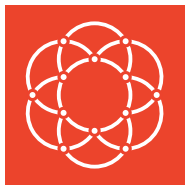
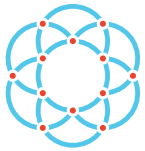
Ockam

White Paper v1.7
February 2018

Chapters

WHITE PAPER V.1.7
FEBRUARY 2018





The internet has been widely used for over quarter century. Over that time an interesting, but not originally obvious, behavior evolved between the users of this communication tool: Trust.

Unthinkable 20 years ago, people now jump into strangers' cars that they summon with their phones. We buy used products online, sight unseen, based on seller-generated descriptions. The sellers of those goods ship their products to buyers, trusting that they will be paid for the transaction. We even invite strangers into our homes to stay for a vacation. These trust mechanisms were built by companies such as Lyft, eBay, PayPal, and Airbnb. For trust to exist in these peer-to-peer networks we rely on these centralized authorities to broker attestation and reputation between accredited users.

There is an accelerating need for trust mechanisms to exist between connected devices that exchange data with each other. The common practice today is to 'hardwire' trust between identifiable machines using rigid APIs. A centralized broker for data exchange between newly introduced machines does not readily exist in the same way that it does with ride sharing or online payments. However, the need for trusted data is more important than ever, particularly with the emergence of artificial intelligence and machine learning.

In the old world it may seem that the next step would be to create a centralized broker for trusted devices that need to share their data with each other. At Ockam we believe in a different future.

There is a far better solution because there is a tragic flaw in trusting a central broker to manage trust. The data breach of Equifax in the summer of 2017 is an example of how our over-reliance on central authorities to manage our data and create trust between users of the internet creates immense amounts of risk of data breaches and improper usage of personal and proprietary data.

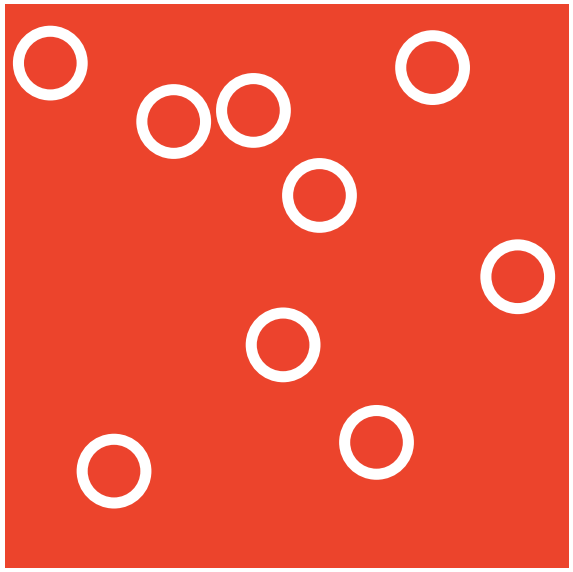
We see an opportunity for new connected device networks to skip past the centralized norms that were created for the sharing economy a decade ago.

Blockchain can create a new trust paradigm for the internet. It is now possible to create a trusted relationship between any two entities without a central authority to oversee the transaction. The decentralized model for blockchain creates trust by design. This is why many refer to blockchain as a 'Trust Machine'.

Ockam is creating a blockchain based platform for connected devices to provide the trust required for widespread adoption of the machines that will change the world.

Let us tell you how...

Matthew Gregory
Founder & CEO



Connected devices are functionally and economically inefficient

Connected devices come in all sorts of shapes and sizes. Their proliferation in the past decade has changed the world. Trillions of dollars are spent in this segment every year, yet there is no common platform to unite the devices. This means that billions of dollars are wasted every year on solution-specific custom integrations.

To understand the dire need for the Ockam Blockchain, first we need to dissect the trends among connected device ecosystems and the economies that they create. We also need to classify each type of device to understand how each component fits into the platform that Ockam is building.

The economic scale of connected devices is already massive … and it's accelerating

8.4 billion connected things were in use worldwide by the end of 2017, a 31% increase from 2016—that's more devices than there are people on the planet. By 2020, that number will surpass 20 billion. Total spending in this market, that barely existed a decade ago, crossed $2 trillion in 2017.

