



Emerald Circuit

Intelligent Objects For Guaranteed
Product Authenticity

Introduction

The cryptocurrency industry and its underlying technology blockchain have undergone three major cycles of innovation and development. In each cycle, new decentralised applications and innovative solutions are put forward to solve existing bottlenecks - oftentimes on the shoulders of prior development. In line with this dynamic, **Emerald Circuit offers a solution to the 'garbage-in, garbage-out' problem that plagues most real world blockchain solutions: secure and networked data collection from intelligent objects.**

Emerald Circuit is a cryptocurrency-based sidechain network focused exclusively on secure data collection and management, using proprietary intelligent objects. Built upon a fully developed and operable blockchain infrastructure, Emerald Circuit focuses on the physical collection of data using 128-bit encryption, patented Internet of Things technology, and original sidechain networking to provide data security and management, as well as anti-tampering and anti-counterfeiting services. From the initial point of collection, until it is hashed onto the blockchain, Emerald Circuit collects, connects, and secures all data in order to guarantee authenticity, increase efficiency, and provide the first fully encrypted and cost-efficient foundation for any network of smart objects.

Understanding the Context

Since the creation of Bitcoin in 2009, cryptocurrencies and digital tokens have exploded across financial markets. Over the past decade, three cycles of growth have ushered in innovative blockchain-based ecosystems, new decentralised applications, and original blockchain-based services across industries of the global economy. On

the cusp of [the fourth crypto evolution](#), more advanced projects are poised to solve industry-wide bottlenecks, while building upon prior innovation to create the next iteration of blockchain-based solutions - both physically and digitally.

Understanding the Problem

‘Garbage-In, Garbage-Out’ is a common phrase used across the blockchain industry to explain the problem of digitizing physical assets and the conditions and information collected by those assets. To date, most security solutions that utilize a blockchain rely upon standard ‘off-the-shelf’ Internet of Things (IoT) devices or manual user input to collect data that is subsequently hashed onto a blockchain. Such methods are neither efficient nor reliable especially in relation to data security. As a result, if there is an error or tampering with the datum at the point of collection, the all inputted data is useless once it has been transmitted and hashed onto its respective blockchain network.

Understanding the Solution

“Secure data, from Product to Blockchain”; Emerald Circuit embeds patented sensor technology into different types of intelligent objects, capable of securely collecting data. Using secure encryption, data can be safely transmitted to a local sidechain network and hashed onto a blockchain. In addition to standalone smart objects, Emerald Circuit integrates such objects with one another to create networks of intelligent devices capable of providing unrivalled physical data security to batches of real-world assets. By combining a fully-functional blockchain ecosystem with networked device security, data from the real world can circulate seamlessly from sensor to blockchain.

Understanding the Vision



As “The Standard for edge data security and secure IoT”; Emerald Circuit will lead the transition for sensing, intelligence and computing capabilities embedded into edge devices which currently lack robust security features. With Emerald Circuit, a strict methodology and standardization process is implemented for IoT devices, so as to set a new trajectory for how data from the edge transmits information between devices in a secure and trusted manner. Ultimately, Emerald Circuit aspires to normalize and industrially scale, how physical devices interact with clouds and IT platforms which support this specific IoT Standard.

The overall vision of the larger Emerald Circuit project is to assure secure data from Sensor to Platforms when edge devices are integrated into everyday objects and industrial processes; To Bring Intelligent Objects Into the World. Emerald Circuit intends to bring intelligent objects into mainstream business practice, by offering best in class security and trusted protocols for all relevant components under strict standards. As an early stage blockchain - IoT solution provider and product creator, Emerald Circuit will play a pivotal role in leading this Standardization process by partnering with IoT providers and world-wide leaders in the field. In the long term, Emerald Circuit will build out the base layer of fully autonomous and intelligent objects of tomorrow: Where machines and devices are able to sense, communicate, react, and alert one another in a fully decentralized and autonomous fashion.

Understanding the Fund Distribution

Unlike many other IEOs, Emerald Circuit has already developed the core products grounding the business model of the project. The Intelligent Objects across the micro (individual product) - macro (holder for multiple products) - and networked (interfacing between products) levels are all developed prototypes with patents, available for deployment and Proof of Concept testing. Meanwhile, an initial version of the Emerald Circuit sidechain built on the Ambrosus Network has already launched. As such, the development of the Emerald Circuit project is more closely aligned with building out a complete team of business, marketing, and industry experts to effectively market, standardize and scale the existing technology available, as opposed to simply developing it from scratch.

Specifically, the existing Emerald Circuit smart container, smart flask, and smart pallet prototypes described hereafter are all operational. IoT Development and innovation post IEO will focus on improving upon these core products, based upon specific industry verticals. Integrating more types of sensors, monitors and data collection capabilities over time ensures that as the market for industrial IoT continues to develop, Emerald Circuit remains on the cutting edge. This vision is deployed across different areas of development discussed in detail in *Section 4*.

Table of Contents

Section 1: The Industrial Internet of Things and Demand For Device Security	7
Overview of the IIoT market and the need for device security	
Section 2: Secure Data Flows from Endpoint to Blockchain	10
Detailed overview of Emerald Circuit and its initial solutions stack	
Section 3: The Emerald Circuit Cryptonomics	33
The Emerald token (EMR) and network integration	
Section 4: Roadmap and Project Milestones	46
Roadmap to Market, Tokensale, IEO details, Community Development Plan, Team Breakdown.	
Appendix 1: Emerald Circuit in Context: Use Cases of Emerald Circuit’s sensor-to-blockchain solutions.	53
Smart Logistics, Organ Transplants, Museum Artifacts, and Luxury Goods	
Appendix 2: Sidechain Technical Features	57
Appendix 3: Smart Box and Smart Flask Image Gallery	59
Appendix 4: Team and Advisors	67

Section 1: The Industrial Internet of Things and Demand For Device Security

The Industrial Internet of Things (IIOT) refers to the application of intelligent devices, objects, and sensors to industrial processes. To date, the majority of industrial and general IoT devices have been utilized for their unique capacity to both create and communicate data from the edge. [With over 14 billion IoT devices actively deployed](#) and an [expected increase to over 41 billion devices by 2025](#), the mainstream digitization of business processes is underway. Now, however, instead of merely creating and communicating data from the edge, IoT devices are challenged to also provide security to the data they collect and the networks they interact upon.

The industry dilemma for the future expansion and growth of the Internet of Things market is centered upon the need for secure IoT devices, and rising demand for data across facets of an organization:

The Need for Secure IoT Devices and Networks

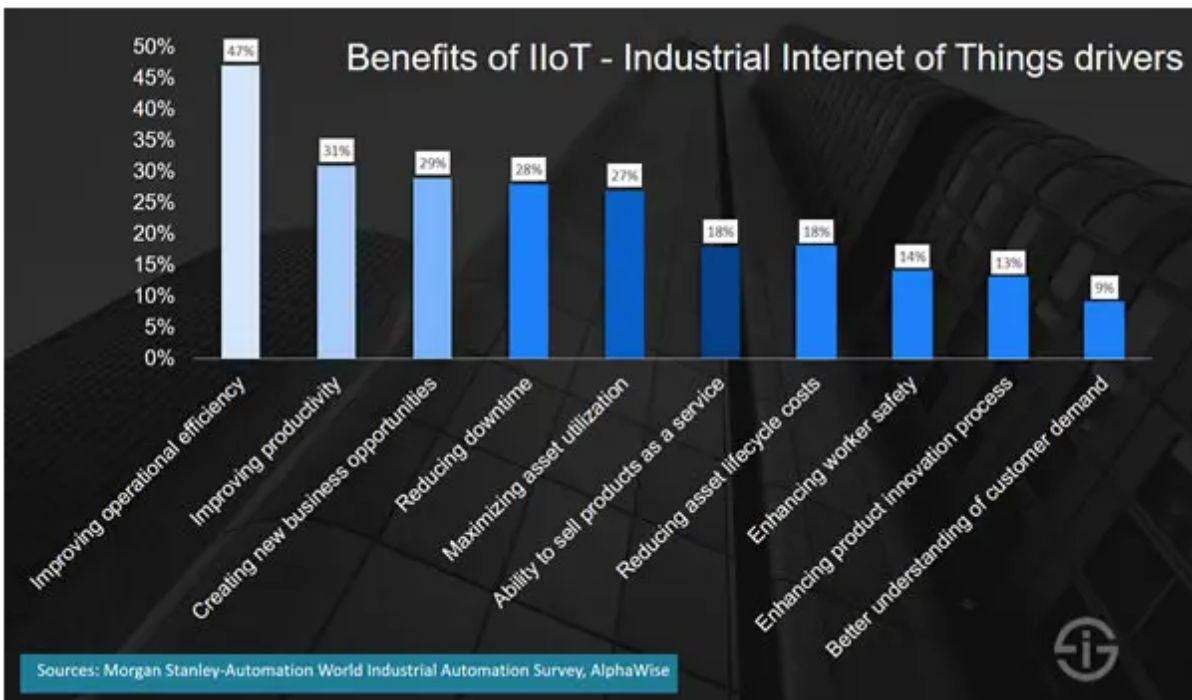
IoT Devices are at risk of counterfeiting, data hacking, identity spoofing, and the unintended modification of device components. Combined, these security challenges have exposed key vulnerabilities in the IoT market:

- Cyberattacks on IOT devices surged 300% in 2019, with an estimated 2.9 billion events observed. ([Forbes](#))
- “98 percent of all IoT device traffic is unencrypted” while “more than half of IoT devices are vulnerable to medium- or high-severity attacks, making IoT the low-hanging fruit for attackers.” ([Threat Post](#))

- IoT vulnerabilities pose legal challenges to companies operating under data protection and security regulations (GDPR). As Deloitte explains in their IoT Security report, “Thanks to the IoT, data security risks will very likely go beyond embarrassing privacy leaks to, potentially, the hacking of important public systems.” ([Safeguarding the Internet of Things](#))
- The most established economies, including the United States and the European Union, have the most to lose from lack of IoT device security, although the challenge affects most businesses around the world.

Rising Demand For IoT Data and Intelligent Logistics Networks

Across industries, and especially in the manufacturing and logistics sector, IoT sensor networks are on the rise with a predicted estimate of “152,200 IoT devices connected every minute by 2025” ([IDC Data](#)). The underlying value provided by networks of intelligent devices is primarily insight: “*To know much more about many more things, far more often.*” ([Deloitte](#))



- The global IoT security market is expected to grow from \$8.2 billion US dollars in 2018, to \$35.4 billion US dollars in 2023. With a CAGR of 33.7% during this period. ([Marketwatch](#))
- By 2021, “Industry analysts predict that spending on IoT endpoint security solutions will be more than \$630 million.” ([Deloitte](#))
- By 2026, the global connected logistics market size is projected to reach a market capitalization of USD 82.14 billion, with an average rise of 24.7% CAGR during this timeframe. ([Global News](#))



Section 2: Secure Data Flows from Endpoint to Blockchain

Emerald Circuit is a protocol-layer network of secure intelligent objects connected to a sidechain infrastructure of the Ambrosus blockchain ecosystem. From the secure management of a single product, to an intelligent container, to the networked management of smart pallets, Emerald Circuit provides secure data flows from sensor to blockchain. Building upon previous development within the Ambrosus Ecosystem, Emerald Circuit aims to provide intelligent, networked objects that can capably solve the **'garbage-in, garbage-out' problem**, while connecting physical assets with tokenized identities.

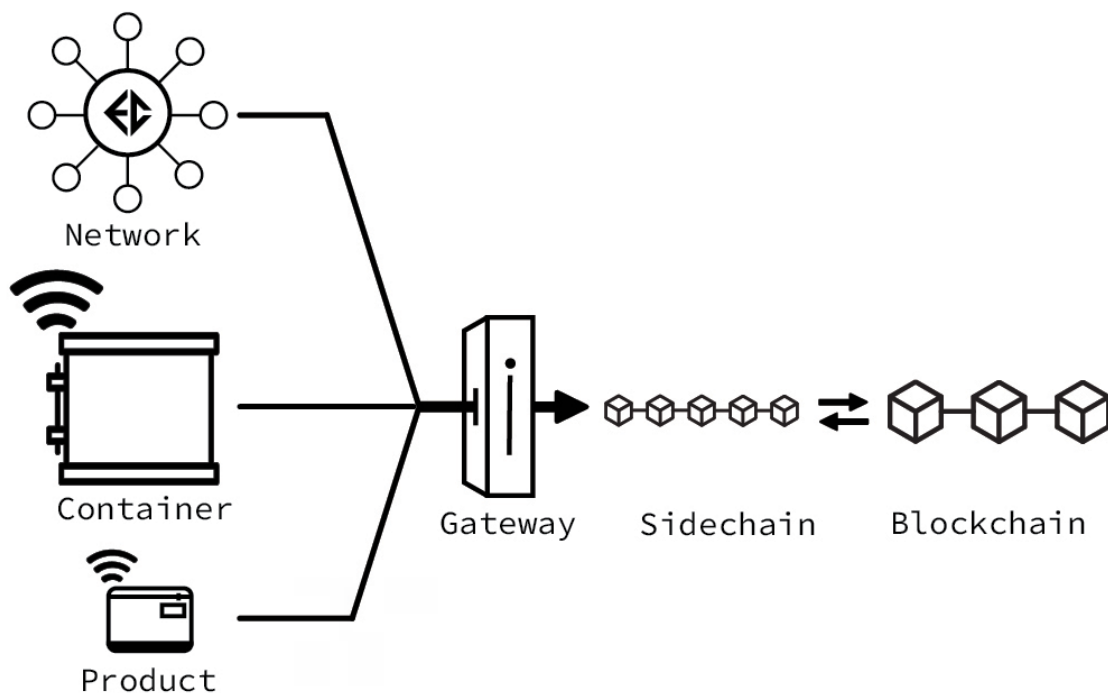


Figure 1: Data Transmission Model From Object to Blockchain

In context, the chip to cloud market for complete end-to-end security management has been described as “[nascent](#)” and “[specifically targeted](#)” for high-growth IoT markets. A complete circuit from endpoint to blockchain makes up a rising fraction of this market, while also encompassing the demands of device security in the 21st century. Together, blockchain and IoT provide secure data collection, networking, transmission, and permanent data storage: An unparalleled list of benefits that offer a previously unimaginable level of data security, anti-tampering protection, and privacy.

Secure Data Collection

Military grade encryption from edge-gateways embedded into intelligent objects means that data collected can be securely transmitted to a localized sidechain network API, with its hash being integrated into the next block in the blockchain.

