Drop Wireless

White Paper

V1.0

dropwireless.io

Table of Contents

Contents

Abstract

The telecommunications industry is on the cusp of a new era with the advent of 5G, promising widespread connectivity and the immense business opportunities associated with the Internet of Things (IoT). However, it also faces significant financial and technical challenges in providing the extensive and cost-effective coverage necessary for seamless machine-to-machine communications required by the IoT. These challenges are deeply rooted in the existing legacy infrastructure, which is dominated by incumbent carriers who struggle with the high costs of establishing and maintaining networks, creating barriers for new entrants. Unfortunately, these centralized network providers and their voice/data-centric systems are ill-equipped to harness the full potential of IoT and deploy cost-effective, densely populated networks. This barrier to entry has impeded growth and innovation. Thankfully, blockchain technology has emerged as a potential solution, opening the door to new possibilities.

Drop represents a paradigm shift in both technology and business. Our vision is to build a communications infrastructure that relies on the collective efforts of network participants, who are primarily owners of Drop nodes and devices. Operating within this individually operated ecosystem, the Drop system utilizes multi-layer blockchains to run the network and its financial incentive system. Similar to setting up a WiFi router at home, individuals can manage the deployment process of the Drop system. The integrated blockchains ensure network security, maintain financial processes, and securely preserve operational history and authentication records. Through the multi-layer blockchains, data requests are reliably handled without human intervention. In essence, the Drop ecosystem incentivizes individual owners to leverage their existing internet connections and set up nodes for the IoT by offering connection and coverage incentives.

Furthermore, we believe that the IoT industry requires an entirely new financial system capable of accommodating a wide range of use cases. To address this need, we introduced our own cryptocurrency called the Drop Wireless Infrastructure (DWIN) running on IoTeX blockchain. It enables highly efficient micro-level transactions within the network, avoiding unnecessary overhead fees.

Our platform leverages these technologies to create the most secure and efficient IoT infrastructure available, supporting the strategic growth of the network. We incentivize wireless nodes to ensure high availability and extended coverage. Device owners also have opportunities to earn DWIN rewards by performing tasks that enhance network coverage and reliability, such as providing wireless link quality measurements and geolocation data. With these measurements, the system can generate graphical representations of wireless coverage and estimated signal quality at various locations.

Drop is at the forefront of developing and delivering IoT infrastructure powered by advanced IoT-optimized blockchains. With hundreds of wireless nodes already operational across the country and overseas.

1 Introduction

Today's wireless telecommunications infrastructure primarily focuses on voice and content delivery for users on centralized carrier networks. Typical use cases may include voice calls, audio/video streaming, and Internet/social browsing. As we enter a new era of machine-generated communications, the system needs to offer an entirely new level of security and scalability to accommodate the sheer number of devices and mission-critical use cases.

The market research firm IoT Analytics estimated that in 2018, there were 7 billion IoT devices around the world, excluding smartphones, tablets, laptops, and fixed line phones [1]. These Internet of Things (IoT) devices may extend their uses into critical infrastructure, such as utilities systems, with implications for national security in areas like electricity and energy distribution. The number of active IoT devices is expected to grow to 10 billion by 2020 and 22 billion by 2025 [1]. In terms of market size, the global IoT market valuation was $151 billion in 2018, and it is forecasted to grow to $1.5 trillion by 2025 [1]. This growth potential is supported by the revenue and income growth rates of companies working in spaces across the spectrum of IoT software, cloud, and services.

Given the large and growing number of connected devices, the IoT architecture requires a highly secure, distributed network where the data can be neither manipulated nor attacked by malicious attempts on centralized data centers. With blockchain technology, data are cryptographically encrypted and stored in a digital ledger distributed over a large number of nodes. If a data modification is needed, it requires a consensus from the participating nodes, so an attempt on a single node will be denied.

Drop proposes a versatile, extensible, multi-tiered blockchain architecture to operate on a wide range of devices at a massive scale. The multi-tier architecture ensures that each blockchain operates efficiently and optimally to accommodate the unique characteristics of the network elements (devices, wireless nodes, and users). On the financial side, the Drop incentive system not only allows a highly cost-effective pricing structure, but also creates the possibility of achieving wide area coverage via collective networks of individually owned wireless nodes.

2 Blockchain IoT

2.1 Security Challenges for Centralized Cloud Networks

Most of the current IoT solutions are based on centralized cloud networks. In a centralized network architecture, the network/data management and control are concentrated in data centers managed by large existing companies. We believe there are significant issues with the centralized approach that present obstacles if the massive IoT revolution is to take place.

In a centralized network infrastructure, security and data breaches are the most significant issues for mission-critical IoT applications. Because adversaries can focus on a centralized data center, the networks are exposed and vulnerable to malicious attacks. This is not speculation: In April 2019, the world's biggest social network suffered the latest of many reputation-damaging breaches when it was revealed that records for more than 540 million users had been publicly exposed on Amazon cloud servers [2]. Another significant security breach occurred in 2018, when the private information of 383 million Starwood Hotels and Resorts guests was exposed, including 9.1 million payment card numbers and 23 million passport numbers [3].

2.2 Blockchain IoT

Blockchain is a network consisting of append-only distributed ledgers, which are "blocks" linked with one another. Once a network is set up with blockchain, it operates autonomously without central authorities. Modification of encrypted data stored in the ledgers requires a consensus among nodes to "approve" the change.

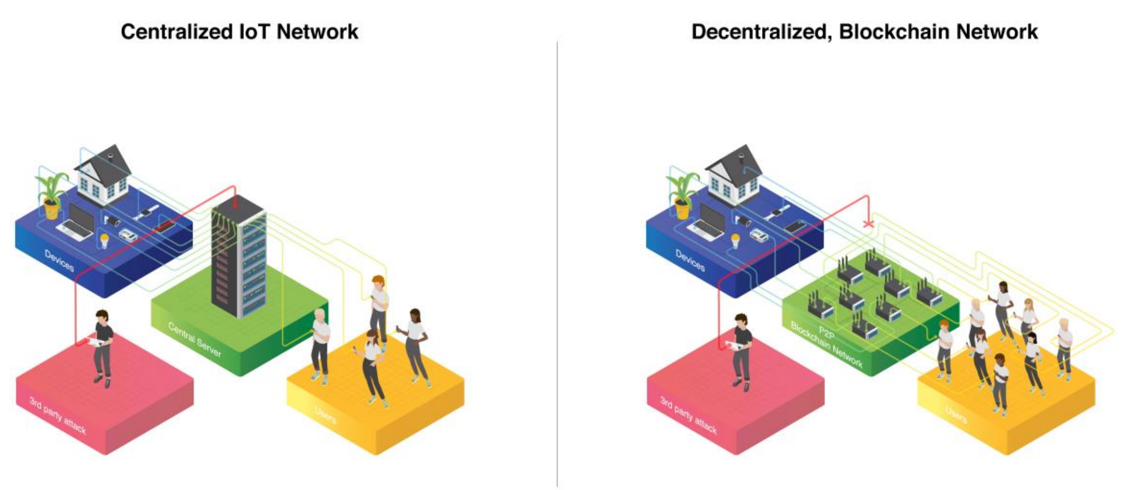

Figure 1 Single-point failure issue for centralized IoT network. With a blockchain IoT network, any malicious attacks would be isolated and recoverable from distributed ledgers

Figure 1 illustrates the vulnerability of the centralized network, in which a malicious attack on the central server can paralyze the entire network. In the decentralized blockchain IoT network, the attack would be isolated and recoverable, as the ledgers are duplicated on other nodes.

Challenges	Centralized IoT Cloud	IoT with Blockchain
Data Security	✕ Vulnerable due to single point failure	✓ Cryptographically encrypted
Data Privacy	✕ Potential for misuse	✓ Encrypted and operated with blockchain
Network Deployment Cost	✕ Significant due to installation logistics	✓ Moderate as the network is set up by motivated individuals

Table 1. Advantages of blockchain IoT and disadvantages of centralized IoT cloud

3 System Overview

The current paradigm of centralized telecommunications networks requires heavy investment and consolidated authority. As mentioned before, this high concentration of data information presents an increased vulnerability for broad-reaching malicious attacks. Centralized, top-down data control from a single corporate provider also allows them to pass costs down to individuals consumers. Not only do users not have control of the data they generate, but they are required to pay high access fees to use it.

This architecture is neither ideal nor sustainable for the growing influx of data and devices that is quickly approaching with the IoT revolution and the arrival of 5G.

Drop offers a radical new alternative to this legacy institution—a next-generation network that is built from the ground up by the people who use it, harnessing the power of distributed edge computing separate from centralized servers and allowing users to reclaim their digital property.

3.1 Community-Built Communications Network

Drop is essentially a web of community-based networks built by their users. It capitalizes on the capacity of individuals to deliver reliable, energy-efficient coverage and support for a massive number of devices at a fraction of the cost of traditional service providers. A local network is established with the activation of individual nodes, and network growth and expansion occur exponentially with each new wireless node. Each new network links to and builds upon other existing networks and devices within its coverage area, now more secure with an even wider area of coverage.