The consumer segment is the largest user of connected things with 5.2 billion units in 2017, representing 63 percent of the overall number of applications in use. Businesses employed 3.2 billion of connected things in 2017. The consumer segment is led by mobile smartphones, connected vehicles, smart TVs and digital set-top boxes. Businesses are rapidly employing devices such as smart electric meters and commercial sensors. [Gartner, 2017]

Artificial Intelligence (AI) and Machine Learning (ML) have recently been introduced to connected devices in both consumer and industrial applications. Some devices use AI / ML directly, while others supply data to enrich AI / ML networks.

Globally, the tech giants spent somewhere between $20 billion and $30 billion on AI in 2016, with 90 percent of this spent on R&D and deployment, and 10 percent on AI acquisitions. Venture capital, grants, and seed investments also grew rapidly, albeit from a small base, to a combined total of $6 billion to $9 billion. [McKinsey, 2017] Since these systems are still in R&D phases we can expect to see a new wave of AI powered applications in our connected devices in the near future.

The ideals of security and interoperability are broken in device ecosystems today

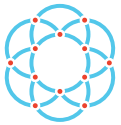
Device brand manufacturers build security around their products to reduce malicious attacks from untrusted connected devices elsewhere in their network. This reduces the interoperability between machines in broad supplier ecosystems.

There is a simple thought experiment that illustrates this point: If you wanted to perfectly secure a device, you would buy it from the store, lock it into a waterproof case, and throw the case into the sea. The device would be perfectly secure in its ecosystem inside of its case. However, it would be equally impossible for it to interoperate with other ecosystems, or other devices.

On the other end of the spectrum, if you wanted to make a perfectly interoperable device, you would remove user credentials, and publicly publish the API and it's URL endpoint to the universe. Thus, any other connected device could then interoperate with your device. However, your device would be exceptionally vulnerable to a multitude of security attacks.

These extremes illustrate the choices that a device engineer must consider when approaching the design of their device. In reality, engineers constantly trade security for interoperability in compromise to deliver practical products to market.

There are a lot of real world examples of these tradeoffs; In the Summer of 2016 a botnet application, Mirai, spread through hundreds of thousands of connected devices, such as routers and webcams, by guessing common factory installed usernames and passwords. The generic user logins allowed consumers easy access to control the devices. Unfortunately, this convenience was also the vulnerability that contributed to the denial of service attacks on Reddit, Spotify, Twitter, and many others, later that Fall, which blocked real users from accessing these services.



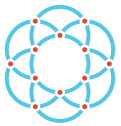
Groups of devices are coalescing into separate, centralized, and hardened ecosystems

One way to hack the choice between security and interoperability is to create trusted walled gardens of devices that are produced by the same brand manufacturer. This allows device designers to collaborate with their other colleagues to create elegant user experiences using similar trusted credentials between different products all sold by the same company.

A good example of this is the Apple ecosystem. You can set up a new Apple TV by resting your iPhone on it. Airplay controls are built into iOS applications, Apple Watch unlocks a MacBook, and so on. Apple created a hardened ecosystem that is relatively secure but does not account for the vast number of devices that could be connected now or in the future. The moment a homeowner adds a non-Apple device, such as a webcam, to their Apple ecosystem, then that ecosystem will be in an unforeseeable configuration that could be made vulnerable to all sorts of attacks. This problem is exponentially exacerbated as the combination of different device brands, in any given network, increases.

Obviously, Apple is not the only hardened and centralized ecosystem in the consumer space. Amazon, Google, Samsung, Nest, and many others could have been used in the example above. Moreover, hardened ecosystems exist outside of consumer brands and extend into industrial, supply chain, and medical applications as well.

Finally, the hardened ecosystem perpetuates brand lockin for consumers. This crowds out innovative new device companies, because the very existence of their products in a network of like-brand devices creates a negative externality around security and interoperability for the entire network. Thus, many separate ecosystems of connected devices have formed.