Secure Networked Data

A low range transmission protocol (i.e. bluetooth) is used to share data between IoT devices. Each time data is shared (i.e. every 10 seconds), the different intelligent objects automatically create a ‘block’ of data using a Proof of Authority consensus mechanism on a sidechain network. This block of data is then automatically transmitted to a Hermes Masternode hosted by the managing party for upload to the Ambrosus blockchain.

End-to-End Data Security

Whether data is being collected by a single device or a network of interconnected smart objects, end-to-end data security is guaranteed from the moment device data is recorded, transferred to an edge gateway, through its transmission to a respective sidechain network, and until it is hashed into the next block in the blockchain.

Secure Data Integration with Stakeholders

Once data has been collected and notarized in a sidechain network, the asset identifiers and events for a particular device or gateway can be safely shared with stakeholders with transparency and proof of quality.

Tokenized-Data Management

In the future, specific products tracked or secured using intelligent objects can be individually partitioned and tokenized so as to manage and track high value assets or entire batches of product with optimal security in both physical and digital environments.

“Whenever possible, companies should err on the side of replacing legacy devices with wholly new purpose-built hardware rather than retrofitting. Failing that, developing purpose built add-ons that are outfitted with appropriate security measures may be the next best route.” ([Safeguarding the Internet of Things - Deloitte](#))

Emerald Circuit represents the initial development of fully integrated IoT-blockchain data circuits. For securing IoT devices, encrypting and hashing product data from sensor to blockchain, and creating secure digital identities for real world assets, Emerald Circuit offers new solutions to product security, anti-tampering networks, and product analytics.

The Emerald Circuit solutions selection are built upon the proprietary intellectual property of Patent no WO 2020/144527A1. At its core, this sensing device is capable of collecting data from physical entities and remotely transmitting such data in a fully secured manner: The core IP provides protections against spoofing

in the form of ID replacement, encryption key replacement, and the retransmission of older intercepted data. It equally protects against malicious and authorized attacks on devices (i.e. the modification of the time stamped data).

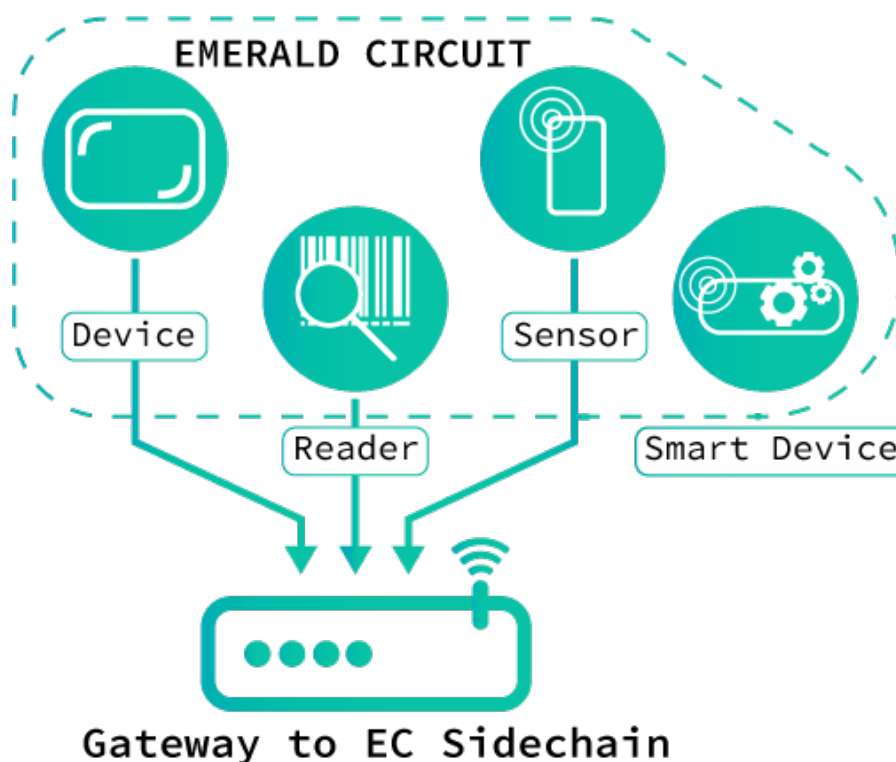


Figure 2: Object to Gateway Connectivity Within And Between Objects

The core technology is strategically incorporated into the specific business solutions Emerald Circuits offers: Fully integrated packaging, intelligent boxes, pallets and containers with additional sensors capable of collecting new and diverse data sources: To 1. Assure integrity of the container and therefore the authenticity of the product, and 2. To monitor in real-time the logistic conditions of a product, so as to assure good transportation practices.

1. Example Smart Box

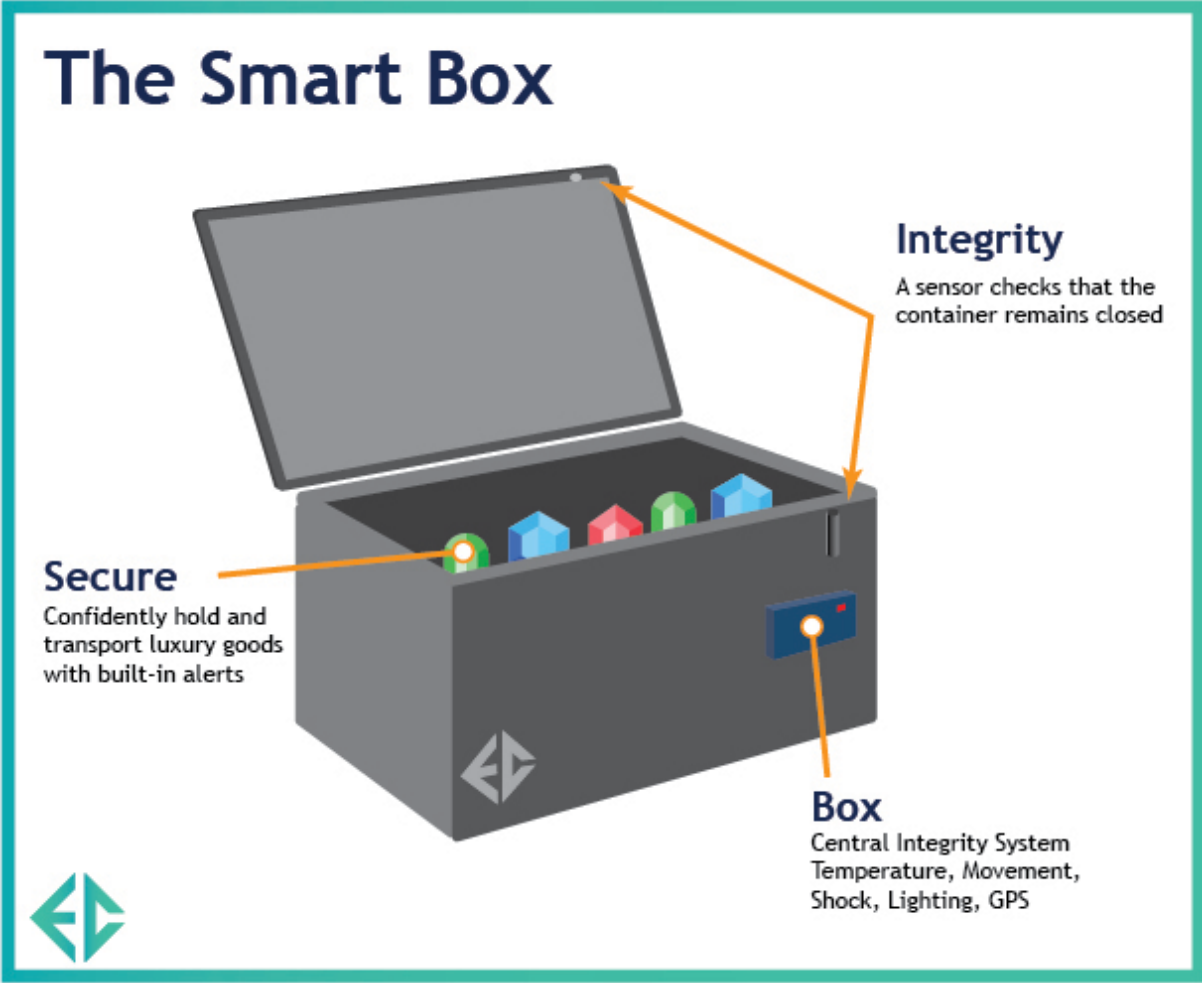


Figure 3: The Emerald Circuit Smart Box: Security, Integrity, Condition Monitoring Included



2. Example Smart Container

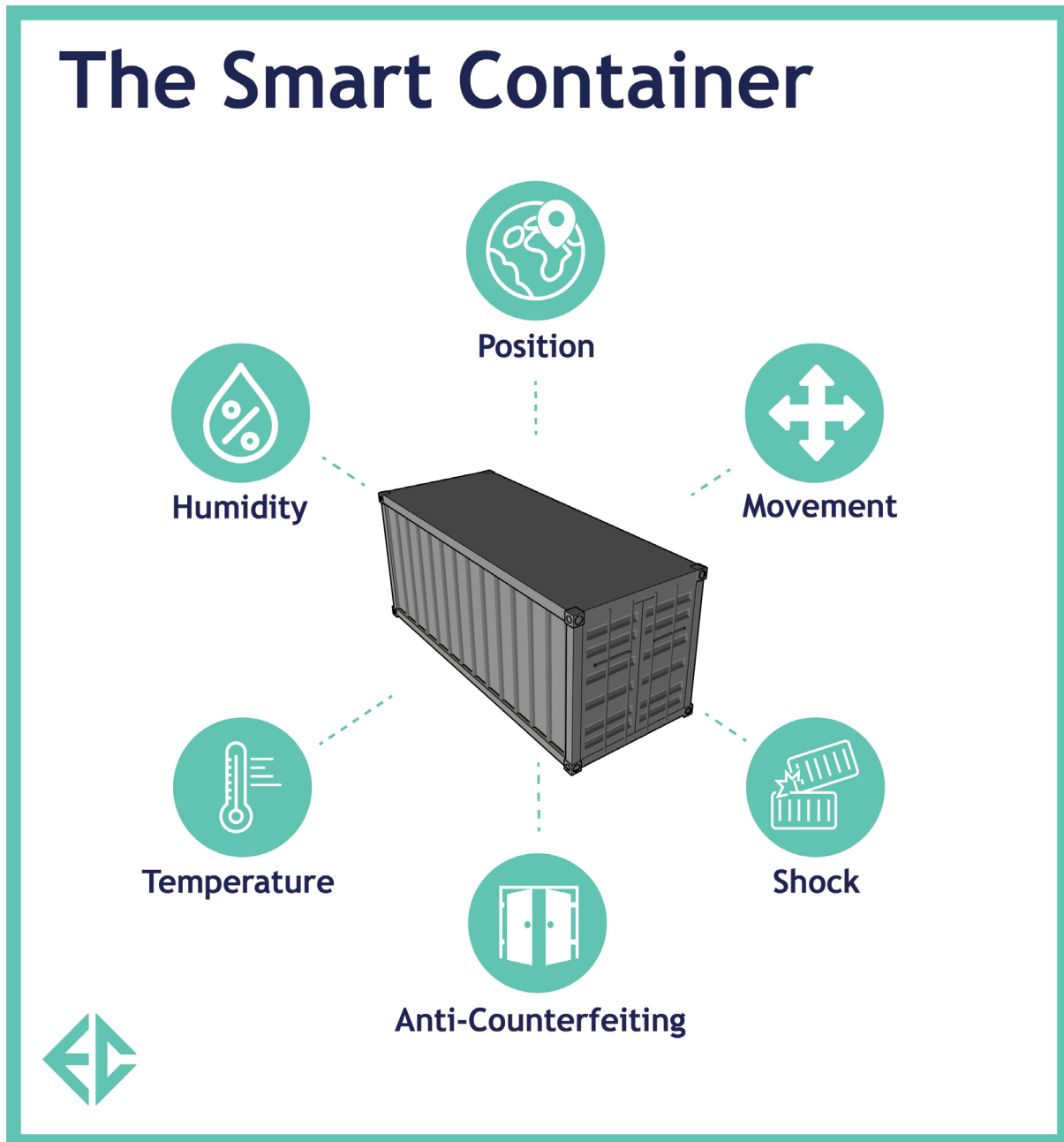


Figure 4: The Emerald Circuit Smart Container: Anti-Counterfeiting Protection for Real-Time Data Collection

The electronic gateways embedded in such solutions, equally operate in a fully secured and intelligent manner: With built-in encryption, keys management, and data transmission to the Emerald Circuit sidechain.

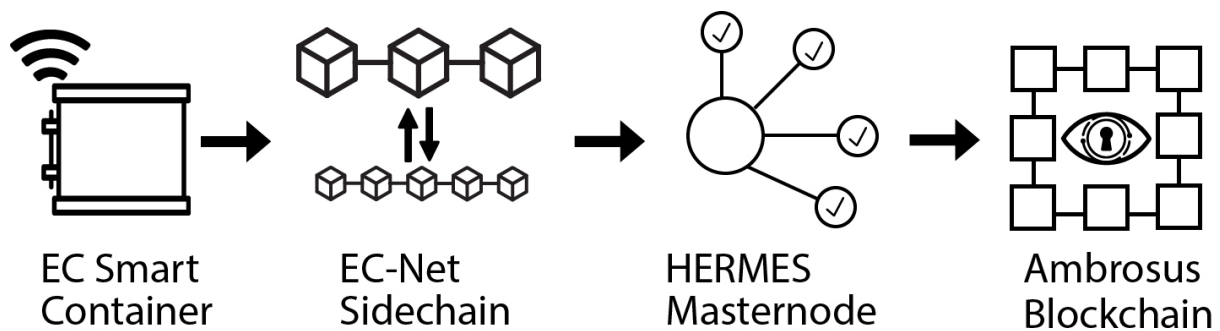


Figure 5: Data Transmission from Container to Blockchain

Section 2.1: Proprietary Intelligent Objects

In its current state, Emerald Circuit has patented, tested, and fully developed three tiers of smart and intelligent objects that can be altered or scaled for industrial implementation. These products include the Smart Container and the Smart Pallet, with the additional capacity to integrate other devices and tags into a comprehensive IoT Network. Each product is capable of operating on its own or in unison with other Emerald Circuit intelligent objects. Depending on the value proposition and specific industry, data from such products can be notarized, utilized for analytics, or even tokenized upon integration with a local sidechain network and the larger Ambrosus Network.