3.2 Decentralized Wireless Network

Drop's decentralized structure allows for a network that is both transparent and secure. Participants create, transmit, store, request, and purchase data all within the distributed environment and are supported by a fair compensation structure.

Because the network is built—and continues to grow—on infinite individual nodes, incapacitating the entire system is nearly impossible. Any attack on a node is confined to that node and that node alone. Moreover, the decentralized nature means that any information or data that originated from that node is still safely stored in the network and accessible from other nodes; it cannot be destroyed or altered by the attack on the target node. This is in direct contrast to a centralized network, in which an attack on the central server compromises every user's security and data, potentially incapacitating an entire system.

3.3 Data Privacy and Protection

In the extant communications environment, all data generated by users is routed to the cloud, where they no longer have any control over it. Data can be sold, used, and manipulated without user consent, knowledge, or compensation.

In a decentralized environment such as Drop, any information or data originating from a device using the network remains within the network. Metadata is extracted and stored securely in the blockchain as unalterable historical data and all raw data remains on the device.

3.3.1 Key Generation

Network users retain full ownership and control of their data via a public/private key pairing. At data origination, a pair of cryptographic public and private keys is generated and assigned to the user's device. The data, now safely stored in blockchain repositories, remains encrypted and inaccessible until the user releases the public key to a data consumer and receives compensation. Because the private key remains with the device, users remain in full control of their raw data, including approval for its distribution, forever.

3.3.2 Blockchain

Data generated by users in the Drop network is protected by multiple layers of blockchain, each with immutable and computationally impenetrable cryptography. The distributed nature of the network also ensures that data remains private and secured in the blockchain where it can be preserved and reinstated in the event of an attack on an individual node, instead of in a more vulnerable centralized server.

4 Technology

The amount of raw data generated in our daily lives continues to grow exponentially, but this raw data carries no measurable value until it is aggregated and processed for practical and beneficial use. Drop is providing reality-driven solutions and compelling value propositions for the future by bringing together advanced communications and blockchain technologies in an accessible, user-friendly platform.
The Drop network is comprised of three critical elements: multi-layer blockchain, IoT communications, and machine intelligence. Each of these are cutting-edge in their own right, but their full potential is only realized if they can be integrated into the broader context of a network. By combining these three powerful and dynamic technologies, Drop can provide a scalable, cost-effective, and unified platform that delivers unprecedented security, transparency, and efficiency. With Drop, we can efficiently store, manage, and facilitate the real-world implementation of today's explosion of information.

4.1 Multi-Layer Blockchains

Traditionally used for financial transactions, blockchain offers a unique solution to the increasingly fundamental issue of data security and ownership. As previously mentioned, blockchain technology can be used to create a distributed, decentralized network that maintains a perpetual, unalterable history of all data generated within it. The network can operate without central authority and ensures the duplication and recoverability of data in the event of a malicious attack.

Drop's unprecedented security and efficiency lies in the integration of three separate, overlapping blockchain layers—device, node, and user—each designed with distinctive characteristics to address specific challenges. For instance, the device blockchain needs to respond to real-time events and therefore requires frequent updates, while the user management blockchain may require updates much less frequently. By linking several blockchains together, every element of Drop can operate safely, securely, and autonomously without the inconvenience and vulnerability of consolidated authority. The redundancy created by multiple layers ensures the preservation and immutability of every piece of data generated by the network.

Additionally, using a separate blockchain for each of the network elements maximizes the system operation's robustness and reliability. The system must continue to operate at all times even when individual wireless nodes experience outages due to power and/or Internet connection failures. Multiple blockchain layers allow each element to continue to function independently and unaffected by any interruptions elsewhere in the network.

This approach to blockchain implementation also promotes full ownership of data by the users who create it, giving them the power to change, sell, and control it at their own discretion. Data created by devices is encrypted at the time of origin and a public/private key pair—which remains with the device—is generated. The encrypted data is then transferred to blockchain repositories for future use, where it remains encrypted and protected until the data owner gives permission to release it, along with the requisite public key.

4.1.1 Device

The device layer is capable of handling data streams and authentication for a massive number of registered devices. It is responsible for:

- Key creation and registration
- Cryptographic data encryption
- Device ownership management
- Location and sensor data generation
- Interfacing with third-party storage networks for raw data archiving
- Data authentication

4.1.2 Node

The wireless node layer creates the foundation of the network with expansive availability and reliability. Responsible for creating and operating the blockchains, the node is the key element to maintaining the network infrastructure and is required to operate 24/7, ensuring consistent reliability. The node layer facilitates:

- Daily block generation
- Multi-protocol network operation
- Node security management
- Machine learning and metadata
- Data encryption

4.1.3 User

The user layer secures the system’s financial integrity and serves as the network’s “first line of defense.” It consists of registered device owners and/or data consumers—essentially any individuals who use the network for data storage and transfer. The user layer also registers and authenticates users to prevent malicious network intrusions

Figure 2 Multiple blockchains for devices, wireless nodes, and user layers

4.2 IoT Communications

Integrating IoT with blockchain technology is premised on the deployment of a vast array of sensors and trackers to fully automate environmental, individual, and industrial processes. These IoT devices are the "feelers" of wireless communication and generate a tremendous amount of data that has the potential to improve any number of domains, from manufacturing productivity and logistical efficiency to improved health and quality of life.

By implementing cutting-edge ultra-wideband (UWB) technology into its network, Drop is able to fully support three different wireless protocols—LoRaWAN, WiFi, and BLE—for consistent, broad-reaching, and high-precision opportunities in data generation, transmission, and trading.

4.2.1 Wireless Protocols

LoRaWAN, or long-range wide area network, is a radio protocol that combines extended coverage capability with low power consumption, making it particularly well-suited for the IoT network. LoRa is our primary focus in the initial network deployment to foster the adoption of IoT ecosystem.

WiFi provides the blockchain network of WiFi hotspots through which users can easily access the Internet without a cumbersome login process. It also serves as a basis for high-precision indoor location and pervasive positioning.

Inclusion of *Bluetooth Low Energy (BLE)* will further extend the Drop node's applicability, as nearly 4 billion Bluetooth® devices are forecasted to ship in 2018 alone [4].

Figure 3 shows the Drop network, in which a variety of protocols are interconnected through the Internet coverage of a wireless node.

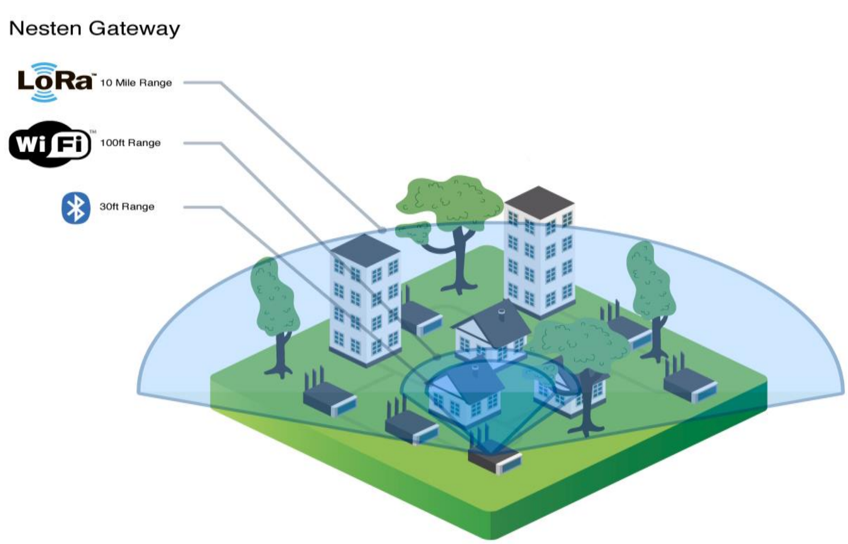

Figure 3 Overview of Drop system infrastructure

4.2.2 Wireless Node

Though their growing capabilities for internal processing and analytics dramatically reduces their dependence on cloud processing, high bandwidth requirements, and cumbersome storage, IoT devices still require constant and immediate event detection, analysis, and storage.

Drop's wireless nodes—upon which the network is built and sustained—are high-performance computing platforms combined with multiple wireless protocols to facilitate an array of user scenarios and coverage ranges. These nodes serve as decentralized wireless nodes that are connected through an existing IP network infrastructure and supported by Drop's multiple blockchain layers.

The wireless node nodes also serve as the first-line reception and analysis point for raw data generated within the network. The programs embedded in the nodes facilitate the recording, storage, and processing of massive amounts of raw data into usable metadata that is secured in the blockchain. This metadata will eventually form the basis for allocating monetary compensation and creating transaction functions between participants.