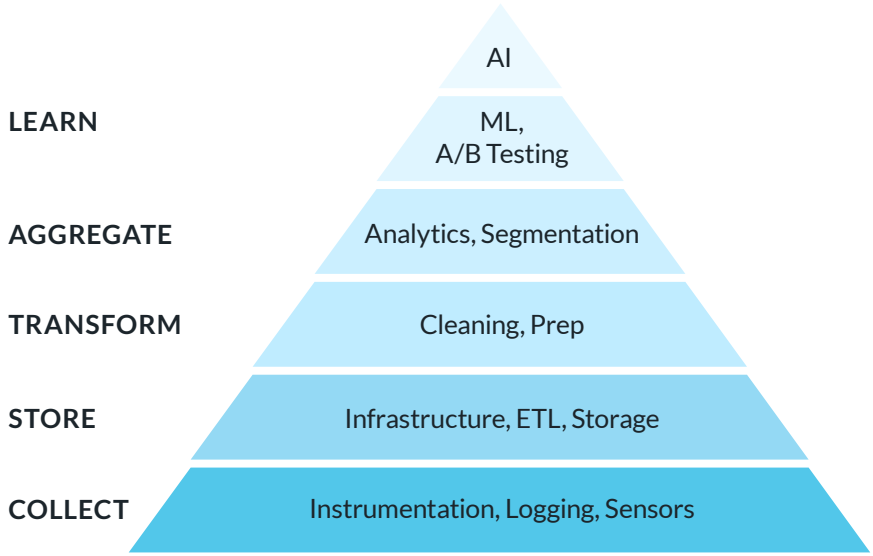
The value of data generated by devices is increasing – rapidly

"Artificial Intelligence is poised to transform business in ways we've not seen since the impact of computer technology in the late 20th century," says Paul Daugherty, chief technology officer, Accenture.

"The world's most valuable resource is no longer oil, but data," published The Economist earlier this year.

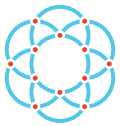
Machine learned (ML), and artificially intelligent (AI) systems not only rely on data to operate, they also need tremendous amounts of it. This means that sensors, instruments, and connected devices are critical components to the future of AI / ML systems. Moreover, the more advanced and pervasive AI / ML systems become, the more valuable the network of data that feeds them will become as well.

This concept is well articulated by Monica Rogati in her article, "The AI Hierarchy of Needs". She juxtaposes a data science stack to Maslow's framework. As you can see, the collection of quality data at the base of the pyramid is critical to the quality of AI / ML at the top.



While an instructive model, it may be easy to forget that this pyramid rests atop a largely offline world. The collection layer is what transforms the real world, through observations, into digital assets. Examples include humidity in the air, the pulse of your heart, the visual indication that a pedestrian is crossing the road in front of your car, the sound command 'Hey Siri', and a person's distinguished facial features.

Thus, while artificial intelligence and machine learning are exciting technologies, it's also important that we recognize the critical importance of connecting billions of trusted devices in order to collect actionable data, lest we fall prey to the data science axiom of 'garbage in, garbage out'.



It is important to understand device topography

Ockam has classified connected devices into four segments; Type I, II, III and IV. These devices lie on a spectrum from simple (I) to complex (IV). We have done this to segment ideas for how each type of device could utilize the Ockam Blockchain to create a cohesive and interoperable device platform. We define them as follows:

Type I - Basic

A Type I device is the most basic connected device. The device is low cost and contains the bare minimum of computing hardware essentials to be connected to the internet. It maintains an address on a local network and has limited storage, compute and networking capabilities. These devices are stateful. For example, an operational traffic light could tell another device if it's displaying a 'green', a 'yellow' or 'red' light.

In most cases these devices are highly specialized and may be controlled by more sophisticated connected devices elsewhere in their network. Typically, these devices are not mobile and are permanently installed in physical locations.

Examples may include light bulbs and switches.

Type II - Sensor

Type II devices have a varied range of compute, storage and networking capabilities. Most notable, the main purpose of these 'specialty-tools' is to gather information from the external environment, convert it into data, and then share it within the network, where it may be stored.

Just as there is a wide range of hardware capabilities for these sensors, there are many different ways that they can be deployed. Some have fixed locations and are close to local area networks. While at the other end of the spectrum, others are on the move, and live in edge computing network environments. It's the later environment, of mobile industrial applications, where there is incredible potential for Ockam to improve interoperability and data exchange between trusted devices.

Examples may include webcams, weather sensors, medical instruments, and near field communications devices (NFC).