The Smart Container (EC-SC)

In what situation does someone need to know where their product is located as well as the conditions of that product over time and distances? Created as a comprehensive smart logistics solution, the Smart Container (EC-SC) consists of securely-integrated IoT devices with an edge-gateway capable of providing analytic tools and encryption to collected data transmitted to a sidechain network. In addition to monitoring temperature, geolocation, shock, and lighting, it is also designed to provide signed records of batch and asset identifiers with an accompanying timestamp.



Figure 6: The Emerald Circuit Smart Luxury Product Box Prototype



Figure 7: Emerald Circuit Smart Food Transportation Box Prototype

Temperature range	-15 to 60 °C ± 0,5 °C
Humidity range	0 to 100 %RH ± 1 %RH
Light range	0 to 100,000 Lux
Acceleration range	16 g
Positioning	WiFi (or through 3G when connected to a gateway)
Communication protocol	Bluetooth Low Energy (BLE) or WiFi (or through 3G when connected to a gateway)
Log capacity	Up to 10,000 samples
Sampling frequency	Customizable, from 1/sec to 1/day
Weight (per casing type)	A: 50g – B: 75g – C & D: standard pallet weight + 200g – E: 150g
CE Certification	2014/30/EU - 2014/35/EU - Radio Emitting certification: 2014/53/EU
Evaluation Assurance Level	EAL4
Sensor Certification	Humidity / Temperature certified NIST

Unlike many existing smart containers which provide a single monitoring variable, the Emerald Circuit Smart Container has been robustly designed to simultaneously prevent different forms of tampering with a product. Each smart container provides a number of added benefits for logistics management and asset identification:

- Easy Setup:** A smart container is quickly and easily operational with visibility provided through using the EC-SC Mobile App. The app provides built in functionality for managing individual smart containers, as well as larger batches of containers all at once. In the event of tampering or container misappropriation, the application provides an instant notification to the user, specifying the exact asset, time, and location. Users can trigger SMS and email alarms on its own before each shipment.
- Data Recording:** For managing large amounts of data, the Smart Container is capable of processing up to 10,000 data entries, with a sampling frequency

customizable from one second to one day.

- **Secure By Design:** Each Smart Container is equipped with data analysis capabilities: they possess the computational ability to preselect or store data collected from the entry module. Upon further transmission data is encrypted and communicated to its respective side chain network. From the moment data is collected to the moment it is transmitted to the cloud, there is complete security for all of the data entries.
- **Simple Data Recovery:** For operators managing data from the cloud, a Smart Container can be customized to communicate data to a cloud/sidechain network through various encrypted protocols and Mesh networks, including: Wi-Fi, 4G or 5G, NB-IOT, LoRa, and Bluetooth. Through such protocols, data can be reliably received in real-time or once the container has re-established internet connectivity.

The Smart Pallet (EC-SP)

In what situation do stakeholders require insight into the status and movements of multiple products and shipments at the same time? The Emerald Circuit Smart Pallet (EC-SP) is an intelligent and networked pallet that has the ability to detect and automatically provide information about its contents and the environment in which it is located. While a normal pallet is a foundation from which products can be transported or stored, a smart-pallet integrates sensing devices into different products on top of the pallet, or inside of transportation containers containing intelligent pallets. It is capable of monitoring and transmitting data about such networked products, including their whereabouts, as well as their real-time temperature and humidity levels.

The EC-SP represents the next level of product innovation for industrial logistics. The core benefits it provides for logistics solutions include:

- **Product Condition Monitoring:** Measurement of temperature, humidity and shock, inside of the packages placed upon the smart pallet.
- **Anti-Counterfeiting Protection:** Geolocation and verification of the status of all of the products connected to it; insight into whether any products have been opened or tampered with unexpectedly.
- **Communication Alert Networks:** To communicate with other-smart pallets or IoT gateways and automatically send alerts to systems managers or other IT systems in the event of an unforeseen problem.

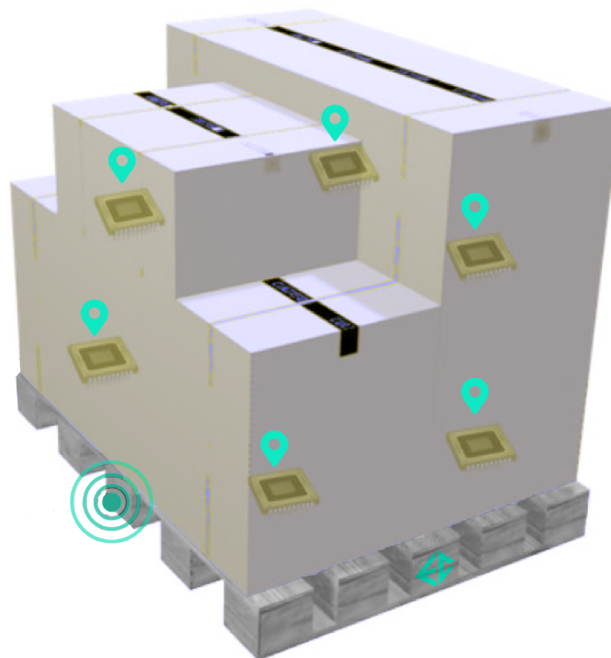


Figure 8: Sample Smart Pallet Interconnected with Intelligent Objects and Tags on Boxes

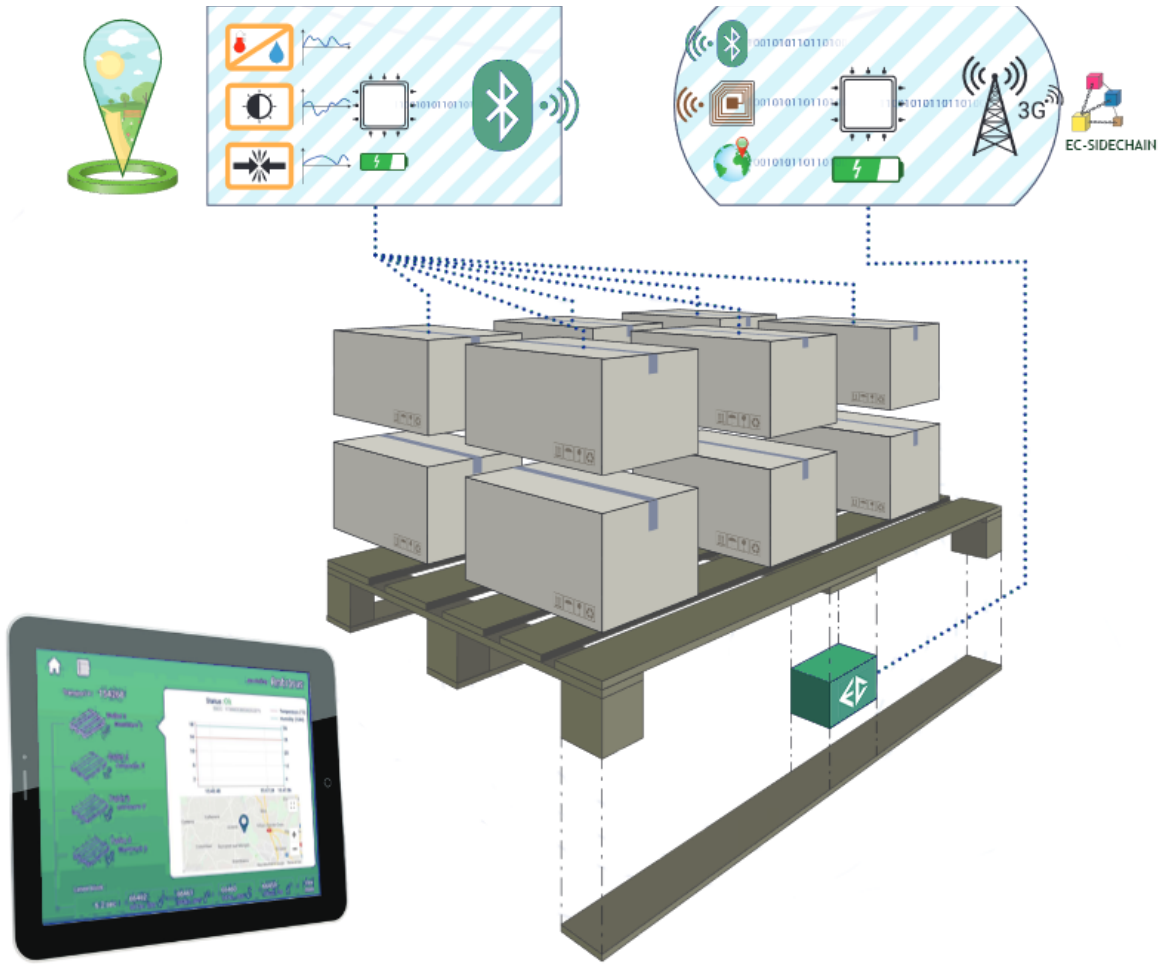
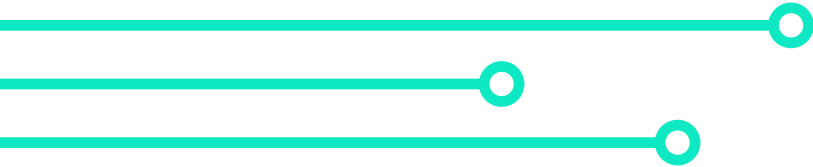


Figure 9: The Emerald Circuit Smart Pallet design and technical specifications



The Smart Pallet in Practice

Combating Fraud and Product Substitution

Sensors or tags attached to both the pallet and the objects placed on top of the pallet send signals to the embedded gateway if a particular product has moved position or been opened. This signal is then stored on a local sidechain network in such a manner that the record cannot be tampered with from the point of collection. Additional geolocation capabilities ensure that a shipment never goes missing, or, that the actors involved can be quickly identified according to the sensor readings.

Serialization and Monitoring of High Value Products

For high value products requiring specific identifiers, tags are applied to individually serialize each item. These tags then communicate with the intelligent pallet for the duration of its journey to ensure that the relevant variables for each item are maintained. This data trail, also immutably recorded on the local sidechain network and the Ambrosus blockchain, can then be displayed to any relevant third party or stakeholder in real-time.

The Advantages of Leveraging the EC-SP

- Constant Connectivity to Tags and Sensors Placed on the Products itself.
- Real-Time Temperature and Humidity monitoring.
- Alerts sent within 5 seconds to logistic operators.
- Automatic data collection and transmission to the sidechain blockchain network.
- Geolocation and unique serialization of each product.

The Smart Flask (EC-SF)



In what situation does someone need to prove that a product, liquid, or chemical, being managed has not been opened or tampered with? This is the fundamental question that guides the creation of the Smart Flask (EC-SF). Designed to be integrated into the product itself, the Emerald Circuit Smart Flask is capable of monitoring temperature while also providing inbuilt anti-counterfeiting features. Such a product is used to secure individual assets, or for entire batches of high value assets that require real-time temperature verification and anti-counterfeiting.

The Emerald Circuit smart flask, also known as an *anti-doping flask*, is useful for storing liquids, medicines, chemicals, and biomaterials in any container in a completely secure manner. With in-built sensing and communications capacities, the smart flask is able to monitor, detect, and communicate tampering of products in real-time and in diverse environments. From product alerts surrounding custom parameters, to personal notifications of product damage and counterfeiting, the Smart Flask is widely applicable to industries and interest groups looking for a safe and secure way of transporting their liquids.

The mechanical and electronic placement is strategically positioned on the inside of the lid cover, with the anti-tampering feature located inside of the body of the flask itself.



Figure 10: Smart Flask Prototype

Data Collection and Monitoring

When the cover of the flask is closed and sealed on top of it, the mechanics of the lid will switch on the anti-counterfeiting loop with a 'click'. As a result the sensor and the electronic are also switched on and prepared to continuously collect data surrounding the flask itself. This data includes temperature, humidity, light exposure, and shock. As a holistic guarantee of the flask's integrity, the anti-tampering loop and collected data can consistently monitor the environment and collect data at all times the device is activated.

Data Transmission

Data can be automatically communicated to the Emerald Circuit sidechain using a variety of communication protocols. From long range protocols like 4G to short range protocols such as NB-IoT (to a gateway or sensor network). Upon transmission data is either collected by a central gateway, an Emerald Circuit object network, or sent directly to the Emerald Circuit sidechain, from which proof of security is stored, and logged data is hashed onto the Ambrosus blockchain.



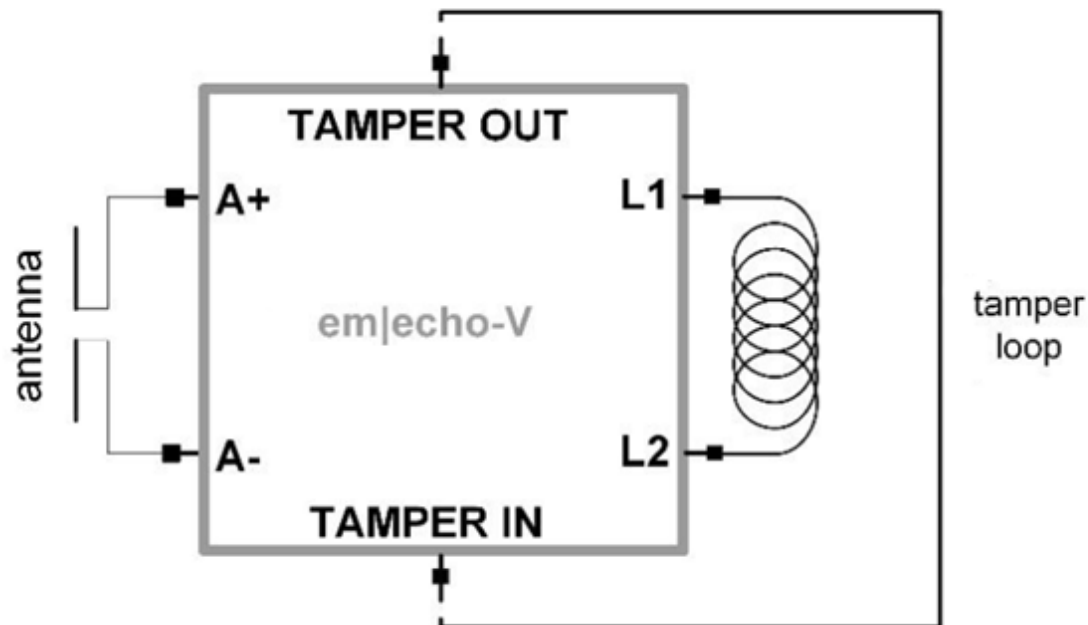


Figure 11: Diagram of Tamper Chip Embedded in Smart Flask

Embedded Sensor of EC Board Base

The sensing system embedded on the board base consists of four sensors as well as security integration features. These sensors are capable of recording data surrounding Temperature (T), Humidity (H), Light Exposure (L) and Shocks (S). The EC electronic base is capable of securely connecting four sensors in total. Additional sensing parameters are therefore capable of being integrated in place of these four. This provides flexibility to the product design, and freedom on behalf of the client in customizing their parameters. As such, any one of these sensors can be substituted for a more robust anti-tampering sensor, or for product packaging authenticity.