Externally, node hardware is operated and maintained by node hosts using existing IP networks and a power source. Internally, the wireless node technology supports the wireless protocols as well as extensive blockchain processing.

Figure 4 shows the wireless node architecture with key hardware elements in the lower box and software components in the upper. In the hardware layer, the Drop wireless node utilizes an i.MX8 from NXP Semiconductors; the i.MX8 is a quad-core ARM processor, one of the most advanced low-power processors. The software runs on a 64-bit Linux operating system with a complete network server, the inclusion of which allows data parsing, processing, and routing to support the blockchain operations.

Figure 4 System overview of Drop wireless node, G1

4.2.3 Tracker

The basic premise of the IoT is the deployment of a vast array of sensors and trackers to fully automate environmental and industrial processes by collecting, aggregating, and securing data for critical event detection. We believe that, in a few years, these wireless sensors will become pervasive in all major industries, as well as everyday consumer life. They will produce tremendous amounts of data to analyze and store, data that has the potential to improve productivity in manufacturing, promote better health for individuals, and create lifestyles with more leisure time as more mundane tasks become automated.

The breadth and depth of Drop’s technology competencies, skill sets, and domain expertise in the IoT sphere makes us uniquely positioned to optimize network capabilities, and our exclusive proprietary tracker strengthens our already solid foothold in the LoRaWAN domain. LoRa and BLE compatible, powered by the blockchain, and ready for immediate Proof of Coverage verification, Drop’s tracker expands possible use cases by instantly and seamlessly connecting devices and services with multiple protocols. The waterproof tracker, as shown in Figure 5, features 6-axis motion sensing and GNSS and WiFi for geolocation, making it ideal for everything from pet tracking and health monitoring to logistic and asset management.

Figure 5 Wearable Tracker, T1

4.3 Machine Intelligence

The fundamental challenge associated with the ever-increasing data generation of IoT devices is the ability to analyze and detect any significant events in real time, to make sense of and giving meaning to all of this data. Drop’s approach to this challenge is rooted in built-in machine learning (ML) capabilities. Real-time machine learning capabilities, coupled with Drop’s nodes fully integrated network servers, provide the cloud analysis and instant event response necessary to optimize the potential of IoT communication. The ML will be implemented with a multi-layer neural network, as shown in Figure 6.

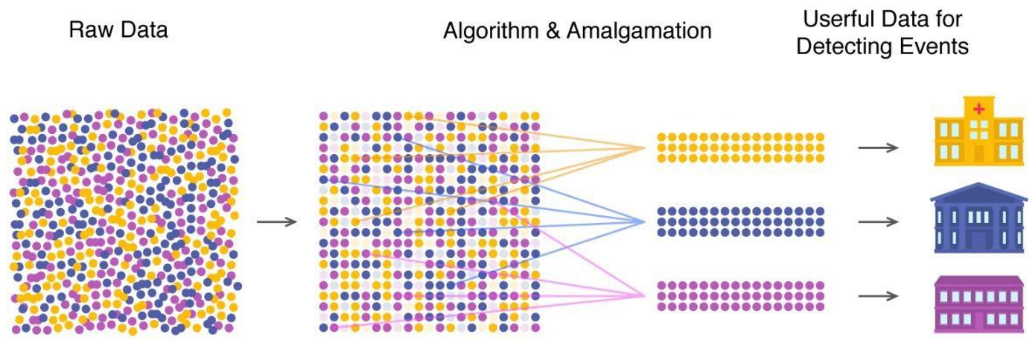

Figure 6 Neural network based-machine learning to autonomously detect safety critical events

Because the Drop network is woven with multiple layers of blockchain technology, expanded coverage from wireless nodes, and independent users all operating simultaneously, massive amounts of raw data can be collected, analyzed, processed, and stored constantly and immediately. Not only can the network quickly extract high-value metadata from important events on a continuous basis, it is securely storing every piece of data created, further improving network security.

4.3.1 Machine Learning at the Hardware Level

Drop ML is focused on metadata extraction and event detection in real time. The metadata extraction minimizes system and storage overheads in the blockchain infrastructure, while the event detection facilitates an effective, efficient response to timing critical solutions.

Drop's ML capabilities are built into the node software where it processes raw data, extracts and encrypts metadata, and sends all data to the blockchain as data packets, or blocks.

4.3.2 Artificial Intelligence for Data Analysis

Drop AI combines ML-extracted metadata and events with domain expertise and heuristics to influence higher decision-making processes. It is ultimately designed to mimic the cognitive function of human intelligence in addressing specific, targeted domain needs.

Also integrated into the node software, Drop's AI technology combines the data packets into superblocks, chains them together, and further processes the metadata.

5 Ecosystem

As cities, communities, and homes become increasingly “smarter,” the need for perpetual, dependable, and affordable IoT coverage becomes increasingly paramount. Drop’s multi-layer infrastructure—woven with devices, users, and wireless nodes and combined with advanced machine learning, artificial intelligence, and IoT—delivers unprecedented service, safety, and security traditional providers can’t match. It is the first technology of its kind to expand blockchain and wireless communication into a reliable, accessible, and community-owned asset that IMPROVES our interconnected experience.

Our mission is to build and establish a self-sustaining ecosystem that is designed to support every level of user and that is economically viable and beneficial for all participants. Drop offers a unique model that allows individuals to provide reliable, energy-efficient coverage and data management for a massive number of devices at a fraction of the cost of traditional providers. By facilitating the generation, storage, and exchange of data, services, and economic benefits, wireless node hosts, device owners, and data customers work together to create the Drop ecosystem. Each participant in the coexistent ecosystem is economically motivated to pursue specific behaviors that create and increase data value and foster the growth and expansion of the network.

5.1 Ecosystem Participants

Drop requires three core participants. These participants create, transmit, store, request, and exchange data within the distributed network in a secure and transparent manner, supported with a fair compensation structure.

1. **Wireless node hosts** —Individuals who purchase, install, and maintain G1 wireless nodes, the network’s primary receivers. The node houses the hardware and software necessary to enable network establishment and growth. Wireless node hosts are the pillars of the network and are rewarded for operating the nodes and generating the blocks. They are incentivized to install and maintain nodes in the most optimal location for providing maximum communication spot coverage and for pursuing consistently high-performance levels, stabilizing the network and building more complete coverage.
2. **Device owners** — Individuals who purchase and use IoT devices for individual or commercial function that operate on the Drop network. Owners can actively participate in the network by expanding and demonstrating coverage of the wireless nodes through their own devices. Device owners maintain complete ownership of the data they create on the network with their device and may be rewarded for generating useful data. When they request data for their own use, they also become the data customer.
3. **Data customer** — Individuals who pay a reasonable fee for data generated on the network and stored in the network’s blockchain repositories. The term applies to both an individual customer and a corporate or enterprise customer. Individual data customers purchase data on demand for personal use while corporate customers purchase data via contract. Data customers serve as an inflow of funds for the network, strengthening the ecosystem and increasing network value as demand in the data market increases.

5.2 Data Perspective

In today's extant telecommunications structure, the bulk of the world's data remains tied up in legacy networks reliant on centralized servers. Data is accessible to users via ever-increasing usage fees but available to corporations and enterprises virtually unregulated. With Drop's decentralized, ground-up design, only backup and duplicated metadata is stored in the blockchain. Raw data generated from devices remains with the device owner. Moreover, release of any data, including that stored in the blockchain, to anyone other than the owner—who created the data—requires exclusive owner permission as well as a public key.

Data mining is one of Drop's core functions. During this process, raw data collected from the device and sent to the node to undergo ML and AI processing—with permission from the device owner—is converted into meaningful, more valuable data, or "metadata." It is this metadata that is sold to data customers in the data market, freeing up resources to reward participants in the Drop ecosystem.