Type III – Advanced Connected Device

Type III devices have advanced compute, memory, storage, and networking capabilities. They have broad platform uses and can be configured to utilize a wide range of software applications that may be installed on them. Increasingly, these devices have machine learning and artificial intelligence capabilities which are reliant upon data from elsewhere in their network.

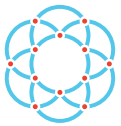
Examples may include smartphones, tablets, laptops, vehicles, and servers or edge devices.

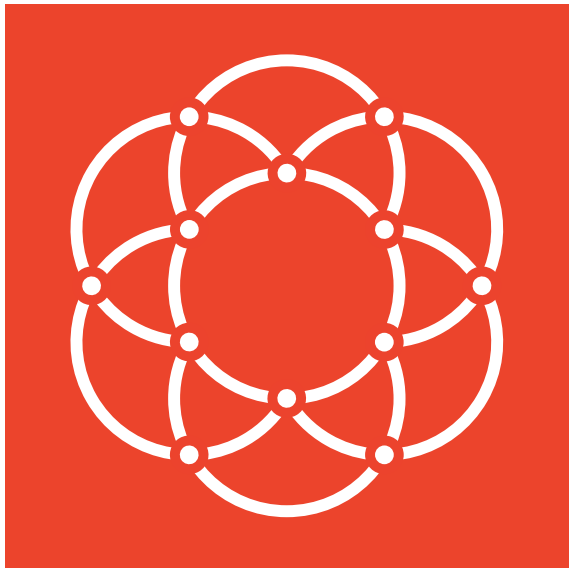
Type IV – Ockam Node

Similar to Type III devices, Type IV Ockam Nodes have advanced compute, memory, storage, and networking capabilities. The key differentiator is that a Type IV device helps to maintain the distributed integrity of the Ockam Blockchain as a Node, which we will discuss further in the next section of this paper.

Examples may include vehicles, industrial devices, autonomous delivery drones, servers.

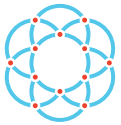
There are several reasons that a connected device may want to be a Node on the Ockam Blockchain. Nodes help to maintain the distribution and immutability of the Ockam network, and may reap the transaction fees that the generation of new blocks produces. It is likely that a device that must read the Ockam Blockchain at a regular and rapid rate may want to have easy access to a local copy of the chain, and thus become an Ockam Node.





Ockam Blockchain is a connected device enablement platform

The Ockam Blockchain is a universal platform that enables all connected devices to interoperate. This platform will be tuned for connected devices, honed for enterprises, and empowering for upstarts. Like other blockchain networks, the Ockam Blockchain is public, decentralized, secure, and immutable. Prior to the proliferation of blockchain enabled peer-to-peer topographies, it was not possible to create a universal device platform with these qualities. Ockam will enable the devices that are supposed to change our world...to change our world.

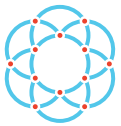


Ockam Blockchain basics

The Ockam Blockchain is a public blockchain, built with an open source code base, and is specifically purposed for connected device interactions.

We anticipate that Ockam Blockchain source code will evolve over time according to the embedded governance model. A couple universal concepts that we want to highlight are virtual machine, nodes, accounts, OCK, gas, and smart contracts.

- **Virtual Machine:** Ockam Blockchain is a network of computers that act like a gigantic single machine.
- **Node:** Each computer in the network is a Node; or as we described earlier, a Type IV Connected Device. A node maintains the integrity of the network by maintaining either a full or a shallow copy of the blockchain. It may also participate in verifying transactions on the network (aka mining).
- **Accounts:** An Ockam Account is a small piece of software that lives in a connected device. It maintains a balance of OCK and a public/private key pair that allows that device to transact with the Ockam Blockchain. The Account is also used to Register a device with a unique identity, which we discuss in the section, 'Ockam Device Registry'.
- **Gas:** The Virtual Machine needs 'fuel' to run. To compensate nodes for the computational and transactional work that they contribute to the network, they are awarded with OCK.
- **OCK:** OCK is the native token for the Ockam Blockchain. OCK may be exchanged between accounts, using the network, anytime an exchange of value is required. OCK is the gas in a computational transaction on the Virtual Machine. Finally OCK maybe utilized in the Ockam Blockchain governance model.
- **Smart Contracts:** Software code that performs a specific action inside of the network. These contracts allow for unbounded possibilities for applications and device-to-device interactions or transactions on the network.