The benefit of this technological design is predicated upon the balance of electronics and security: The base is able to remain nimble, and minimally connected with only four sensors, while also robust enough to provide full functionality and security

(Including 128-Bit encryption). In addition, all data is continuously collected with an inbuilt and immediate alarm system in the event of breakdown or product tampering.

In combination with the Anti-Tampering loop chip, the Board Base fully assures the physical integrity of the product, the security of all data collected, and the safety of all data transmitted from a physical environment, through a hardware application, and onto the cloud and sidechain/blockchain state.

The Anti-tampering Loop

The anti-tampering loop is an electronically integrated circuit based on CMOS technology that includes a UHF/NFC tag and anti-tampering loop architecture. The Tamperloop possesses the following characteristics:

- 12.5mF Capacitance
- 40nH Inductance Between Tamper Pads
- 10MΩ Resistance
- 47pF Capacitance between Tamper IN and OUT to assure an open-loop

In the technical design of the larger Smart Flask, the Tamperloop is embedded onto an EC Board Base.

The following product designs are a result of the combination of both anti-tampering features (Base Board and Anti-Tampering Loop) integrated inside of a single flask:

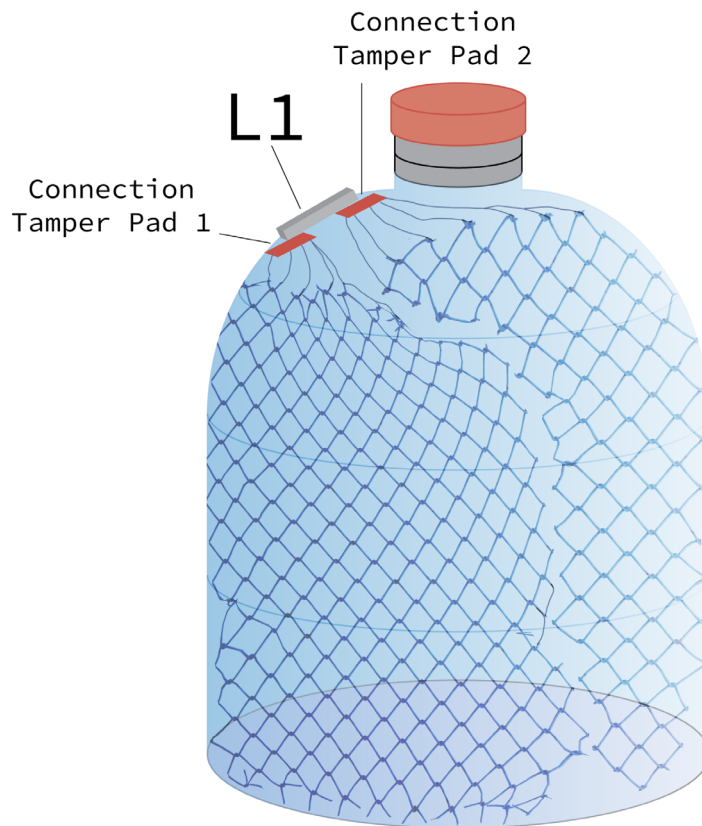


Figure 12: Diagram of the Emerald Circuit Smart Flask - Embedded electronics and mesh microwires assure flask integrity from product penetration and premature extraction of contents contained within.

Real-Time Arrival and Resetting

Upon arrival to its final location, the cover of the smart flask can be opened. If the flask is opened prematurely, before arrival in its final location (i.e. it is tampered with before reaching a lab) an alarm is generated with a specific time and violated parameters. This proof of tampering is further sent to the sidechain. Upon safely reaching its final destination, the Smart Flask indicates via Web Application the date, time, and location from which its measurement started.

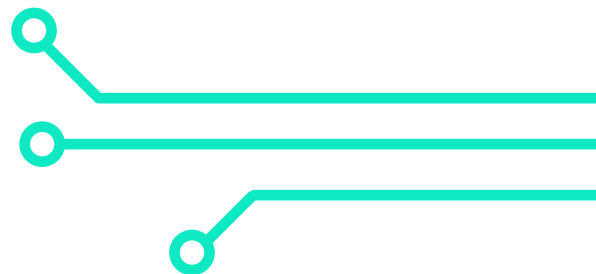
2.2 Distributed IoT Networks on the Edge



The three primary intelligent objects developed by Emerald Circuit, are each capable of being integrated into different networks of intelligent devices, containers, and pallets, so as to offer holistic logistics management and end-to-end data security as required by a given situation.

Notably, each smart object can also be converted into a validator of a physical proof of authority consensus mechanism maintained through each intelligent device connected to the local network of intelligent objects: A low range (i.e. bluetooth) transmission protocol is used to share data between intelligent objects. Each time data is shared (i.e. every 10 seconds), the different smart-pallets automatically create a 'block' of data using a Proof of Authority consensus mechanism. This block of data is then automatically transmitted to a Hermes Masternode hosted by the managing party and subsequently stored on a local sidechain network. From the Hermes Masternode, operators are capable of accessing the history of all of the data from the various pallets, which can be managed and utilized through a specific application.

Applicable to warehouses, storage units, and supply chains, a smart-pallet or smart container network provides enterprises with the opportunity to possess real-time insights into the location, conditions, history, and security of all monitored products - from each individual asset, to batches of assets, to entire shipments of assets.



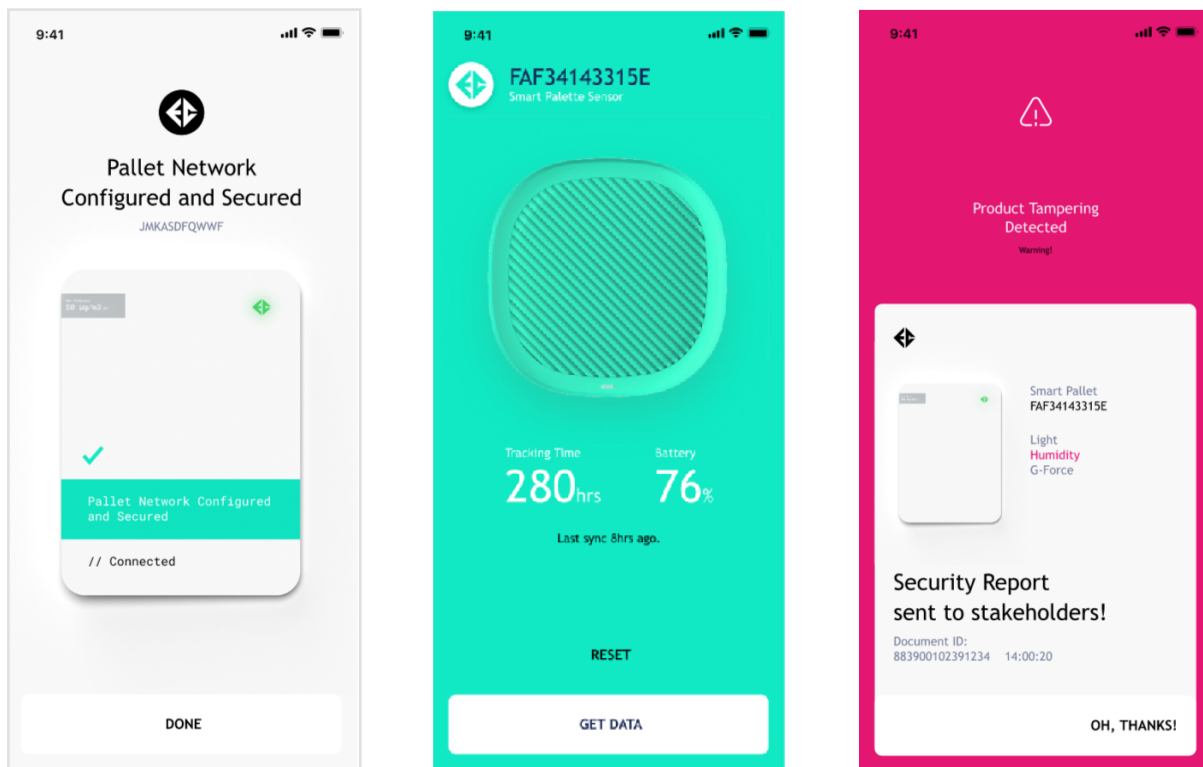


Figure 13: Prototype mobile app screens

Cost-Effective IoT Networks

The entire sidechain infrastructure for smart-pallets can be stopped and ‘rebooted’ when a specific set of smart pallets or containers has completed their objective or journey. More specifically, the collected data can be reset so the pallet can be used for its next journey. Another physical sidechain can then commence when the pallets are required once again. This design allows smart pallets to be recycled for different purposes and for the management of different products: Once sufficient data has been collected from a particular logistics process, all final data is sent to a local sidechain network and the main Ambrosus blockchain. All pallets are then reset and re-configured according to new settings, for a different purpose. In this manner, the costs of a sidechain network can be considered over an extended duration of time and across multiple production lines. Management of deleting, resetting, and re-configuring a particular set of pallets or containers, is done seamlessly through a web application.

Section 2.3: Sidechain Integration and AMB-NET

When data is collected by an intelligent object, it is directly transmitted to a local sidechain network. For asset identification or event data notarization, this information is subsequently integrated with a Hermes Masternode on the Ambrosus Network, and then hashed on to the Ambrosus Blockchain. With such a design, the local sidechain network and the Ambrosus Network are at the end of each circuit of data flows to ensure local data authenticity and compliance, and immutable data storage, respectively.

Sidechains

A sidechain is a separate blockchain network that operates in parallel to a main blockchain network. While a sidechain can be privately managed, in accordance with specific local data regulations of different stakeholders, it must be tied to the main network with some form of interoperability between the two. Importantly, a sidechain does not need to be configured in the same manner as a main network: it may be a different network altogether that still interacts with the main network.

In the case of Emerald Circuit, local sidechains that are deployed to host data collected from intelligent objects, serve the purpose of guaranteeing data privacy and authenticity through the 'Emerald' token (EMR), in line with local regulations. Data notarization and management is complemented by the Ambrosus Network, when private sidechain data is transmitted to Hermes Masternodes, and bundled onto the Ambrosus Blockchain via 'Amber' (AMB). Together, the two tokens guarantee the two most essential parts of an integrated data circuit: secure data collection (Emerald Token), and secure data management (Amber).

Sidechain Technicalities: Nodes, Data, and Hash Structure

The Emerald Circuit network consists of nodes, each of them comprising two main components: (1) A blockchain validator and (2) A distributed data storage node.

IoT data is recorded in distributed storage. Distributed storage, in turn, maintains blocks of data. Contained within each block is a hash which allocates an address to each particular block. In such a manner, one can always be sure that the requested data has not been changed. At any point in time, data can be requested from any node from distributed storage. All the nodes are connected to the network, so that any node can resolve block data requests, in case the initially requested node does not hold the particular block. Ultimately, distributed storage ensures that data is stored not only in one node, but is copied to other nodes respectively.

The hash that validates the data is recorded on the Ambrosus blockchain. Blockchain validators are linked in a peer-to-peer network for data exchange. Validators establish a consensus among themselves determining their order of blocks validation. With each validator authorised to join the network, the security of the blockchain is guaranteed through the behavior of the operators.

Intelligent Object Data Structure

All IoT Device data consists of Objects and Actions. Objects store information about an IoT device, its creation date, and other metadata. Actions refer to what happens to the Object such as sensing information about a physical environment like temperature or pressure, the opening of a container, the changing or adding of data about the Object, or ending the life cycle of the Object.

Notably, every Object possesses an Asset ID which is a hash of all its data when it's created. This ID is used as an identifier for each Object. Every Action meanwhile, is categorized as a separate immutable data entry in distributed storage and contains within its datum the Object ID that the action refers to. In this manner, all data in the distributed storage is encrypted with asymmetric algorithms.

In tandem with each Object and its accompanying Actions, an Index entity is also created in distributed storage. This Index Entity contains hashes of the Object and its related Actions. The Index hash is recorded on the blockchain by the Object creator only with a smart contract.

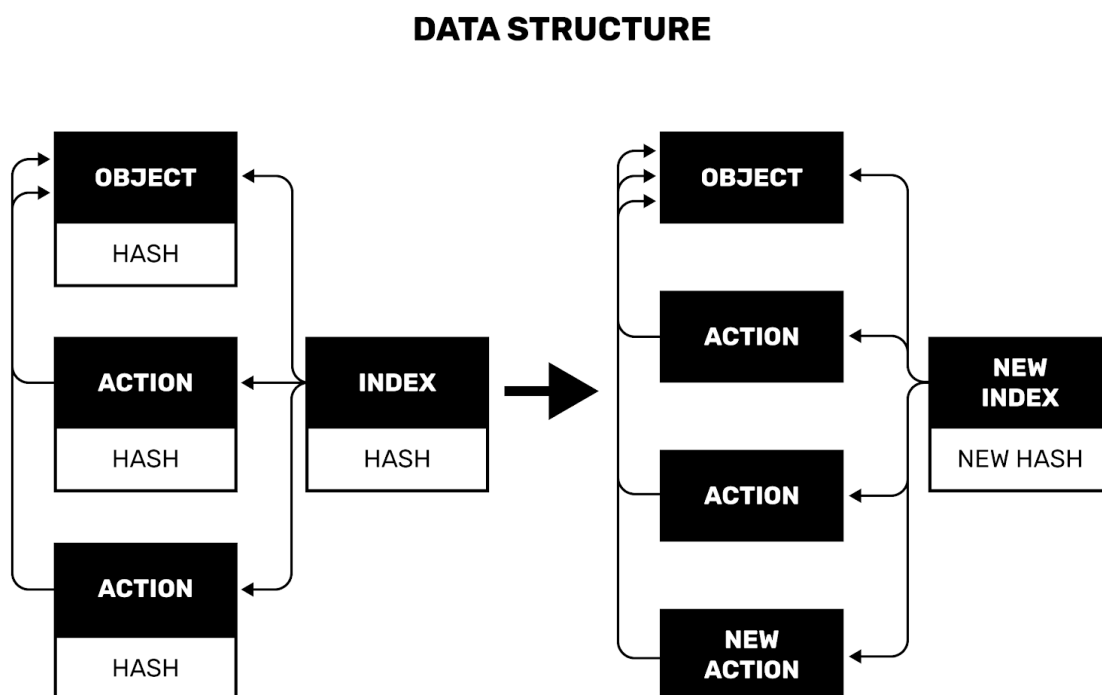


Figure 14: Object / Action data structure on the Emerald Circuit sidechain

Section 3: The Emerald Circuit Cryptonomics

Section 3.1: The Emerald Circuit sidechain & the Emerald Token

Emerald Circuit is a sidechain protocol integrated with the Ambrosus Network (AMB-NET). As a sidechain, Emerald Circuit receives and transmits data according to its own proof of authority consensus mechanism, as well as through its own native token. The hash of each sidechain transaction is integrated into the Ambrosus network, and ultimately hashed onto the Ambrosus blockchain - AMB-NET. The benefits of managing data on a separate sidechain are that: 1) The Ambrosus Network is not overloaded with transactions, 2) transactions can be localized on the Emerald Circuit sidechain for regulatory and data protection purposes, and 3) the unique advantages of the Emerald Circuit cryptonomic model (i.e. commission fee) can be imbued through the Emerald token and disbursed to Emerald Circuit node operators for the services they provide to the sidechain network.