Data flow in the Drop network:

1. Data is wirelessly transmitted from the sensor or tracker device to the G1 wireless node
2. G1 wireless node hashes the data, generates a block, and transmits it to the Drop blockchain
3. Drop blockchain stores and prepares data for user applications in a bounty pool
4. Individuals and enterprises request data for on-demand or analytics
5. Upon approval from data owner, data is released to requester

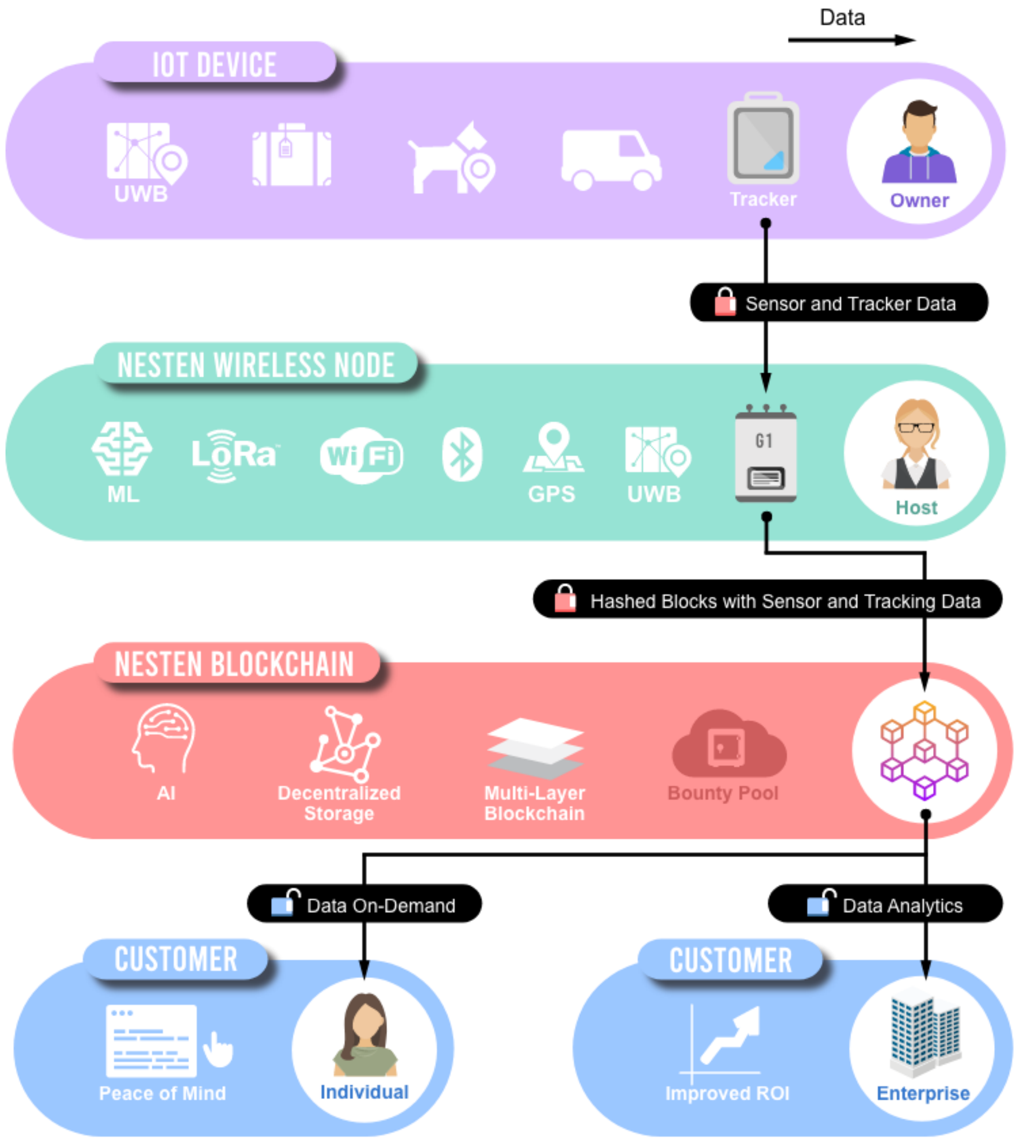

Figure 7 Data perspective of Nesten ecosystem

5.3 Financial Perspective

Rewards to Drop participants are paid in cryptocurrency. This cryptocurrency is used not only as a reward for maintaining the blockchain ecosystem, but also as a currency medium for distributing all data generated in the ecosystem. Drop's cryptocurrency—the Drop Wireless Infrastructure, or DWIN—is listed on the global cryptocurrency exchange and linked to the real economy, making it a stable, cost-effective method of buying and selling data created in the ecosystem while also strengthening and growing the network.

Financial flow in the Drop network:

1. Individual or enterprise data customers request data directly from the data (device) owner using DWIN
2. Bounty pool serves as a reserve for DWIN distribution
3. Device owner and wireless node host are both compensated in DWIN for their contributions
4. DWIN is real financial compensation for the data created by device owner

5.3.1 Drop Wireless Infrastructure (DWIN)

The financial compensation aspect of our ecosystem is critical for motivating node operators to maintain the consistent and optimal performance of their nodes, and, in turn, the network as a whole. Without meaningful economic compensation, node operators do not have adequate incentive to maintain the node, undermining the security and reliability of the entire network.

Compensation is awarded by our cryptocurrency, DWIN. Compensation in cryptocurrency provides a cost-effective solution that links monetary rewards to the real economy without the added requirement of transaction fees or third-party entities.

5.3.1 Handling of Micro-transactions

DWIN is the essential currency of the Drop ecosystem and can be used for data access. In most cases, IoT data transmissions will incur only a tiny fraction of one DWIN coin. As such, an actual commercial transaction will take place only when a user accumulates a certain number of data transmissions and/or requests above a preset threshold. This thresholding mechanism is essential to minimize overhead associated with coin transactions. A simple example may be a location tracking use case in which a GPS tag may be sending its location every minute. This will amount to 720 data transfers per day. It will be far more efficient to execute a single financial transaction over a sufficient period as opposed to each occurrence.

As mentioned in 5.1, the Drop blockchains will maintain escrow pools to reduce the number of transactions that can occur across the different domains of data users, node hosts, and device owners. In essence, each of the network participants will only need to interact with the escrow pools. This will also help to reduce miniscule peer-to-peer transactions.

As shown in Figure 17, the Drop network maintains an "escrow" pool to enable an efficient financial ecosystem, minimizing miniscule transactions that are expected to occur in IoT systems.

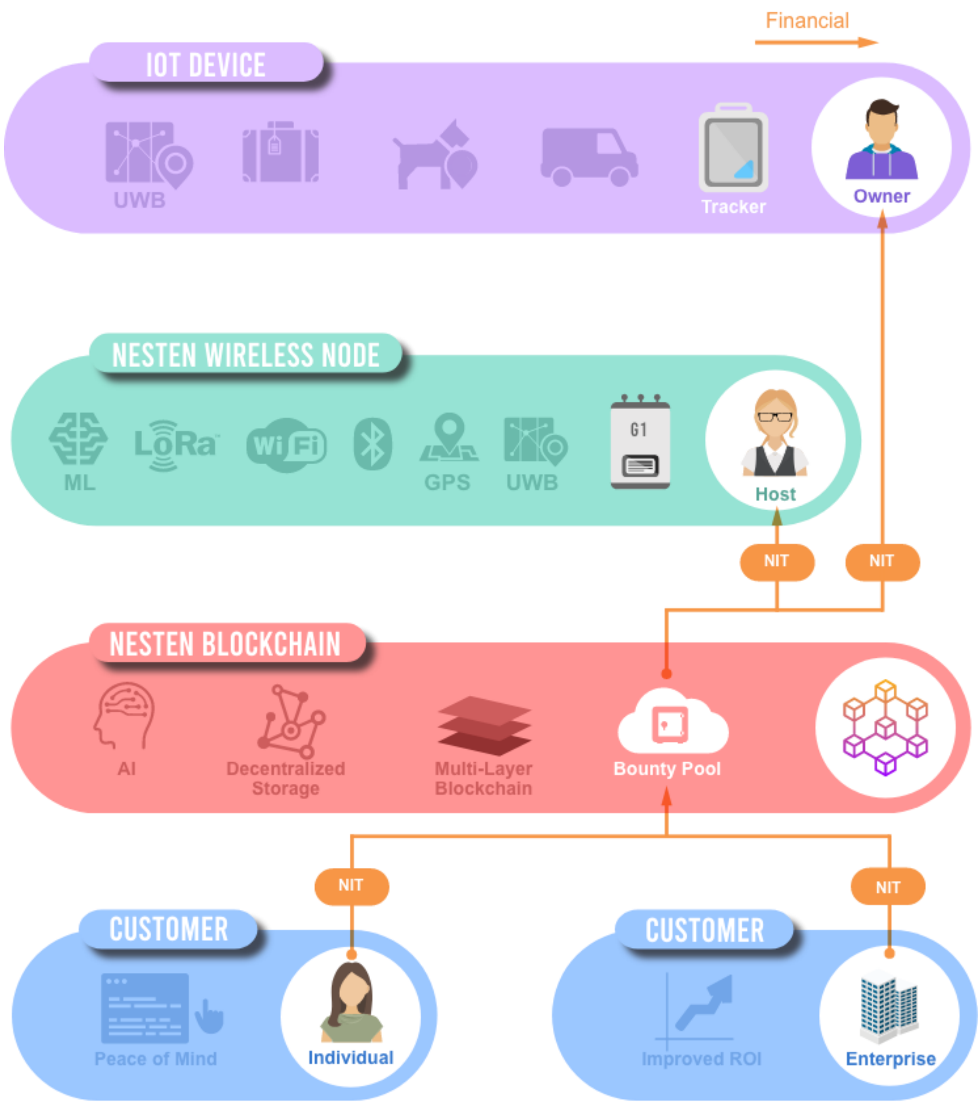

Figure 8 Financial perspective of Nesten ecosystem

5.4 Proof System Built for Network Reliability and Coverage

Drop's decentralized network depends on the reliable and continuous operation of the constituent wireless nodes. Thus it is essential to keep the node owners motivated to maintain a reliable Internet backhaul connection as well as uninterrupted power source. Drop's financial ecosystem is built to provide such motivation. It is also intended to be fair and transparent as well as being effective. The ultimate goal is that such an ecosystem can lead to a self-sustaining operation as well as network expansion.