Smart Contracts extend the platform

Eventually there will be thousands of Smart Contracts that run on Ockam's Blockchain. The most important of which, and the first that we will build, is the Ockam Device Registry.

Ockam Device Registry

The Ockam Registry ('The Registry') is a foundational component on the Ockam Blockchain.

Introduction

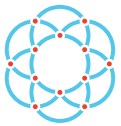
The Registry is a smart contract that stores a list of connected devices that have attestation on the platform. Devices that register themselves on the Ockam Registry will have immutable and decentralized identity that can be accessed by other devices in the network. Thus the Ockam Registry is a necessary substrate to enable interoperability in next generation applications that utilize data from, push data to, or control connected devices.

Access to this Registry is available to anyone on the network. The only expense for registering is the gas computational transaction fee of OCK that the nodes on the network require to process the request.

The decentralization of device identity and interoperability

The Registry shifts today's centralized model of device interoperability into a decentralized one. There are a couple reasons why a decentralized Ockam Registry is better than the groups of centralized ones that currently exist today. Centralized device management creates hardened ecosystem silos, as we discussed earlier. In a model with multiple centralized device management solutions, device makers are the first order in the logical ordering of a device's attestations. The device attributes, like ownership and permissions, are controlled by the applications that are built into the device. This means that devices that are produced by the same manufacturer may easily share information with each other, but when users mix and match devices it becomes difficult to order permissions across applications to control the devices.

Since roles and hierarchies of centralized device makers ecosystems are abstracted away in the decentralized Ockam Registry, a new ordering of device control is possible. Because device identities are publicly available, existing silos are removed. More so, the Ockam Device Registry makes it possible to know the history of attestation and reputation for every registered device. This means that decentralized applications can be built to provide a control plane and permission structure for any device on the network.



Applications can utilize The Registry to give ownership of a device to an individual. For example, after adding devices to the Ockam Registry it will be possible for an individual to control her own devices with the application of her choosing, if she also creates a decentralized identity for herself, using any one of the many blockchain based protocols that specialize in personal identity management. This creates endless opportunities for new applications to emerge based on the Ockam Registry platform.

Other Smart Contracts are under consideration

Staking claims for reputation

This is a smart contract that allows a device to stake a claim of OCK against it's attestation to affirm its reputation on the network. In a staking scenario, OCK are held in 'escrow' as collateral against the creator's claim to its reputation. The reputation of a device could be claimed by its owner, or the device itself. Moreover, the reputation of the device can also be challenged by another party on the network if a self-claimed reputation is deemed inaccurate.

The benefits of the Ockam Registry, paired with a staking contract, are particularly obvious when we look at Type II devices in public networks. Currently, it is nearly impossible to get data from a device and know it's reputation for providing trusted information based on other users' experience with that device's data. However, when attestation is paired with a staked reputation this problem is solved.

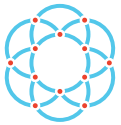
Curated Registries

Curated Registries are subsets of the Ockam Registry. Each of these curated lists could be a separate smart contract, and could group devices by manufacturer, reputation, service level agreements, function, or maliciousness.

Ockam Blockchain is poised for adaptations through decentralized governance

It is is vital for the long term viability of the Ockam Blockchain that we allow flexibility for growth and the unforeseeable future requirements of the network. Blockchain is a very young technology and we need to prepare for adaptations as technology evolves. A specialized device network that was separated from general purpose networks allows the Ockam Blockchain to solely focus on the problems of connected devices.

Ockam Blockchain's decentralized governance not only creates a future-flexible network, but it also enables completely new decentralized business models and economies to emerge around connected devices ~ anything is possible!



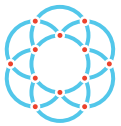
Ockam Blockchain's governance model will make it future-proof

Decentralized governance is a critical for a decentralized blockchain network. It is the mechanism that allows the network to grow, adapt, and become future-proof. It seems obvious in a centralized software paradigm that there should be updates to software that fix bugs, improves functionality, and changes with evolving external factors. However, in a decentralized network model, a mechanism is needed to make these types of fixes and improvements going forward.

