *163*, 105064. https://doi.org/10.1016/j.resconrec.2020.105064

European Commission. Directorate General for Environment., Trinomics., & IEEP. (2022). *Biodiversity financing and tracking: Final report.* Publications Office. https://data.europa.eu/doi/10.2779/950856

Fritz, S., See, L., Bayas, J. C. L., Waldner, F., Jacques, D., Becker-Reshef, I., Whitcraft, A., Baruth, B., Bonifacio, R., Crutchfield, J., Rembold, F., Rojas, O., Schucknecht, A., Van Der Velde, M., Verdin, J., Wu, B., Yan, N., You, L., Gilliams, S., … McCallum, I. (2019). A comparison of global agricultural monitoring systems and current gaps. *Agricultural Systems*, *168*, 258–272. https://doi.org/10.1016/j.agsy.2018.05.010

Georgiou, O., & Raza, U. (2017). Low Power Wide Area Network Analysis: Can LoRa Scale? *IEEE Wireless Communications Letters*, *6*(2), 162–165. https://doi.org/10.1109/LWC.2016.2647247

Granados, J., & Schlüter, A. (n.d.). *Blockchain and payments for environmental services: Tools and oppertunities for environmental protection*.

Haleem, A., Allen, A., Thompson, A., Nijdam, M., & Garg, R. (n.d.). *A Decentralized Wireless Network*.

Haleem, A., Javaid, M., Singh, R. P., Suman, R., & Rab, S. (2021). Blockchain technology applications in healthcare: An overview. *International Journal of Intelligent Networks*, *2*, 130–139. https://doi.org/10.1016/j.ijin.2021.09.005

Hidayat, M. S., Nugroho, A. P., Sutiarso, L., & Okayasu, T. (2019). Development of environmental monitoring systems based on LoRa with cloud integration for rural area. *IOP Conference Series: Earth and Environmental Science*, *355*(1), 012010. https://doi.org/10.1088/1755-1315/355/1/012010

IT University of Copenhagen, Beck, R., Müller-Bloch, C., IT University of Copenhagen, King, J. L., & University of Michigan. (2018). Governance in the Blockchain Economy: A Framework and Research Agenda. *Journal of the Association for Information Systems*, 1020–1034. https://doi.org/10.17705/1jais.00518

Kadir, E. A., Efendi, A., & Rosa, S. (2018). Application of LoRaWAN sensor and IoT for Environmental Monitoring in Riau Province Indonesia. *Proc. EECSI 2018*.

Kays, R., & Wikelski, M. (2023). The Internet of Animals: What it is, what it could be. *Trends in Ecology & Evolution*, *38*(9), 859–869. https://doi.org/10.1016/j.tree.2023.04.007

Kučas, A., Balčiauskas, L., & Lavalle, C. (2023). Identification of Urban and Wildlife Terrestrial Corridor Intersections for Planning of Wildlife-Vehicle Collision Mitigation Measures. *Land*, *12*(4), 758. https://doi.org/10.3390/land12040758

Kumar, M., Raj, H., Chaurasia, N., & Gill, S. S. (2023). Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0. *Internet of Things and Cyber-Physical Systems*, *3*, 309–322. https://doi.org/10.1016/j.iotcps.2023.05.006

Lewis, R. J., Marstein, K.-E., & Grytnes, J.-A. (2023). Incentivising open ecological data using blockchain technology. *Scientific Data*, *10*(1), 591. https://doi.org/10.1038/s41597-023-02496-2

LoRa Alliance. (2017). *LoRaWAN™ 1.1 Specification 2*.

Marstein, K., Grytnes, J., & Lewis, R. J. (2024). ECKOCHAIN: A FAIR blockchain-based database for long-term ecological data. *Methods in Ecology and Evolution*, 2041-210X.14280. https://doi.org/10.1111/2041-210X.14280

Meijer, D., & Ubacht, J. (2018). The governance of blockchain systems from an institutional perspective, a matter of trust or control? *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, 1–9. https://doi.org/10.1145/3209281.3209321

Michener, W. K. (2015a). Ecological data sharing. *Ecological Informatics*, *29*, 33–44. https://doi.org/10.1016/j.ecoinf.2015.06.010

Michener, W. K. (2015b). Ten Simple Rules for Creating a Good Data Management Plan. *PLOS Computational Biology*, *11*(10), e1004525. https://doi.org/10.1371/journal.pcbi.1004525