Drop's proof system is based on five separate proof metrics to improve the network performance and expand the coverage as well as values of data generated and processed within Drop network. The proofs themselves are determined according to objective criteria that are measured by the proprietary programs built into the Drop's multi-layer blockchain. While each of the five key metrics serves its own purpose, they collectively help to achieve the network reliability and availability to reach commercial viability. The metrics will continue to be fine-tuned and optimized as we find more about how the ecosystem behaves in response to financial incentives.

5.4.1 Proof of Performance (PoP)

The primary goal of PoP is to achieve the reliability needed for a dependable communications network. Each node in the network sends a “heartbeat” status message to the blockchain at regular interval, which currently occurs at every hour as shown in *Figure 9*. The heartbeat represents a snapshot of the node’s performance as well as the quality of its Internet connection. The collective integration of the heartbeats from all of the nodes provides a visibility of the entire network operation on a continuous basis. If the PoP blockchain does not receive a heartbeat from a node for several consecutive intervals, a notification will be sent to the node owner with appropriate action to take.

Example of Proof of Performance in practice:

Once a wireless node is purchased, plugged in, and properly configured, the node will emit a “heartbeat” message to the blockchain every hour over a 24-hour period to signal that it is connected to the Drop network. These messages are recorded and stored in the blockchain. If the node completes 24 messages within the 24-hour period—indicating that there were no outages or interruptions in power—the node operator will be rewarded.

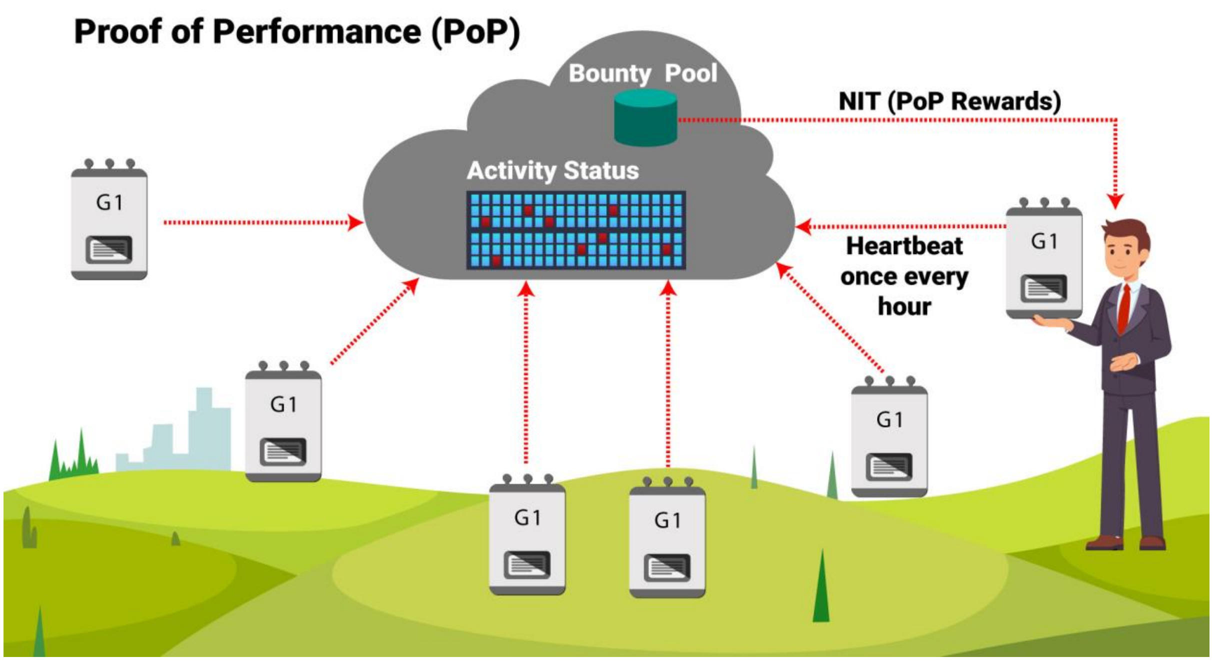

Figure 9 Proof of Performance

5.4.2 Proof of Coverage (PoC):

In wireless communications, a dependable coverage is essential to capture commercial opportunities. Drop has its unique means of verifying its own coverage. The Drop is developing a wearable tracker not only to track locations but also to verify its wireless coverage.

Example of Proof of Coverage in practice:

A Drop tracker is synced with a wireless node that has been plugged in and properly configured. The tracker is then deployed throughout the node's projected coverage area to evaluate the existence and strength of the signal in various locations. The node will register data collected from the tracker, indicating that the node is transmitting a suitable signal throughout its designated coverage area. Both the node operator and the tracker owner will be rewarded for coverage verification.

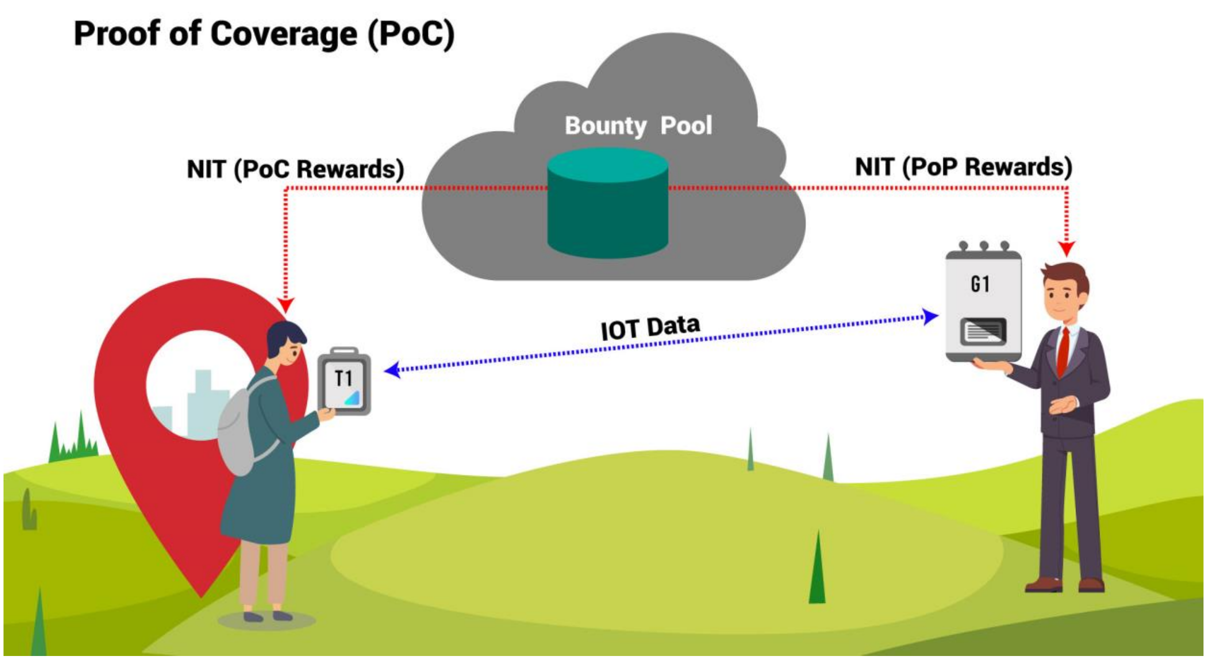

Figure 10 Proof of Coverage

5.4.3 Proof of Data (PoD)

PoD is a reward distributed according to the amount of data collected by the wireless node. It is evaluated based on the level of data "traffic" passing through the node and the number of data packets that are processed by the node.

Example of Proof of Data in practice:

Data generated by a device on the Drop network is received by the wireless node, processed into metadata packets, and sent to the blockchain to be archived. The blockchain maintains a tracking record of all data submitted from each wireless node. The node operator will receive a fixed amount for a baseline amount of data processed through their node and will be rewarded an additional DWIN for amounts above and beyond the baseline.