In the Ockam Blockchain's earliest days, Ockam Inc. will be its most prolific supporter and serve as the central governor. This is because Ockam Inc. will, initially, be the majority holder of OCK tokens. We will build features into the Ockam Blockchain as we adapt the network to the requirements of early adopters. We will also champion the effort to onboard a vast group of governors who have the network's best interest at heart. As more and more people, companies, and institutions hold OCK tokens, the more distributed the Ockam governance will become. Eventually, through the complete distribution of OCK, the network's governance will finally become entirely decentralized, and controlled by the OCK token holders.

The details of the governance model can be adapted as part of the governance of the network. We have not yet concluded the precise model that we will adopt for governance, but we are considering a master node concept, where nodes on the network that maintain a minimum OCK balance shall be entitled to submit proposals for consideration. Other master node owners can then vote on the inclusion of that proposal.

We already foresee several unique requirements that this network will need to adapt for connected devices and enterprises.



Adaptations required for connected devices

Scale and scalability

Connected devices outnumber connected people, and they transact far more frequently than those people. Thus connected devices operate at a scale that warrants its own dedicated network that adapts to the unique requirements of those devices.

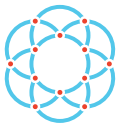
As of this writing, there are 20 million user accounts and 28,000 nodes running on the Ethereum Blockchain network. By contrast, there are 8 billion connected devices in the world today. Each could need their own account on Ockam Blockchain. Thus it is a reasonable assumption that the Ockam Blockchain will need to account for several orders of magnitude more account identities, and at least an order of magnitude more nodes, than the Ethereum Blockchain. If this assumption turns out to be true, then we will want the freedom to tune the Ockam Blockchain for connected devices scale and throughput needs as they emerge.

Ockam Blockchain's capabilities should scale one-to-one with the needs of connected devices because this network serves devices. One of the advantages of a blockchain network that is solely tuned for connected devices is that this network will not be impacted by extraneous activity on the network, like ICO financial transaction spikes or DigitalCat games.

Ockam may adjust block size, or deploy data sharding structures that best suit this network's unique scaling and throughput requirements. As new technologies emerge, and as Ockam Blockchain's adoption grows, the network can choose to immediately adopt, pivot, delay, or ignore those new technologies in the best interest of this network's specialized purpose.

Sovereign device identity with self-stored metadata

Connected devices have an identity that could be summarized with metadata. For example; manufacturer, model, serial number, location, and a litany of technical hardware and software features could all describe a unique connected device. A connected device could even describe itself by explaining its own API endpoint. There is currently no way for connected devices to share their metadata with other devices, without prior 'hardwiring' of handshakes between known devices. As we previously discussed, this is typically done in a centralized way. Devices need a common and trustful way to store, share, and look up metadata. The Registry is the first step to enable self-sovereign identity and self-stored metadata. We anticipate further adaptations to enhance device self sovereign identity though hardware and software partnerships.



Complex communications

Connected devices also need to converse and share data with each other. They need to communicate one-to-one, one-to-many, and many-to-many to enable true device interoperability. Thus a built-in and decentralized messaging service is a likely adaptation for the Ockam Blockchain.

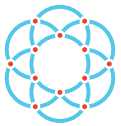
We are reviewing and tracking the development of Whisper and Matrix as open source, decentralized messaging services that could enhance the ability for any two connected devices to share data with each other via these messaging protocols.

Edge computing integrations

Devices are, by their widely distributed nature, already 'decentralized'. It's the way that they are currently connected to the internet that 'centralizes' them in a client-server architecture. Many are connected through local area networks that connect to an internet service provider, and thus their back-end servers. Increasingly, devices are connecting through wireless mobile networks. To meet the needs of mobilized devices, in the classic client-server centralized web architecture, centralized cloud service providers are moving servers out of data centers and into cell towers to be closer to the devices. This is called edge computing and it is booming due to the expansion of connected device deployments. This is great news for the Ockam Blockchain because it moves advanced computing resources closer to devices and geographically distributes computing power. We anticipate that Ockam nodes will live in edge computing environments increase the performance of device-to-device operability through partnerships with telecoms and edge compute providers. When Ockam Blockchain is added to edge computing infrastructure, the networks will architectually match the distributed nature of connected devices and become decentralized.