Munir, M. A., Habib, M. S., Hussain, A., Shahbaz, M. A., Qamar, A., Masood, T., Sultan, M., Mujtaba, M. A., Imran, S., Hasan, M., Akhtar, M. S., Uzair Ayub, H. M., & Salman, C. A. (2022). Blockchain Adoption for Sustainable Supply Chain Management: Economic, Environmental, and Social Perspectives. *Frontiers in Energy Research*, *10*, 899632. https://doi.org/10.3389/fenrg.2022.899632

Musaddiq, A., Maleki, N., Palma, F., Mozart, D., Olsson, T., Omareen, M., & Ahlgren, F. (2022). Internet of Things for Wetland Conservation using Helium Network: Experience and Analysis. *Proceedings of the 12th International Conference on the Internet of Things*, 143–146. https://doi.org/10.1145/3567445.3569167

Nandutu, I., Atemkeng, M., & Okouma, P. (2022). Intelligent Systems Using Sensors and/or Machine Learning to Mitigate Wildlife–Vehicle Collisions: A Review, Challenges, and New Perspectives. *Sensors*, *22*(7), 2478. https://doi.org/10.3390/s22072478

Navarro, L. M., Fernández, N., Guerra, C., Guralnick, R., Kissling, W. D., Londoño, M. C., Muller-Karger, F., Turak, E., Balvanera, P., Costello, M. J., Delavaud, A., El Serafy, G., Ferrier, S., Geijzendorffer, I., Geller, G. N., Jetz, W., Kim, E.-S., Kim, H., Martin, C. S., … Pereira, H. M. (2017). Monitoring biodiversity change through effective global coordination. *Current Opinion in Environmental Sustainability*, *29*, 158–169. https://doi.org/10.1016/j.cosust.2018.02.005

Oberhauser, D. (2019). Blockchain for Environmental Governance: Can Smart Contracts Reinforce Payments for Ecosystem Services in Namibia? *Frontiers in Blockchain*, *2*, 21. https://doi.org/10.3389/fbloc.2019.00021

Pereira, H. M., Ferrier, S., Walters, M., Geller, G. N., Jongman, R. H. G., Scholes, R. J., Bruford, M. W., Brummitt, N., Butchart, S. H. M., Cardoso, A. C., Coops, N. C., Dulloo, E., Faith, D. P., Freyhof, J., Gregory, R. D., Heip, C., Höft, R., Hurtt, G., Jetz, W., … Wegmann, M. (2013). Essential Biodiversity Variables. *Science*, *339*(6117), 277–278. https://doi.org/10.1126/science.1229931

Pilkington, M. (2016). Blockchain technology: Principles and applications. In F. X. Olleros & M. Zhegu (Eds.), *Research Handbook on Digital Transformations*. Edward Elgar Publishing. https://doi.org/10.4337/9781784717766.00019

Poisot, T., Bruneau, A., Gonzalez, A., Gravel, D., & Peres-Neto, P. (2019). Ecological Data Should Not Be So Hard to Find and Reuse. *Trends in Ecology & Evolution*, *34*(6), 494–496. https://doi.org/10.1016/j.tree.2019.04.005

Rainey, H. J., Pollard, E. H. B., Dutson, G., Ekstrom, J. M. M., Livingstone, S. R., Temple, H. J., & Pilgrim, J. D. (2015). A review of corporate goals of No Net Loss and Net Positive Impact on biodiversity. *Oryx*, *49*(2), 232–238. https://doi.org/10.1017/S0030605313001476

Rajagopalan, S. (2018). Blockchain and Buchanan: Code as Constitution. In R. E. Wagner (Ed.), *James M. Buchanan* (pp. 359–381). Springer International Publishing. https://doi.org/10.1007/978-3-030-03080-3_17

Raza, U., Kulkarni, P., & Sooriyabandara, M. (2017). *Low Power Wide Area Networks: An Overview* (arXiv:1606.07360). arXiv. http://arxiv.org/abs/1606.07360

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, *88*, 173–190. https://doi.org/10.1016/j.future.2018.05.046

Reyneke, M., Mullins, B., & Reith, M. (2023). LoRaWAN & The Helium Blockchain: A Study on Military IoT Deployment. *International Conference on Cyber Warfare and Security*, *18*(1), 327–337. https://doi.org/10.34190/iccws.18.1.944

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, *57*(7), 2117–2135. https://doi.org/10.1080/00207543.2018.1533261

Sahoo, S., Kumar, S., Sivarajah, U., Lim, W. M., Westland, J. C., & Kumar, A. (2022). Blockchain for sustainable supply chain management: Trends and ways forward. *Electronic Commerce Research*. https://doi.org/10.1007/s10660-022-09569-1