3.1.1 The Emerald Token (EMR)

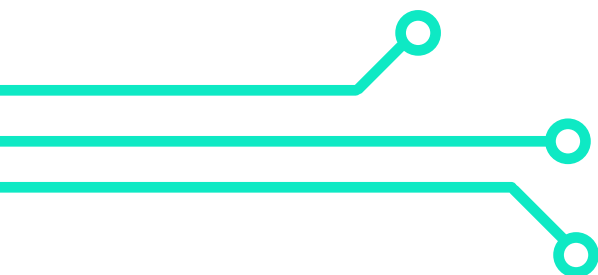
The Emerald Token is a fixed stable coin pegged to the US Dollar on the Emerald Circuit side chain. Such a token is directly tied to the data sent from proprietary IoT Devices also referred to as 'intelligent objects'. The logic behind the cryptonomic design of the Emerald Token is straightforward: Enterprises require stability in purchasing and managing software and data. Node operators are rewarded for validating transactions of this data. As more transactions are sent across the network, more transaction fees are dispersed to the relevant node operators increasing the incentive to operate a node on the network.

Through such a design, enterprises are able to seamlessly pay (on a subscription basis) for software and blockchain services in a manner that can be directly translated into a token-based model for securing distributed network data. In a similar fashion, third party consultants or other entrepreneurs wishing to integrate Emerald Circuit IoT devices with their own solutions can easily do so without price fluctuations or exchange difficulties.

The Emerald Circuit Token

Type of Token	Utility Token
Token Name	Emerald Token (EMR)
Total Supply	14,000,000 EMR
Subunit of Token	Embers

Additionally, a built in ‘commission’ fee for the sale of the physical hardware devices, is also factored into the transaction fee rewards for Emerald node operators (See section 3.5 *Commission Fee*).



Section 3.2: Data Flows and Cryptonomic Dynamics

In every public blockchain ecosystem, an accompanying cryptonomic design must balance three primary considerations: speed, security, and scalability - also known as the blockchain trilemma. For the Emerald Circuit Sidechain in particular, these three considerations must be adequately applied to the management and security of IoT device data as it is collected and hashed onto the chain.

Scalability

Emerald Circuit is able to address the challenge of scalability through utilizing Hermes Masternodes to bundle and hash asset and event sensor data, at a rate of 16,384 readings per bundle. With all data eventually being hashed onto the main Ambrosus blockchain - after first passing through the Emerald Circuit Sidechain - the model is capable of scaling to the point of managing hundreds of thousands of sensor readings per second.

Speed

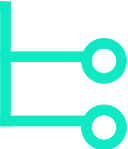
Sensor data is frequently collected at intervals measured in seconds or minutes. As such any sidechain or blockchain will need to guarantee that data can be stored quickly and efficiently without delays or long transaction periods. To do this, Emerald Circuit is able to quickly achieve consensus on the side chain, among a number of node operators according to a proof of authority consensus mechanism in which validators are selected based upon their commitment to the security of the network and the stake they are willing to lock into the network.

Security

A secure sidechain must process transactions from a distributed network of (self-interested) validators. Using game-theory dynamics the security of a sidechain must be designed in a manner such that network validators are not incentivized to corrupt

or falsely validate transactions. As a result, sidechain security is closely connected to the cryptonomic design and incentive structure built into the network. Emerald Circuit's sidechain security is achieved through rewarding validators according to their uptime on the network, and their stake in the sidechain system.

Emerald Circuit's cryptonomic model is built upon a Proof of Authority consensus algorithm, designed to securely and scalably manage data flows from endpoint IoT devices. In essence, the system is controlled by two key parameters:

- 
- The Flow of Data Onto the Network.
 - Cryptonomic Incentives for Validators to Maintain Consensus on the Network.

Data flows refer to the collection of data onto the Emerald Circuit sidechain from intelligent objects. Specifically, device data is the 'lifeline' or 'blood' of the sidechain as users and stakeholders will utilize the 'Emerald' token (EMR) to digitally value and manage their data. As more devices collect and transmit real-time information onto the sidechain, the more activity, incentive, and value is created on the sidechain network.

Cryptonomic incentives for network validators refer to the token-rewards generated from maintaining the state of the network. The incentive structure built around the Emerald token, is discussed in further detail in Section 4 - *Emerald Token Cryptonomics*. The proposed system is a middle-ground solution for accommodating enterprise needs, long-term growth of the ecosystem, as well as network security.

Section 3.3: Proof of Authority Consensus

The Emerald Circuit sidechain mirrors the Ambrosus blockchain in operating according to a Proof of Authority consensus mechanism. A single tier of authority nodes are utilized to secure the Emerald Circuit Sidechain:

Jade Validators	Requiring a stake of 2,000 EMRs or more
Silicon Validators	Requiring a stake of 10,000 EMRs or more

Following Ethereum's [Aura-Authority Round Consensus Algorithm](#), finality is established among consenting operators based upon a simple majority vote. Malicious node operators can therefore not finalize a block unless they are able to operate in unison, more than a majority of nodes on the network. Using a *Forced-Sealing* command, blocks are produced as soon as the network is launched regardless of transaction load. This ensures that blocks reach finality in a timely fashion.

Silicon and Jade validators lock up Emerald Tokens (EMRs) on the Emerald Circuit sidechain as a placement of stake in the longevity of the network. When achieving finality, node operators validate transactions and maintain the state of the network, from which they are entitled to receive a *CoinBase Reward* in proportion to their stake.

As a public permissionless sidechain, Emerald Circuit is therefore structured similar to the Ambrosus Blockchain. Consensus is achieved from a set of authoritative actors who have a vested interest in the maintenance of the network. Malicious behavior is curtailed and malicious nodes are penalized through the loss of their stake on the network. Finality is achieved in a round-robin fashion with each operator validating the next block on the chain.

Section 3.4: Emerald Token Cryptonomics

The cryptonomic design built around the Emerald token must consider three primary factors:

1. The security and efficiency of the network.
2. The commercial incentives for utilizing the network.
3. The validator incentives for securing the network

To create a robust sidechain infrastructure that will someday manage millions of IoT Device readings every hour, Emerald Circuit's cryptonomic model - built around the Emerald Token (EMR) - is grounded in the following design:

Coinbase Reward

Following the design of other blockchain ecosystems, Emerald Circuit's cryptonomic design ensures consistency of gas fees for commercial usage purposes, while also incentivizing validators to maintain state security. Of the initial circulating supply, the network protocol will issue 10% new tokens of the existing circulating supply on an annual basis, of which 90% will be diffused to network validators for securing the network in proportion to their stake in the network. 10% is then maintained as a protocol treasury for the growth of the Emerald Circuit sidechain development.

Utility Token for Anti-Counterfeiting Services

For commercial purposes, the Emerald Circuit sidechain utility token - known as the *Emerald token (EMR)* - will be issued at a price of \$1.00 USD per token as a utility token used to designate anti-counterfeiting data security on the Emerald Circuit sidechain. For commercial SMEs (Small and Medium Sized Businesses) anti-counterfeiting data

managed on the Emerald Circuit sidechain will be offered according to a Software as a Service model (SaaS) in which enterprises pay a fixed price of USD in EMR for the tracking of their devices security. This service will be offered alongside blockchain as a service (BaaS) costs paid in Amber.

Intelligent Object Licensing

The licensing model for intelligent objects is built around sending data to the Emerald Circuit sidechain and ultimately the Ambrosus blockchain. While the objects are first bought for a fixed price in US Dollars paid in EMR, a software license of five dollars per intelligent object (calculated as a single total per order) is charged on a monthly basis. Payment of such a license is directly pushed into EMR tokens on the Emerald Circuit sidechain. A sensor operating area, similar to the Ambrosus masternode operating area, will be built in order to allow network validators to visualize the current state of usage and different types of sensors on the network.

Protocol Treasury of 20% per annum to bolster Ecosystem Growth and Development

Last but not least, the Emerald Circuit Foundation has created a protocol treasury of 25% of the annual Coinbase reward tokens. These tokens will be allocated for the development of the Emerald Circuit ecosystem: for community bounties and growth opportunities, for entrepreneurs building specific industry verticals leveraging an Emerald Circuit intelligent object, for pitches and presentations, and for dApp development that facilitates ease of access for commercial enterprises.

Section 3.5: Integration with AMB-NET

To ensure the security of the Emerald Circuit network, the hash of each block along with the address of the validator that created it, is added to the bundle of a special Hermes node in the AMB-NET. A separate validator on the side of the Hermes node validates that the hashes match the real hashes in the Emerald Circuit blockchain. The AMB-NET ensures safety of this data due to the distributed and reliable storage of bundles on Atlas nodes. In case of the bundle loss on the Hermes node, it can be restored from the copy stored on the Atlas node.

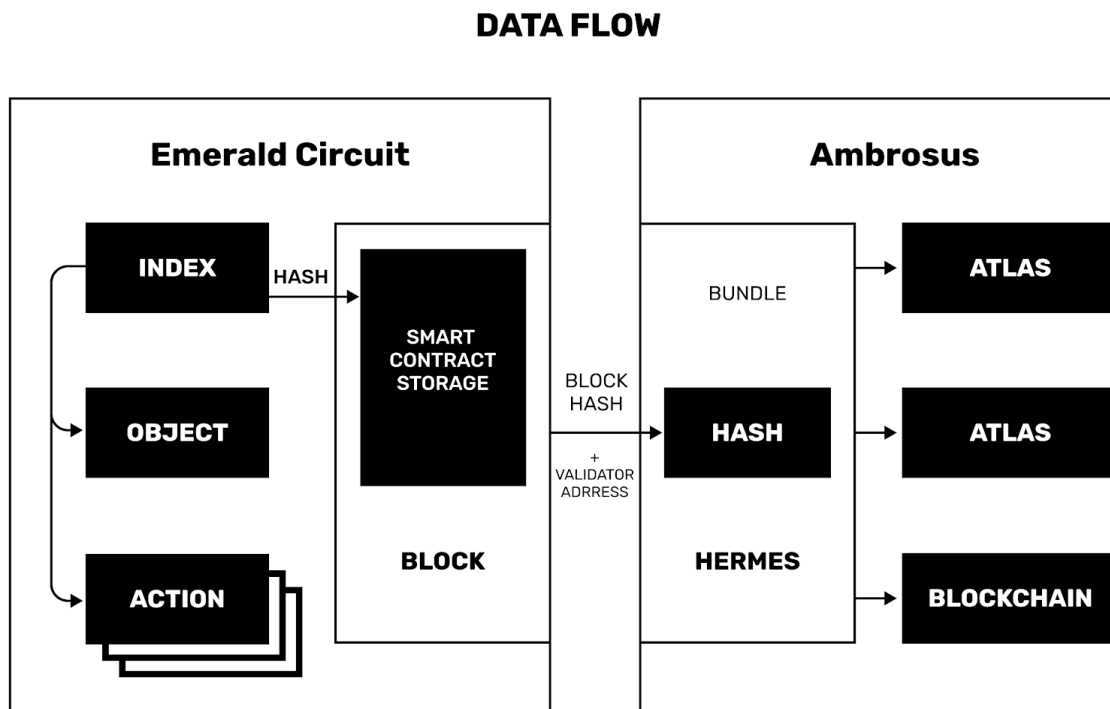


Figure 15: Sidechain to blockchain data flows

Section 3.5.1: Data flows from sensor to blockchain

Data flows from the end-point of an intelligent object are either networked through a physical gateway before being directly sent to the Emerald Circuit sidechain, or simply sent straight from sensor to sidechain. Depending on enterprise preferences, this data can be sent to a custom ERP or private database in unison with its transmission to the Emerald Circuit sidechain. Upon arrival on the sidechain, data is validated and a hash is recorded by Emerald Circuit node operators. The data of the IoT devices is then sent on to the Ambrosus network from which a bundle of the data is stored by Ambrosus masternode operators.

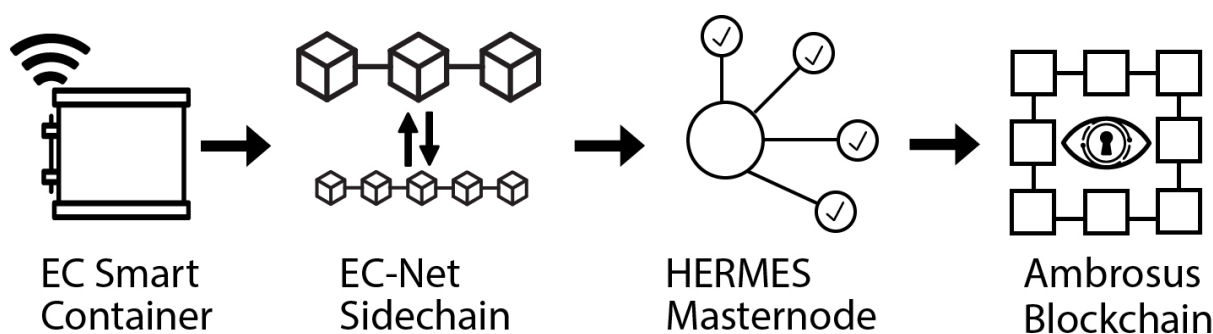


Figure 16: Data flow from sensor to blockchain

The transfer of value for the security of the data mirrors the flow of the data through the sidechain and onto the Ambrosus blockchain: Using a licensing model, enterprises pay for their data security and storage directly to the Emerald Circuit sidechain. As EMR is a fixed stable coin, enterprises are guaranteed a direct exchange rate without worry of volatility. Upon payment, data is hashed onto the Emerald Circuit sidechain: 85% of transaction fees on the sidechain are then burned, with the remaining 15% being sent with the data to the Ambrosus Network for data storage purposes.