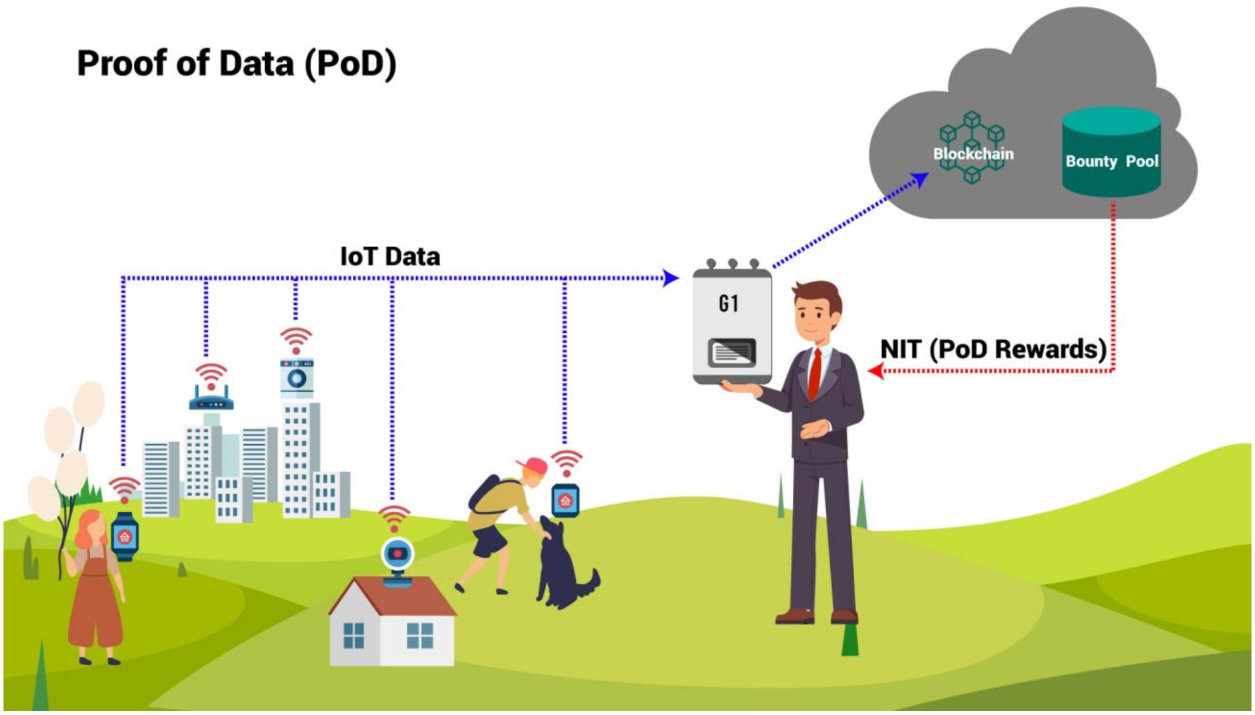

Figure 11 Proof of Data (PoD)

5.4.4 Proof of Value (PoV)

Data means nothing unless someone can use it. During Drop's data mining process, raw data, received from devices, undergoes Machine Learning processing, where any underlying patterns can be detected.

An example of PoV in practice:

A patient in a hospital can be monitored on continuous basis. His/her walking patterns can represent the patient's health conditions. The node owner, who is responsible for data processing, can receive DWIN rewards for performance of the data extraction.

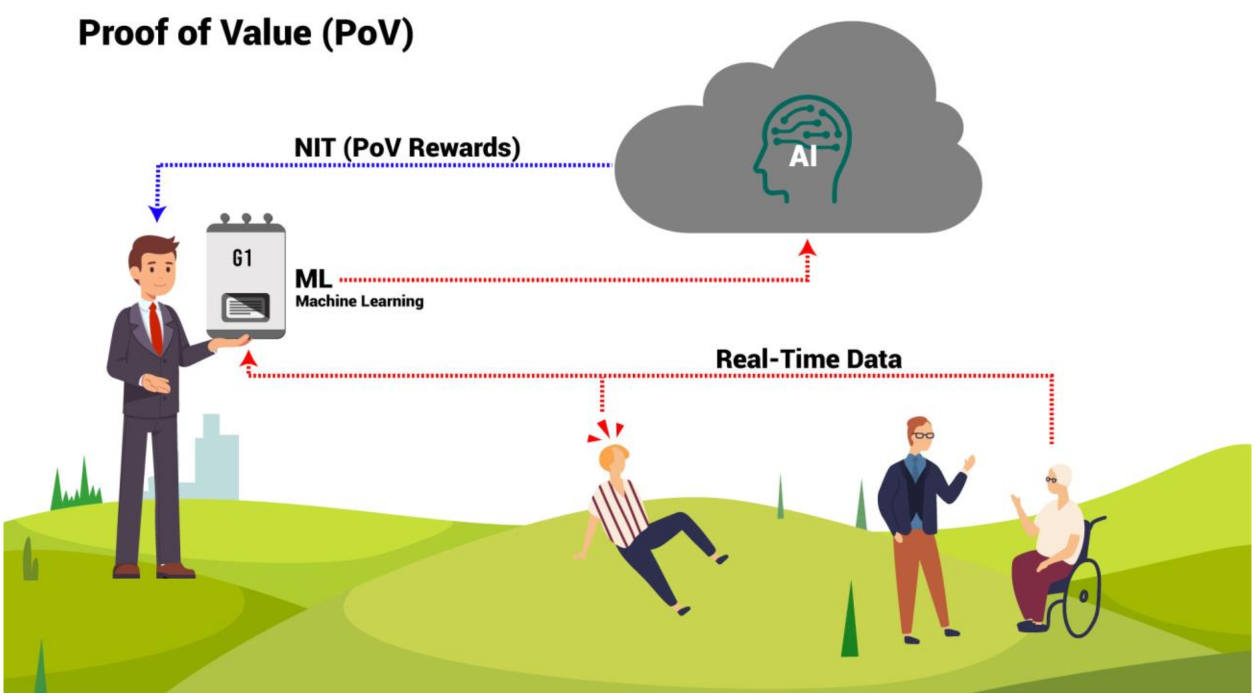

Figure 12 Proof of Value (PoV)

5.4.5 Proof of Efficacy (PoE)

The broader the Drop network is, the stronger its security and the greater the accessibility. Unlike the centralized telecommunications networks, which lose bandwidth and speed with an increase in users, Drop's decentralized framework improves in performance as it expands; more users actually makes it operate better and more securely.

PoE rewards are evaluated based on the geographical efficacy of the node location. It is a one-time incentive bonus paid when a node establishes network coverage in a previously uncovered area.

Example of Proof of Efficacy in practice:

An individual in an area without Drop coverage purchases, installs, and properly configures a wireless node. When that wireless node successfully establishes network coverage for the surrounding area, the wireless node operator receives additional DWIN rewards for expanding the network into a new strategic location.

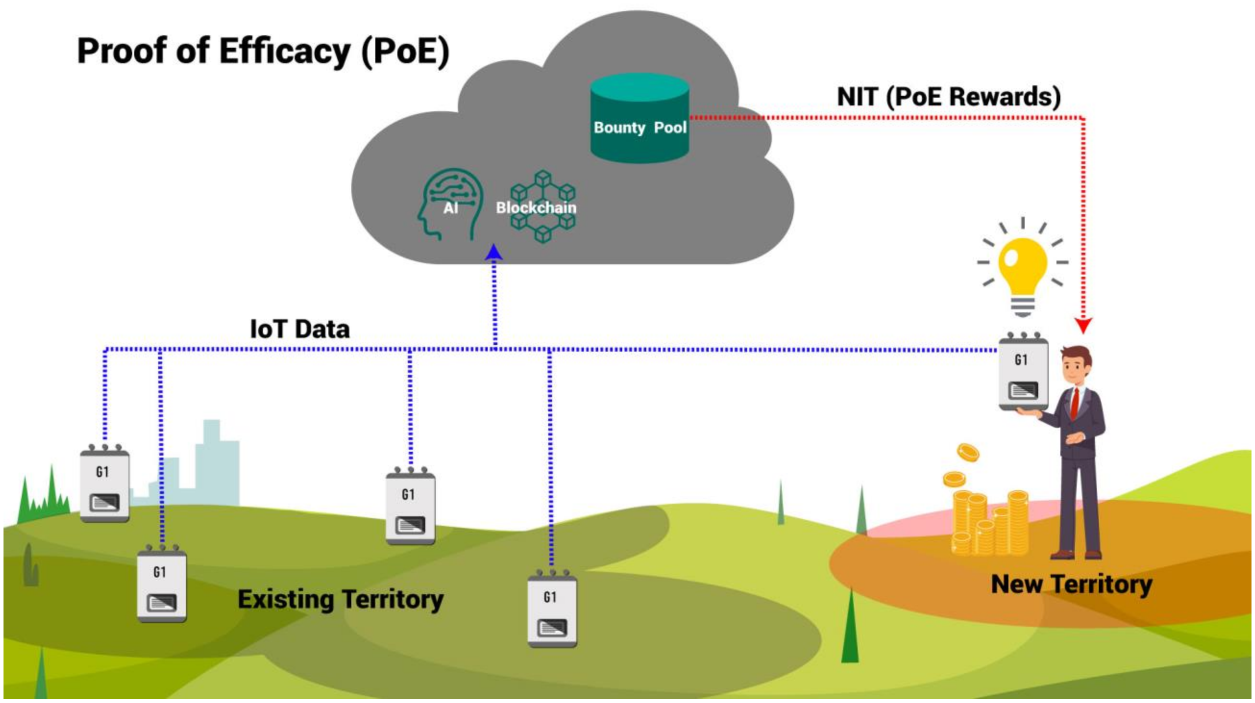

Figure 13 Proof of Efficacy (PoE)

6 Tokenomics and Use Cases

IoT communications services often require constant interactions among heterogeneous devices, protocols and applications across an array of stakeholders. As such, a financial architecture that can efficiently support micro services is key for large-scale, complex IoT use cases such that all stakeholders are fairly compensated without third-party overheads. Our token, DWIN, was created for this purpose of supporting and facilitating real-world use cases in a highly efficient manner.