Sansone et al., S. A., & Catharina. (2019). FAIRsharing as a community approach to standards, repositories and policies. *Nature Biotechnology*, *37*(4), 350–351. https://doi.org/10.1038/s41587-019-0051-0

Schneider, A. (2012). Monitoring land cover change in urban and peri-urban areas using dense time stacks of Landsat satellite data and a data mining approach. *Remote Sensing of Environment*, *124*, 689–704. https://doi.org/10.1016/j.rse.2012.06.006

Sharma, A., Nayyar, A., Singh, K.J. et al. (2023). An IoT-based forest fire detection system: Design and testing. *Multimed Tools Appl (2023)*. https://doi.org/10.1007/s11042-023-17027-9

Sree, A. S., Deepthi, K., & Nikhil, K. (2023). *IOT Based Wildlife Monitoring System*. *4*(5).

Strange, N., Ermgassen, S. Z., Marshall, E., Bull, J. W., & Jacobsen, J. B. (2024). Why it matters how biodiversity is measured in environmental valuation studies compared to conservation science. *Biological Conservation*, *292*, 110546. https://doi.org/10.1016/j.biocon.2024.110546

Swan, M. (2015). *Blockchain: Blueprint for a new economy* (First edition). O'Reilly.

Swanson, T. (n.d.). *Great Chain of Numbers: A Guide to Smart Contracts, Smart Property and Trustless Asset Management*.

Szabo, N. (n.d.). *Unenumerated Bit Gold*.

Szabo, N. (1997). *The Idea of Smart Contracts*.

Thangavel, S., & Shokkalingam, C. S. (2022). The IoT based embedded system for the detection and discrimination of animals to avoid human–wildlife conflict. *Journal of Ambient Intelligence and Humanized Computing*, *13*(6), 3065–3081. https://doi.org/10.1007/s12652-021-03141-9

White, T. B., Petrovan, S. O., Booth, H., Correa, R. J., Gatt, Y., Martin, P. A., Newell, H., Worthington, T. A., & Sutherland, W. J. (2022). Determining the economic costs and benefits of conservation actions: A decision support framework. *Conservation Science and Practice*, *4*(12), e12840. https://doi.org/10.1111/csp2.12840

White, T. B., Petrovan, S. O., Christie, A. P., Martin, P. A., & Sutherland, W. J. (2022). What is the Price of Conservation? A Review of the Status Quo and Recommendations for Improving Cost Reporting. *BioScience*, *72*(5), 461–471. https://doi.org/10.1093/biosci/biac007

Wieczorek et al., J. (2012). Darwin Core: An Evolving Community-Developed Biodiversity Data Standard. *PLoS ONE 7(1): E29715. Doi:10.1371/Journal.Pone.0029715*.

Wilkinson, M. D., Dumontier, M., Aalbersberg, Ij. J., Appleton, G., Axton, M., Baak, A., Blomberg, N., Boiten, J.-W., Da Silva Santos, L. B., Bourne, P. E., Bouwman, J., Brookes, A. J., Clark, T., Crosas, M., Dillo, I., Dumon, O., Edmunds, S., Evelo, C. T., Finkers, R., … Mons, B. (2016). The FAIR Guiding Principles for scientific data management and stewardship. *Scientific Data*, *3*(1), 160018. https://doi.org/10.1038/sdata.2016.18

Wunder, S., Fraccaroli, C., Bull, J. W., Strange Olesen, A., Pacheco, A., Muys, B., Swinfield, T., Maron, M., Tegegne, Y. T., White, T. B., Zhang, H., Zu Ermgassen, S., Evans, M. C., Jellesmark

Thorsen, J., Jones, J. P. G., Eyres, A., & Dutta, T. (2024). *Biodiversity credits: Learning lessons from other approaches to incentivize conservation*. *Preprint*.

Yoeseph, N. M., Purnomo, F. A., Hartono, R., & Nuryani. (2022). Lora-based IoT sensor node for Real-time Flood Early Warning System. *IOP Conference Series: Earth and Environmental Science*, *986*(1), 012060. https://doi.org/10.1088/1755-1315/986/1/012060

Zu Ermgassen, S. O. S. E., Howard, M., Bennun, L., Addison, P. F. E., Bull, J. W., Loveridge, R., Pollard, E., & Starkey, M. (2022). Are corporate biodiversity commitments consistent with delivering 'nature-positive' outcomes? A review of 'nature-positive' definitions, company progress and challenges. *Journal of Cleaner Production*, *379*, 134798. https://doi.org/10.1016/j.jclepro.2022.134798