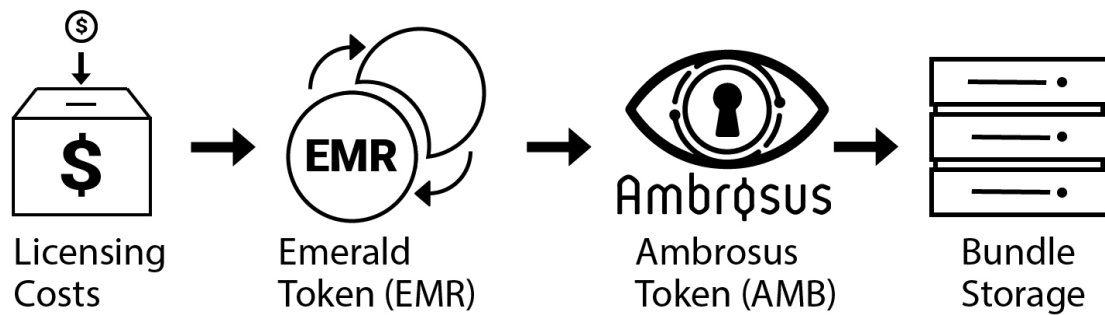
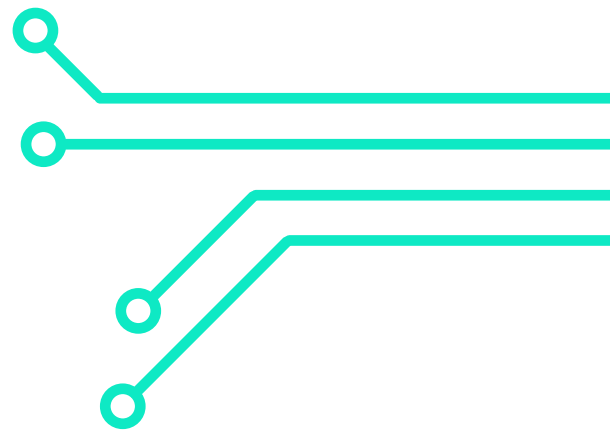


Figure 17: Cryptonomic data flows from license to storage

As a utility token, EMR is used to pay for data authentication and IoT storage on the Emerald Circuit sidechain, and for ultimately covering transaction and storage costs on the main Ambrosus blockchain. In operating as a sidechain, IoT device data can still be authenticated without clogging the Ambrosus network over time, while data storage and its accompanying benefits can still be sent to the Ambrosus blockchain and stored by Ambrosus node operators. Both the larger Ambrosus ecosystem, and the Emerald Circuit sidechain can therefore grow in a mutually beneficial fashion.



Section 3.6: IEO Tokensale Details

The Emerald Circuit IEO will run in Quarter 1 of 2021. A total of 7,000,000 (seven million) EMR's will be issued for the public offering. During the first round offering the first two million EMRs will be offered for a 20% discount for \$0.80 cents on the dollar. The remaining five million EMRs will be offered at a 10% discount from its price point of \$1.00 USD. The total hardcap of the Initial Exchange Offering will cap out at 7,000,000 EMRs in the token sale.

Token Name	Emerald Token (EMR)
Token Price	\$1.00
Round 1 Sale	2 million EMRs at 20% discount = \$1,600,000 Soft Cap
Round 2 Sale	5 million EMRs at 10% discount = \$4,500,000 Main Sale
Hard Cap	7 million EMR for total valuation of \$6,100,000 USD Hard Cap

Management of IEO Funds

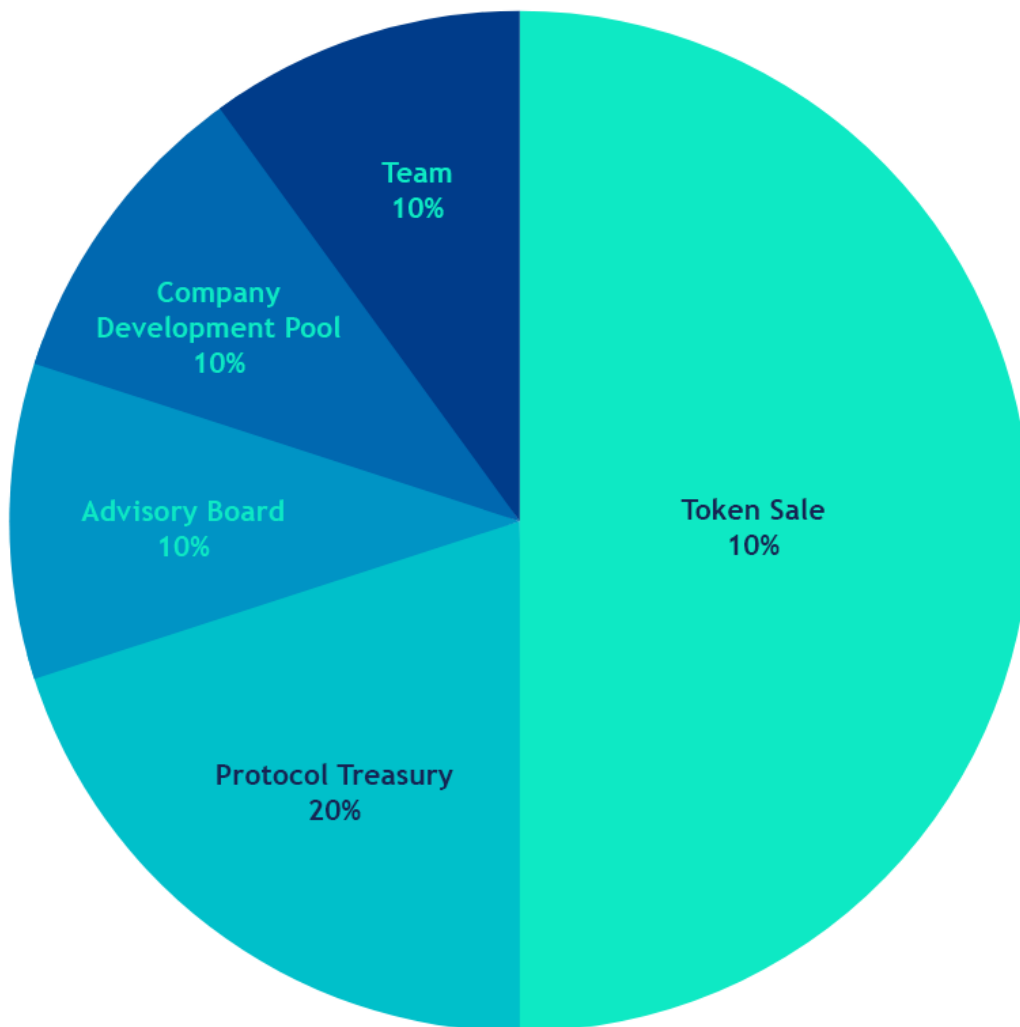
The funds raising in the Emerald Circuit Initial Exchange Offering will be used by the Emerald Circuit Team to launch the full-scale production of its proprietary IoT devices; to fully develop the sidechain functionality; to establish business development and marketing strategies for selling Emerald Circuit devices across the globe; and for team member compensation and community development initiatives.

Total EMR Emission Distribution: 14,000,000 EMR Total Issued

Token Sale: 50% (7,000,000 EMR)

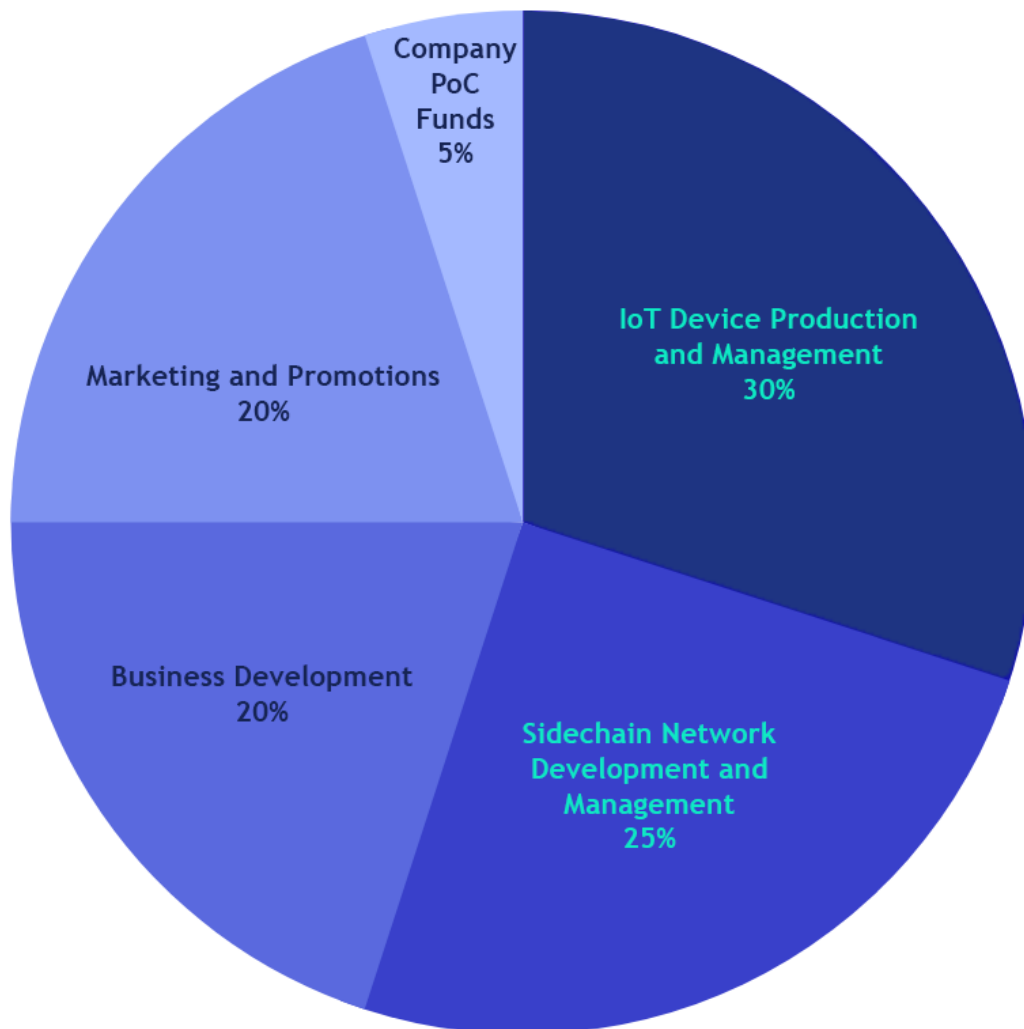
Company: 50% (7,000,000 EMR)

- Protocol Treasury 20%
- Advisory Board 10%
- Community Development Pool 10%
- Team 10%



Operational Funds: Collected in BTC / ETH / AMB from Token Sale

- IoT Device Production and Development: 30%
- Sidechain Network Development and Management: 25%
- Business Development: 20%
- Marketing and Promotion: 20%
- Company PoC Fund: 5%



Further details of the roadmap after the IEO are discussed in *Section 4 Roadmap and Deployment Strategy*.

Section 4: Roadmap and Project Milestones

Unlike many other IEOs, Emerald Circuit has already developed the core products grounding the business model of the project. The Intelligent Objects across the micro, macro, and networked levels are all developed prototypes with patents, available for deployment and Proof of Concept testing. Meanwhile, an initial version of the Emerald Circuit sidechain built on the Ambrosus network has already launched. **As such, the development of the Emerald Circuit project is more closely aligned with building out a complete team of business, marketing, and industry experts to effectively communicate and scale the existing technology available.** This vision is deployed across different areas of development.

IoT Development and Innovation

The existing Emerald Circuit flask, container, and smart pallet prototypes are all fully operational. IoT Development and innovation post IEO will focus on improving upon these core products, based upon specific industry verticals. Integrating more types of sensors, monitors and data collection capabilities over time ensures that as the market for industrial IoT continues to develop, Emerald Circuit remains on the cutting edge.

Sidechain Development

The development of the Emerald Circuit sidechain focuses on improving the efficiency and scalability of the network, while also working to integrate the Emerald Circuit cryptonomic model into other decentralized finance opportunities and with other projects. The sidechain development is therefore focused on:

- 1) Effectively developing and scaling the amount of data capable of being uploaded, validated, and transmitted on the sidechain to the main Ambrosus network

- 2) Building out dApps and applications for specific industry verticals of Emerald Circuit devices
- 3) Working to integrate Emerald Circuit nodes into existing Decentralized Finance marketplace opportunities as a stable coin with a fixed yield

Partnership Development

While Emerald Circuit is already actively working with a number of industrial manufacturers the project will continue to expand its network of manufacturing and development partners in different geographical locations to expand product capacity and support business development. Notably, the Emerald Circuit team will take an active role in working to develop partnerships with other entrepreneurs utilizing the Ambrosus network.

Business Development

Creating a sustainable and robust market for Emerald Circuit IoT devices is the key focus point for developing the project and increasing the amount of data uploaded to the Emerald Circuit sidechain. Emerald Circuit's business development goals include integrating the EC Intelligent Objects with consulting firms, large scale enterprises, and with other entrepreneurs working in IoT.

From the identified markets discussed in *Appendix 1*, the Emerald Circuit team will work closely on expanding its offerings in logistics, secure transportation of precious objects and luxury products, in the management and security of museums and high value exhibits, and in the deployment of IoT solutions in agriculture, water management, and other areas of resource conservation. While the industrial internet of things is only an emerging market the opportunities for leveraging fully secured IoT devices are expected to increase over time.