6.1 Location and Motion Tracking Use Cases

The versatility of the advanced wearable described in Section 4.2.3 supports a number of possible use cases. Foremost are senior care and pet tracking.

In the senior care scenario, Drop's end-to-end system can track client locations and enable medication reminders or emergency assistance support, as well as push motion sensing notifications for prescribed events like falls. For pet tracking, Drop and the device can allow pet owners to monitor and analyze health diagnostics, receive alerts or notifications if the pet leaves a designated area, and quickly locate a missing pet. The entire operational costs can be covered with DWIN, eliminating third-party overheads and paperwork.

Unlike other system providers and integrators, Drop is committed to and capable of providing a complete turnkey solution that gives potential customers the technical and financial advantages while also minimizing third-part overheads.

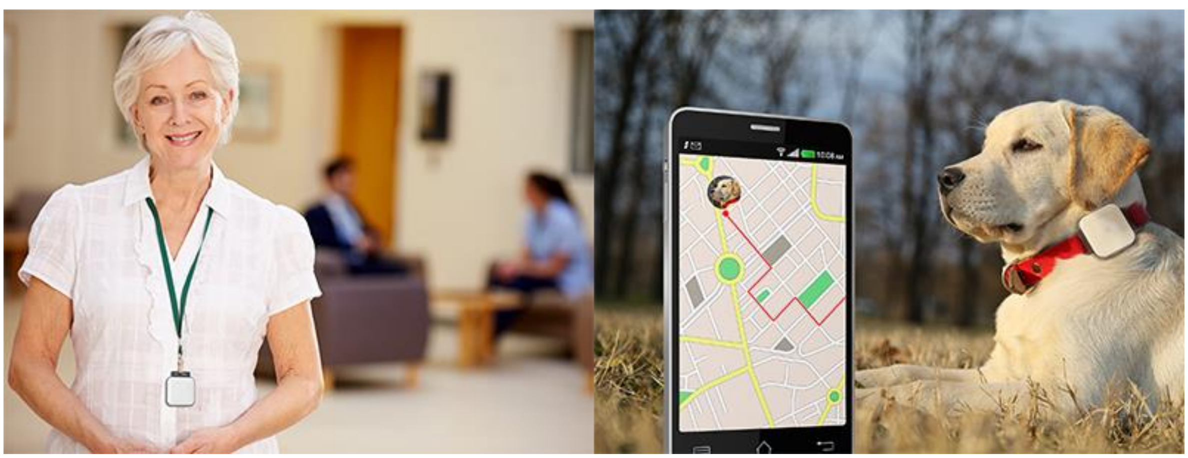

Figure 14 Use case for wearable tracker

6.2 Shared Smart Parking System

Drop has also developed a smart parking platform that can monitor in real time the occupancy status of parking spaces via LoRaWAN wireless connectivity. The real-time monitoring capability allows the concept of shared parking spaces. Furthermore the parking fee transactions can be conducted all within the Drop blockchain. The bounty pool operates as an escrow process in which the payment from the user is held upon occupying the space and released when the user leaves the space according to the reserved time.

The advantages of DWIN as the primary currency to operate the system are two-fold. Firstly, it minimizes overheads, which in turn leads to cost saving for space users and enhanced profit for space owners. Secondly, it provids financial flexibility to promote and facilitate the consumer adoption of the shared parking economy. In particular, users and owners who currently hold DWIN based on their DWIN accumulation via the proof mechanims described in Section 5.4 will have opportunities to utilize DWIN without spending cash.

As the shared parking deployment gains traction, the wireless infrastructure initially established for shared parking can be used for other purposes, expanding the profitability potential for the wireless node owner.

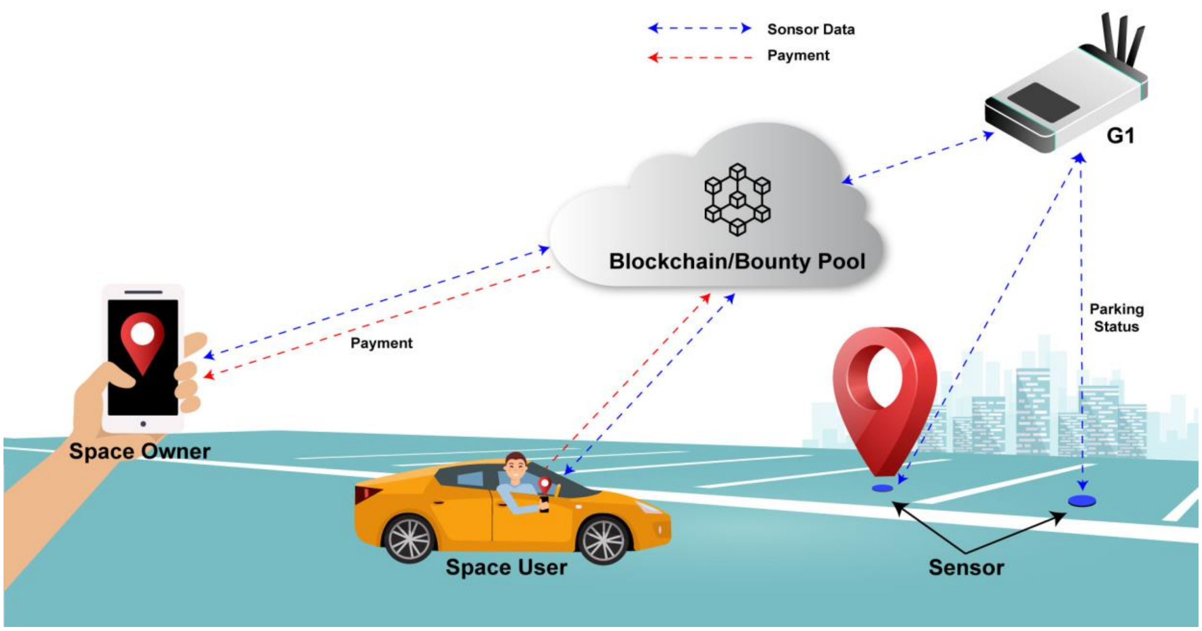

Figure 15 Shared smart parking

6.3 Autonomous Vehicles Traffic Management System (Patent Pending)

Self-driving vehicles are the future of the automotive industry, but most development to date in this sphere addresses just half the challenge of a safe and dependable driving environment, primarily limited to sensor technology and machine learning to make individual cars more intelligent as opposed to improving the entire system operation.

The driving ecosystem as a whole consists of myriad moving parts and elements beyond single vehicles—such as other vehicles and drivers, pedestrians, highway infrastructure, and weather—all constantly changing and interacting instantaneously. Universally reliable autonomous driving requires a strategically designed system-level approach that integrates all of these elements and allows them to communicate continuously and instantaneously with each other via secure, immutable data exchange and multiple wireless protocols.

Drop's distributed blockchain network addresses the critical shortcomings of extant approaches to developing autonomous driving, which depend primarily on improving the sensing and processing capabilities of individual vehicles.

By integrating multiple wireless technologies, including a secure multi-layer blockchain, our network provides the system-level solution necessary to improve the driving environment, balancing fast response times with high-level security. Multiple levels of blockchain allow for the cryptographic encryption of data that cannot be misused or hacked, while varying degrees of wireless protocols enable uninterrupted, accurate, and critical time-sensitive data exchange between components within milliseconds. The integration of multiple technologies and wireless protocols with dynamic real-world scenarios allows an infinite amount of data regarding the driving environment to be exchanged instantaneously and securely, drastically improving the safety of autonomous driving for drivers and pedestrians alike. Moreover, unlike narrowly-focused technological advancements implemented in singular vehicles or system layers, our complete, turn-key solution is flexible and broad-reaching enough to lend itself to secure and accurate data exchange applications in various transportation and logistics sectors.