Business Model

As a blockchain-based IoT ecosystem Emerald Circuit leverages the benefits of both centralization and decentralization in scaling its product across markets. On the one hand, there is a legal entity and centralized business team focused on selling and implementing Emerald Circuit's products across industry verticals (see above). This business team has already established working partnerships with Zimt, Crayonic, and the InnoLab Engineering SARL with the resulting products being a combination of shared IP technologies. As a bridge between product development sales and industrial partnerships, the core business development team is responsible for growing Emerald Circuit, its product offerings, and its implementation across industries.

In parallel to this development, the opportunity remains open for entrepreneurs, consultants, developers, and other businesses to license or purchase Emerald Circuit sensors and its accompanying sidechain data security model for their own business purposes. This includes whitelabelling Emerald Circuit IoT products, integrating Emerald Circuit software with key APIs and ERP systems, and building industry specific verticals using Emerald Circuit devices for entrepreneurs' own monetization. As a holistic approach, it is therefore adequate to consider the Emerald Circuit business model as both centralized and decentralized, with one ultimate purpose: to scalably implement intelligent and secure objects into industries ripe for disruption.

The Emerald Circuit Business Ecosystem Includes:

- Emerald Circuit Business Development Team and Core Tech Team
- Entrepreneurs
- Consultants
- Developers
- Industrial Manufacturing Partners and Whitelabel Wholesalers

Section 4.1: Community development and the Emerald Circuit protocol treasury

As a public permissioned sidechain network protocol, Emerald Circuit prioritizes the development of a robust and active community that will eventually govern the network protocol and any future changes to the cryptonomic model. The underlying design philosophy of the Emerald Circuit cryptonomic structure is based upon *longevity, reliability, and stability* in the EMR utility token dynamics. Initiatives that are designed to grow the Emerald Circuit community into an independent, rational, and engaged community interested in the future of the project includes:

Q4 - 2020

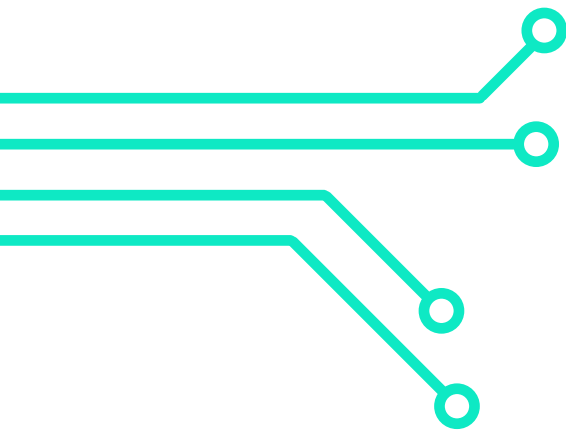
- Bi-directional Telegram and community launches
- Emeraldcircuit.io webpage release
- PR and placed media campaign on Emerald Circuit and the Industrial IoT
- Team and advisor finalization
- Bounty program: translation, placed media, promotion, content creation, listings
- Digital roadshow and pitching

Q1 - 2021

- Sidechain network goes live
- Demo of application and products
- IEO launch
- Post IEO team build out and business and marketing development
- Protocol treasury launch with ecosystem growth objectives

The community development and marketing plan for the Emerald Circuit project incorporates traditional cryptocurrency community building plans via bounty programs and bi-directional telegram. In tandem, the launch of the Emerald Circuit protocol treasury after the IEO follows other blockchain ecosystem designs in ensuring community growth and development sustainably into the future.

With an enterprise friendly stable-coin, and a proof of authority consensus design on the Emerald Circuit sidechain, the Emerald Circuit community is incentivized to support the growth of the project for the long-term, mutually beneficial, stable, and routine rewards that can be accumulated throughout the development of Emerald Circuit and its marketplace in the IIoT market.



Section 4.2: Emerald Circuit Roadmap

The two year roadmap for the development of Emerald Circuit outlines the key areas of development discussed above and their expected progression over time:

2020

- Build out full Emerald Circuit team including core top-level management of the project
- Implement business strategy: first prototype to focus on, first product to be finalized, first market to deploy.
- Align business model with community feedback over IEO time

2021

- Sidechain Version 1.0 Launch
- Finalizing IoT Smart Objects products
- Build up partnerships and collaborations with IoT service providers to start standardization of secure IoT protocols
- Preliminary market research and testing of business model
- Deployment of Emerald Circuit business development plan

2022

- Deploy regional business development strategy
- Expand network of manufacturers and retailers
- Research and development initiative into next generation EC solutions

Conclusion

As the blockchain industry continues to mature, and new solutions further integrate blockchain with other emerging technologies and industrial opportunities, Emerald Circuit is positioned on the frontier of blockchain and IoT development. With core prototypes already developed, and a prospering industrial internet of things market expanding by the year, the Emerald Circuit team is positioned to launch and scale Emerald Circuit across industries, and among enterprises, entrepreneurs, industrial manufacturers, and consultants.

With a clear solution to the problem of ‘garbage-in, garbage-out’ Emerald Circuit is prepared to integrate end-to-end product security into countless industry verticals. As cybersecurity, automation, and digitization continue to increase in importance, Emerald Circuit’s products, long-term focused cryptonomics, and core team will continue to iterate and improve its product offerings over time so as to stay on the cutting edge.





Emerald Circuit Smart Logistics Solutions: From Sensor To Blockchain

“The use of standard data transmission systems will certainly spread across the world - on every container, in every vehicle and in a high number of valuable individual shipments. But that’s not all. The sensors we use will become more powerful and more intelligent than they are today.” - [DHL](#)

Smart Logistics: The utilization of cloud networks, sensors, and devices, to connect, manage, and respond to the movement of products transported between stakeholders.

Problems to be Fixed

The core problem affecting the logistics industry revolves around the lack of digitization among stakeholders: Real-time product management, anti-tampering, and digital product management remain in their early stages of adoption. Coupled with changing business expectations for products to be shipped quickly and for low-costs, the industry is undergoing its largest period of disruption and innovation in more than four decades. Key Bottlenecks to the adoption of smart and automated systems include high setup costs, and a lack of technical literacy.

Emerald Circuit Solutions

Smart Pallets and Smart Containers: For guaranteed product security, real time geolocation, and temperature and humidity monitoring, Emerald Circuit is able to introduce third party logistics providers, air freight carriers, and warehouse operators to a simple, secure, and manageable IoT network.

Primary Value Provided

For logistics providers Emerald Circuit solutions will provide easy-access to digital services and insights: from analytics and alerts, to collaborative business models, and documentation streamlining. Temperature and Humidity sensors built into the smart container provide exceptional security and anti-tampering services to cold-chain logistics companies as well.



Market Size and Geographical Hot Spots

The connected logistics market is expected [to be valued at \\$27 billion US Dollars by 2023](#), with geographical hotspots arising in India, China, and the United States.



Emerald Circuit Organ Transplant Solutions: From Container To Blockchain

“Beating the clock becomes more important than ever when there are human lives on the line, and real-time visibility also goes from being a routine offering to life-saving necessity. Doctors need to know where the organ is located in order to prepare for the procedure and deal with any potential delays. Often, it can be difficult and time-consuming to nail down the location of the shipment throughout the process.” - [FreightWaves](#)

Organ Transplantation: The process in which an organ donor, upon death, has their organs removed from their body and transported to a medical facility and implanted inside of a patient in need of that specific type of organ. On average, only 3 out of every 1,000 organ donors are eligible to donate upon death.

Problems to be Fixed

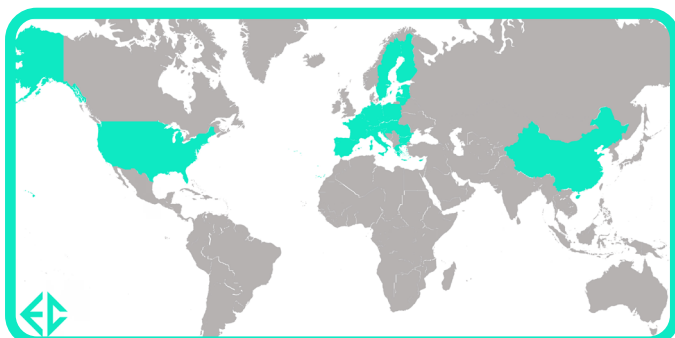
To successfully ensure an organ transplant, the preservation and transportation time must be efficient and with no external interference. Current organ management systems are analogue based, with organs being transported without real-time insight, alerts, or security. Organ verification and journey is essential in the short time frame to the patient.

Emerald Circuit Solutions

Networked Smart Containers with a Mobile App: For securely managing the status, temperature, humidity, and exposure conditions of these life saving organs. Each Organ box is uniquely identified, and tracked throughout its entire journey. Through a mobile application doctors and health care providers are able to stay connected with the timeframe of the organ.

Primary Value Provided

Real-time monitoring and conditions management of life-essential products. Secondary value is provided by digitizing and manageable the movement of the products from their donor to the patient.



Market Size and Geographical Hot Spots

The global transplantation market is estimated to be worth over \$9 billion dollars per year. Global hotspots include the United States, China, and the European Union.



Emerald Circuit Artifact Preservation and Monitoring Solutions: From Exhibit to Blockchain

“As a result, monitoring and controlling the museum’s ambient conditions is the most important task to prolong the lifetime of the museum contents”

-[IoT Monitoring of Museums](#)

Museum Artifact Preservation:

The management of ancient or delicate artifacts - often art or historical objects - maintained under specific conditions for the public to observe and for experts to study.

Problems to be Fixed

Lack of continuous measurement of the contents of museums or fine Art, coupled with the labor intensive management process of the conditions of exhibits and artefacts creates a problematic and costly management environment.

Emerald Circuit Solutions

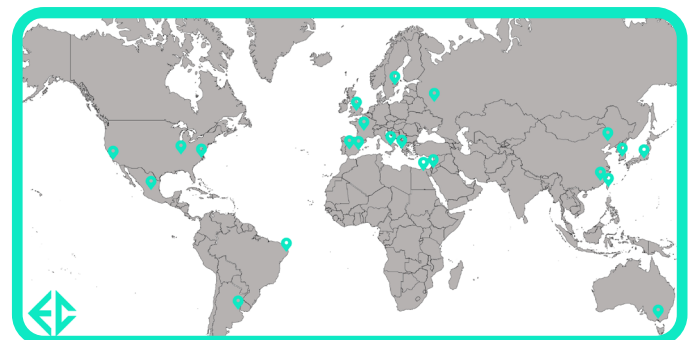
Integrated humidity and temperature sensing solutions into exhibits, networked with one another and providing alerts to museum curators in real-time. For the transportation, preservation and non-public management of artifacts, museums are able to utilize the smart container for keeping objects under monitored conditions in real-time.

Primary Value Provided

Artifact security from decay, anti-tampering from the public, and increased efficiency and management for museum curators. Digitalizing the artifact protection process leads to better preservation of artifacts which can also make a museum more fit for hosting shows or events that involve the movement of artifacts from one place to another.

Market Size and Geographical Hot Spots

There are over [55,000 museums in more than 200 countries](#). In the United States museums report [average revenue of \\$15 billion dollars](#). As of February 7th of 2020, the Museum Technology market has been indicated as being [‘on the rise’](#) largely due to investments in security. Geographical hotspots include the United States, China, Russia, the Middle East, and Europe.

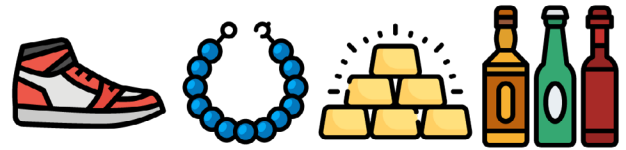




Emerald Circuit Luxury Management: From Box to Blockchain

“Digital permeates every purchase. By 2025, the online channel will represent 25% of the market’s value, up from 10% today. Approximately half of all luxury purchases will be digitally enabled thanks to new technologies along the value chain, and nearly all luxury purchases will be influenced by online interactions.” - [Bain & Company](#)

Luxury Management: The identification and management of high value products and goods as they are transported or held in storage.



Problems to be Fixed

Luxury products suffer from counterfeiting, in-transport damage, and lack of verified identification (digital notarization). This refers not only to high value jewellery and precious metals, but also electronic parts, chemicals, fashion products, automobile parts, fine wines as well as art.

Emerald Circuit Solutions

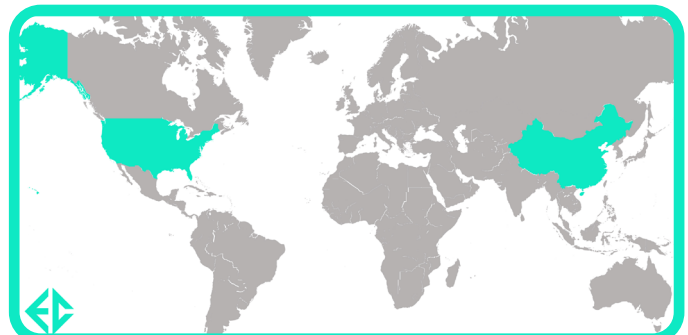
Networked Asset identification and management via the Emerald Circuit smart pallet, and smart containers allow for individual tracking and insight into the real-time status and conditions of luxury products. With geolocation, temperature, and humidity data all time stamped onto a secure network, luxury goods can be demonstrated as genuine, avoid counterfeiting, and retain visibility during transportation or storage.

Primary Value Provided

Digital notarization and real-time condition tracking of high value products (geolocation, temperature, humidity, light exposure). Individual product tokenization and proof of custody management. Proof of authenticity and anti-tampering protection.

Market Size and Geographical Hot Spots

In 2018, the global luxury industry was valued at [over \\$1.2 trillion dollars](#). The industry is comprised of multiple sectors across global markets including: personal goods, food, art, furniture, jets, yachts, and cars. The largest markets include China and the United States, however global luxury consumption continues to grow across the map.



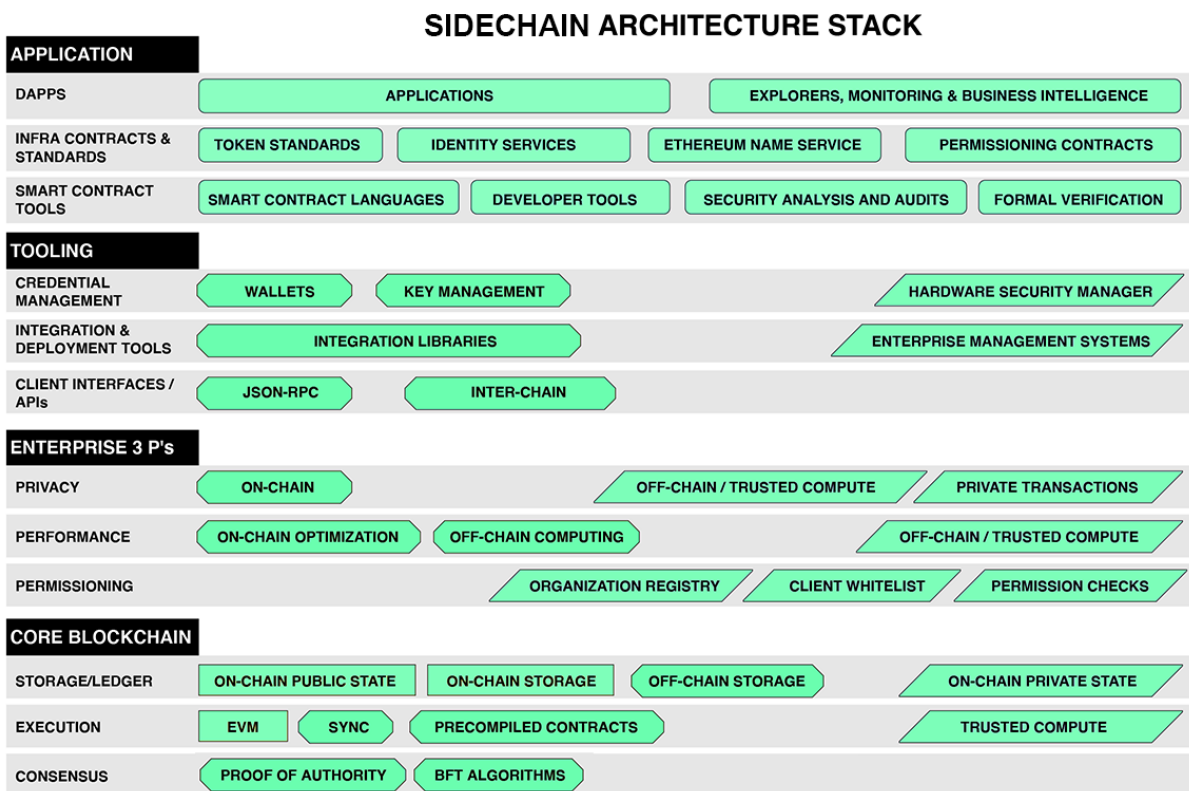
Appendix 2: Sidechain Technical Features

Following the design of the Ambrosus Network, the Emerald Circuit sidechain is based on Ethereum's Aura Authority Round Consensus Mechanism to effectively secure the network. Validation of blocks and maintenance of the state of the network is therefore based upon staking EMR's and not based upon a Proof of Work mining model. The key characteristics and technical features of the Emerald Circuit sidechain include:

- **Compatible with Ethereum Solidity:** All Smart Contracts can be executed as on the Ethereum blockchain, but for 10,000 times cheaper.
- **Wallet, Address, and Transaction ID Integration:** Addresses, Wallets, and Transaction IDs (tx-id) are 100% Ethereum Compatible which has most popular development software enabled by default.
- **AMB-NET Compatible:** All sidechain data is pushed through a Hermes masternode to the Ambrosus Main Network Blockchain for validation.
- **Hermes Masternode Compatible:** All data is validated using Ambrosus Hermes Masternodes, capable of collecting ,segregating, privately storing, and bundling data compactly before uploading to the Ambrosus blockchain.
- **Block Time:** 5 Seconds (3 Times Faster Than ETH).
- **Transaction Fee Paid in Ember:** Gems Limit + Gems Price is used to cover the cost of transactions included in each data upload onto the sidechain.

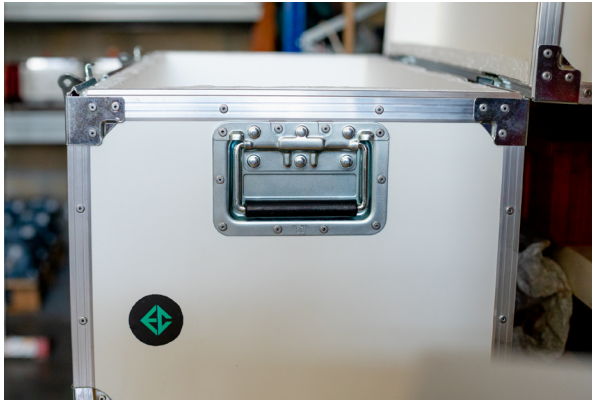
20,000 Sensor Support: Up to 20,000 Sensors are currently supported per Account on the Emerald Circuit Sidechain.

Complete Core Blockchain Layer: The Emerald Circuit sidechain is fully functional as a complete blockchain sidechain: Designed to include *Storage, Distributed Ledger, Execution, and Consensus Sublayers*. For more details see the design below originally based upon the Ethereum Architecture:

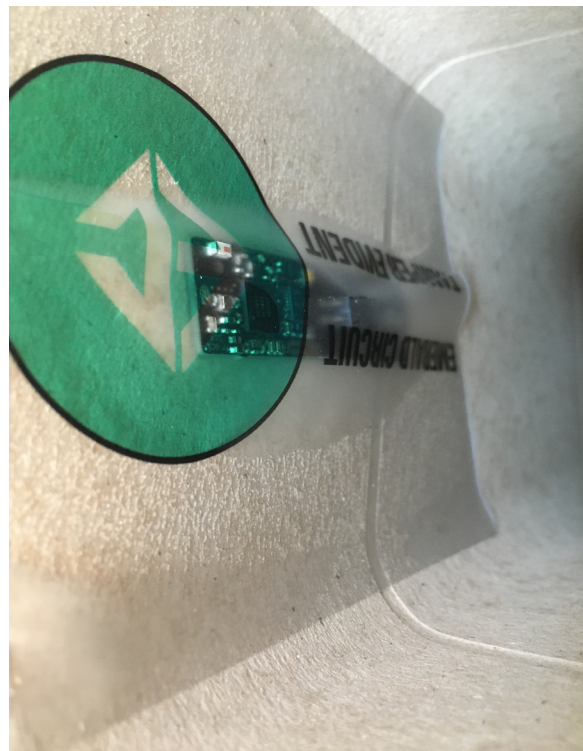


Appendix 3: Smart Box and Smart Flask Image Gallery

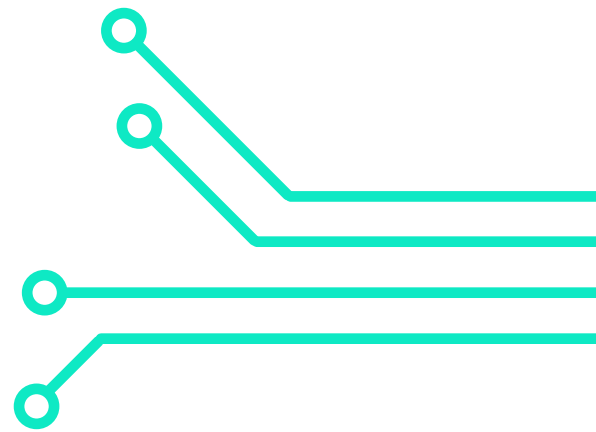
1. Smart Box Prototype for Luxury Products



2. Document Box



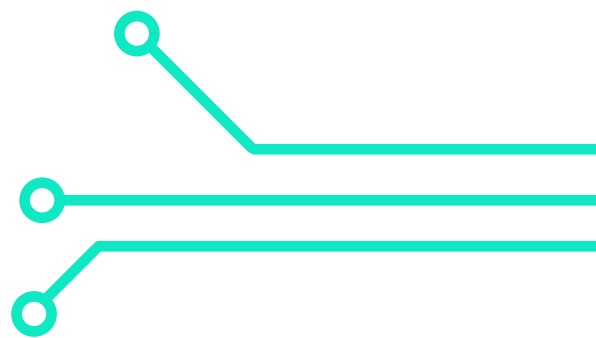
3. Pharma Box



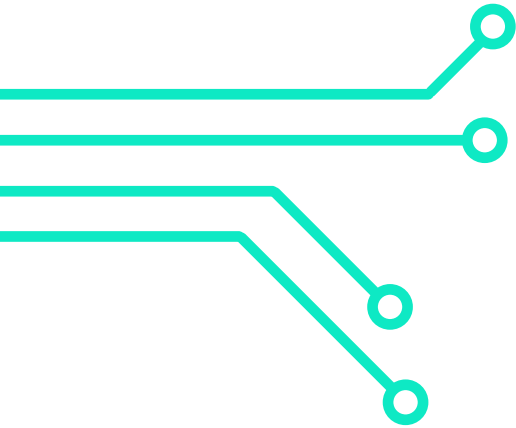
4. Box for Dangerous Products



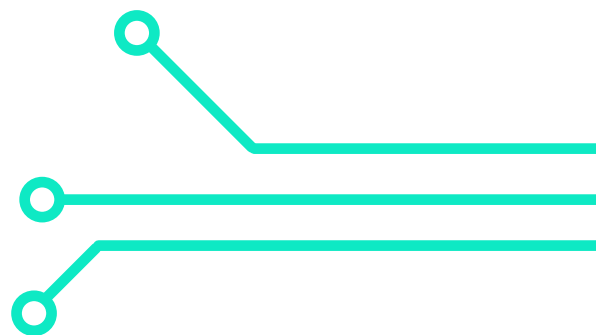
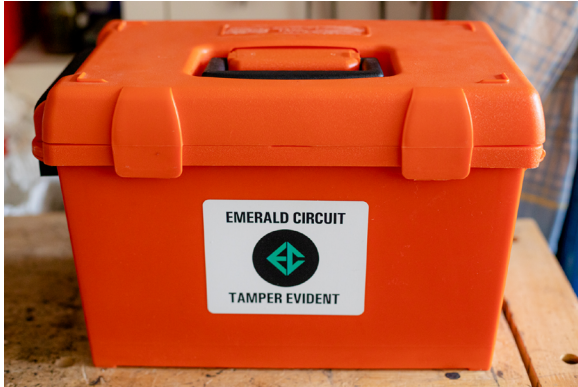
5. Food Box



6. Fisherman Box



7. Organ Transportation Box



8. Smart Flask



Appendix 4: Team and Advisory Board

Project Leader

Dr. Stefan Meyer - Stefan is a Serial Entrepreneur that brings close to three decades of experience working at the intersection of IoT, data encryption, food analysis, and ultrasound sensors. Dr. Stefan Meyer has successfully exited two projects sold to the Maersk Group and Perrot GmbH respectively. He was the Founding Managing Director of the Integrative Food and Nutrition Center at the Swiss Federal Institute of Technology (EPFL). With a PhD in Food Science (Leeds University) and an MSc in Geosciences (University of Lausanne) Stefan has also led R&D projects at Nestle, MHM Microtechnique and Vitargent Biotech. He now specializes in building IoT Architectures with low-energy automatization processes to power the systems of the future.

Core Team

IoT Architect: Tiphaine Paulhiac - Tiphaine brings close to a decade of experience to working at the intersection of IoT, supply chain management, and product verification. As a specialist in Materials Scientists, Tiphaine has worked with both Nestle and EPFL on quality assurance in food and for materials. Before that, Tiphaine worked as an Engineer and Scientific Researcher for Firmenich on encapsulation and delivery systems for high value commodities and products. She holds an MSc in Materials Science and Food Technology from the Swiss Federal Institute of Technology (EPFL) and Imperial College London.

Core Blockchain Developer: Valeri Marshalin - Valeri is a serial entrepreneur out of Ukraine bringing more than a decade of experience to software development

- and more recently blockchain ecosystems. As Co-Founder and Chief Technology Officer of INC4, Valeri has successfully managed and grown a number of blockchain based projects in recent years, including most notably the deployment of the original Ethereum Infrastructure. Before founding INC4, Valeri worked as a Technical Lead Engineer for AdGale. He holds a Masters Degree in Computer Systems Networking and Communications from Volodymyr Dahl East Ukrainian National University.

Front-End Developer: Pavlo Matsenko - Pavlo is a Full Stack developer with close to half a decade of hands-on experience. Programming Languages that Pavlo has mastered include: JavaScript, React, jQuery, CSS and Node.js. Prior to entering software development, Pavlo was a Sales Manager at [2MAC](#). Based upon this skillset, Pavlo will work on the Front-End Development of Emerald Circuit Applications to ensure that product managers and users are able to seamlessly utilize the Emerald Circuit Application for managing products and responding to security breaches.

Advisors and Collaborators

Dr. Jean-Paul Sandoz: Jean-Paul is an acclaimed expert in analog-to-digital signal processing for ultrasound sensors. After 10 years as a signal engineer in Canada and Switzerland, Jean-Paul served as Professor of Electronics and Signal Processing first at the Engineering College of Le Locle and later at University of Applied Sciences of Western Switzerland for over 30 years. He studied Electronics Engineering at Ottawa University. Currently, Dr. Sandoz researches the intersection of supply chain management and anti-counterfeiting technology.

Dr. Vlad Trifa: Vlad is the Founder of Web of Things and former Chief Product Officer at Ambrosus. He is currently CEO of ZIMT, a Startup offering boutique blockchain and IoT services from within the Ambrosus Ecosystem. As Co-Founder of EVERYTHING, he

has designed and built large-scale IoT platforms used by Fortune 100 companies (incl. Coca Cola, Unilever, LVMH, GE). Previously he served as Research Associate at MIT and UCLA. He holds a PhD and MSc in Computer Science from ETH Zurich and EPFL respectively.

Igor Stadnyk: Igor is currently the Chief Technology Officer (CTO) at Ambrosus. He brings over a decade of experience at the intersection of business, finance, and blockchain technology. With a Masters from the National Technical University of Ukraine, and a proven track record of success in project management, marketing, business development, and distributed network operations, Igor is nothing short of an expert in the blockchain industry. Before joining Ambrosus, Igor has served as Chief Executive Officer of Minerall.io—a leading multi-coin mining pool operator, that has garnered deep experience working with various consensus mechanisms across the industry.

Ken Nogushi: Ken is a member of the International Institute for Management Development in Lausanne Switzerland. With decades of experience behind him, including long-term commitments at Fertin Pharma A/S and Philip Morris International, Ken brings a practical and business oriented perspective intent on bringing new products into changing markets. As a strategic adviser Ken will help position and evaluate the market potential for the signatory Emerald Circuit products. Ken holds a Bachelors in Mathematics and Computer Science from the University of Waterloo.