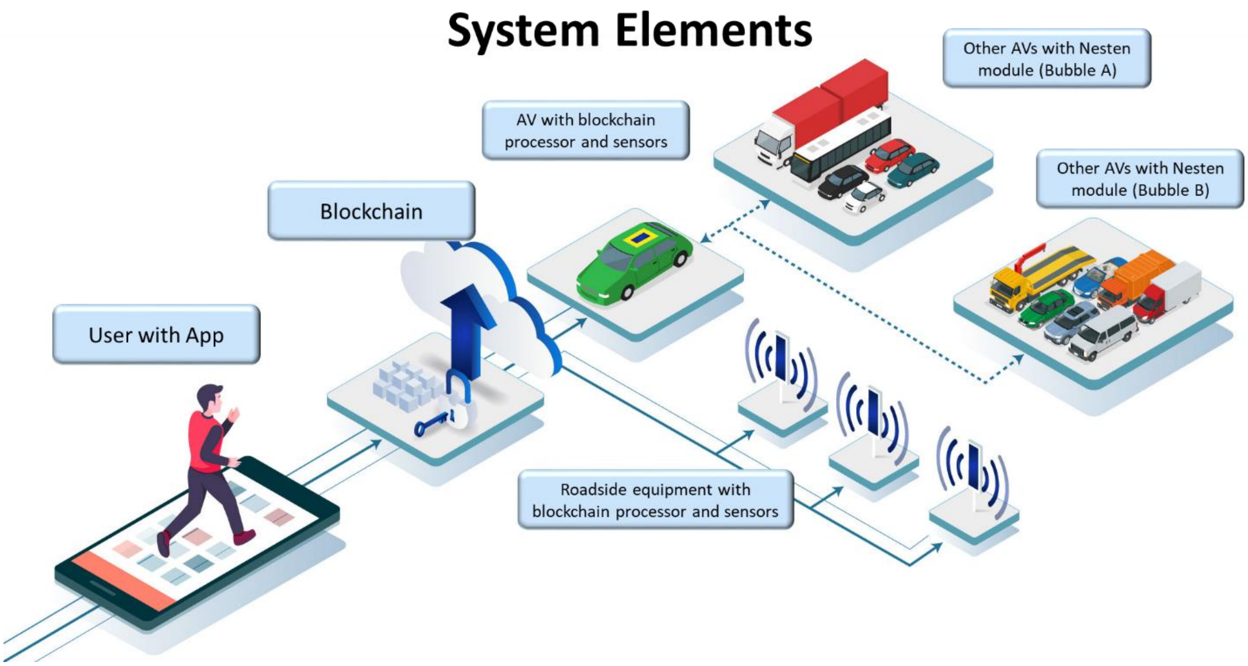

Figure 16 System elements of Drop's autonomous vehicles traffic management system

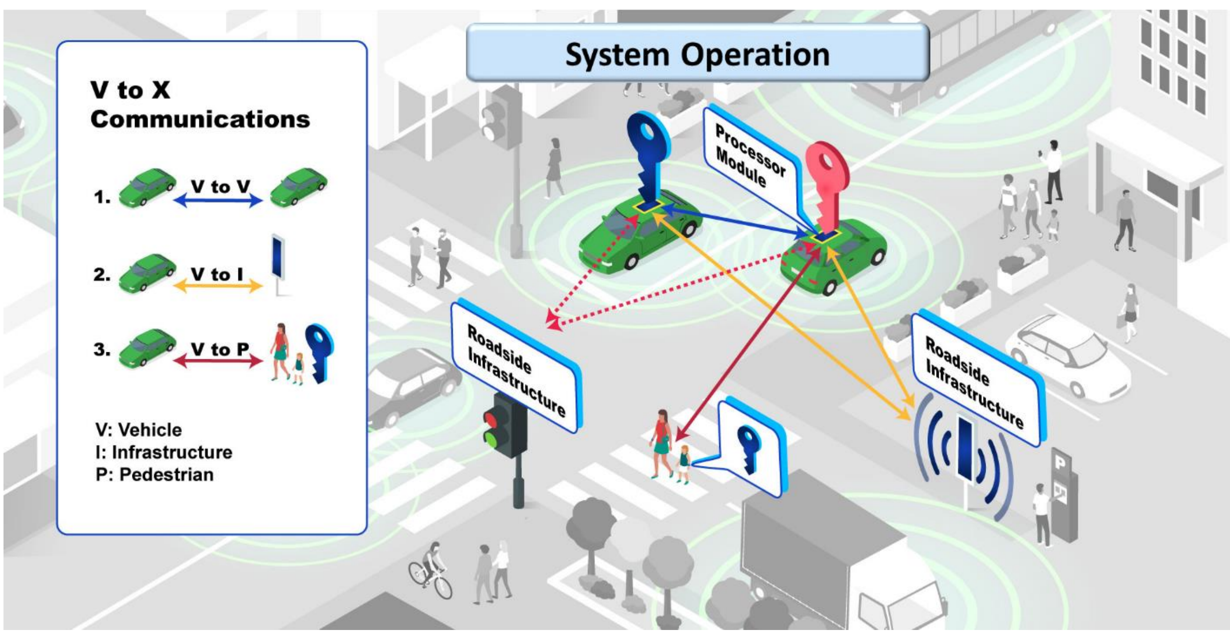

Figure 17 Operational view of Drop's autonomous traffic management system

7 Current Status

As of May 2031, Drop has deployed more than 1,500 G1 nodes across major markets in the U.S., including Houston, Georgia, California, the New York, New Jersey, and Washington, D.C. suburbs, as well as select markets in Canada, Mexico and South Korea. Drop's consumer-based deployment model enables end users to deploy their own flexible LoRa-based applications built on the G1 node, and operate and maintain their own IoT network without the associated costs traditionally found with telecom carriers. Leveraging the end user and blockchain as the cornerstone of each LoRa-based deployment, Drop is also able to provide extensive data protection and privacy.

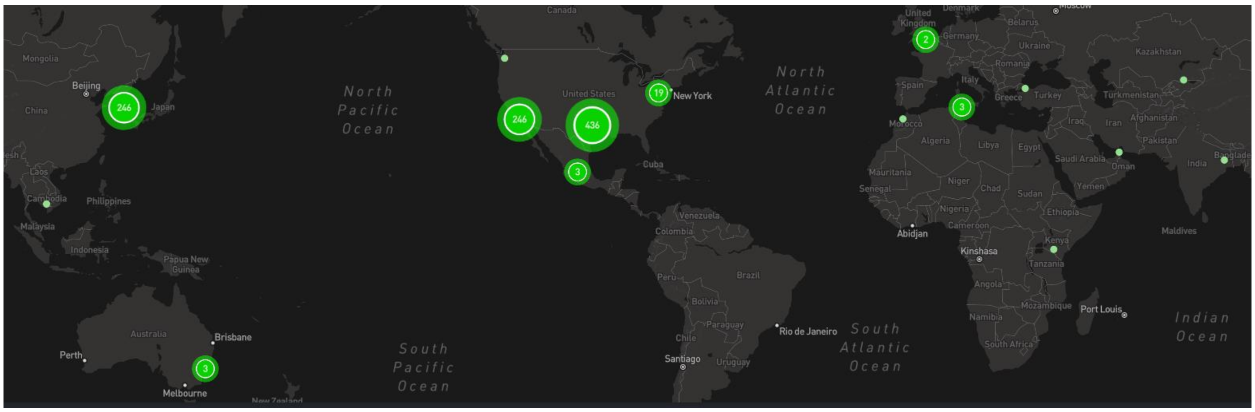

Figure 18 Current Status

8 Team Drop

Core Team ***Advisor***

Andrew Baek PhD

- >24 years of wireless communications
- Startups, Lucent Bell Labs
- PhD and MS from U of Penn
- BA from Cornell

H Paek PhD

- > 24 years of SOC and AI development
- Startups, Kolorific, Samsung Electronics
- PhD, MS, and BS from SNU

H Law

- Successful entrepreneur since 1999
- CEO at Trasilica, Tensorcom, Ethernom
- MSc from Univ of London

J Mun PhD

- > 20 years in electronic manufacturing
- Substantial experience in supply chain management
- PhD, MS, and BS in EE

J Goldman

- Embedded systems
- Mobile app development in iOS and Android
- BS in CS from UCI

E Shin

- Full stack Engineer
- iOS and Android development
- Master in CS from USC

J Xing

- 15 years of embedded software development
- Lucent Bell Labs, BTI Wireless

S Igor

- IoT software engineer
- LoRa protocol
- Cloud integration
- University of Calcutta, B. Tech

E Ding

- Embedded system
- STM32 development
- ARM-based MCUs

References

(1) "State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating," *IoT Analytics*, https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

[2] "Another 540 Million Facebook Users' Data Has Been Exposed," *Slate*, https://slate.com/technology/2019/04/facebook-data-breach-540-million-users-privacy.html

[3] "Starwood Guest Reservation Database Security Incident", https://answers.kroll.com/

[4] "2018 Bluetooth Market Update," https://www.bluetooth.com/bluetooth-resources/2018-bluetooth-market-update/

[5] "Delegated Proof-of-Stake Consensus," https://bitshares.org/technology/delegated-proof-of-stake-consensus/