Devices are not always connected

How should the network react when a device goes offline, or when a mobile device moves out of cell tower range? After all, connected devices are not always connected and they may be on the move. Moreover, what about two registered devices that meet each other in a one-on-one setting, where they are disconnected from the network, but can communicate with each other via bluetooth or a closed local network? These are difficult problems with connected devices that we plan to solve for. Regardless of the specific solutions that we add to the platform to solve for the 'not always connected' issues, we expect a resolution to this issue to become a foundational part of this network's unique functionality.



Adaptations required for Enterprise

Elastic Scale

We anticipate that enterprises will be power-users of the Ockam Blockchain and we will build this blockchain to meet their emerging needs.

Enterprises operate at massive scale and need a blockchain that can keep up with their high throughput and service level specifications. For example, we envision an adaptation where an Enterprise would be able to signal to the network that they require an elastic scale out of resources to process heavy workloads, say during a product launch.

Management of stakeholders

Ockam is a public blockchain, and thus the information on it is available to anyone on the network. We anticipate that the Ockam Blockchain could become a hybrid public/private network to satisfy the unique needs of Enterprises. They may have legal governance, competitive pressures, or closed partnerships that warrant that their transactions happen within the network but amongst a private and closed consortium of members.

Inside of the enterprise, employees will need varying degrees of role-based access controls (RBAC) to engage the Ockam Blockchain, and to manage their fleets of devices. Moreover, customers may need unique access, or ownership, of their devices as well. These control mechanisms can be built into the on-chain records for device management.

Curation of lists

We plan to build curated list functionality into smart contracts that allow enterprises to manage their fleets of devices. These contracts will also allow device manufactures to exchange data with permissioned business partners with private and secure communications. The corollary to one of these whitelists is a blacklist. Enterprises will also be able to create blacklists for devices that may cause known harm to the customers of their devices.

Privacy and data indemnification

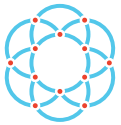
Data privacy is a growing and necessary concern for Enterprises. The products that they sell create data. In many scenarios, the Enterprise is responsible for maintaining secure records of this data. By using upcoming adaptations to the protocol, and through specialized smart contracts, device owners can take ownership of the data that their devices produce. This empowers consumers and unburdens enterprises.

For example: Imagine if a connected medical device, that was registered on the Ockam Blockchain, could send its data directly to a patient who had a self-sovereign identity. This scenario could shift the entire landscape for HIPAA compliance since neither the healthcare facility nor the device providers would have to manage the patient's data. At the same time patients would own their own data from the moment their data was created.

Ockam product roadmap is a catalyst to drive adoption

Ockam Inc. is committed to the long term growth and viability of the Ockam Blockchain. This includes far more than the coding of new adaptations and the management of the first nodes of the blockchain. We plan to evangelize Ockam Blockchain to its early adopters, and to establish partnerships with the enterprises and upstarts that will use it as a platform for their own growth.

We anticipate that Ockam Inc. will be one of the first power-users of this platform. This means that we will build our own smart contracts, like the Ockam Registry. To lower barriers to broad adoption we will build SDKs, dApps and cloud services that link devices, users, and enterprises to the Ockam Blockchain.



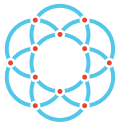
Ockam Blockchain

We plan to build the first Ockam Blockchain nodes on Microsoft Azure. Microsoft Azure provides a fantastic platform to quickly scale out resources, horizontally and vertically, as the network grows. This initial deployment will also enable third parties to quickly launch and then manage their own Ockam Nodes on Azure. We will also make it possible for network participants to stand up their own Type IV device nodes.

The heart of the platform is The Ockam Registry; mostly all other products and functions that Ockam will create will use this tool. Thus, it is the first Smart Contract that we will build and it will be part of the initial launch of the Ockam Blockchain.

Ockam SDKs

We envision a suite of Ockam SDK (Software Developer Kit) products that enable devices to easily register themselves to the Ockam Registry. These SDKs will be device specific, as needed, to create the easiest possible developer experience for our manufacturing partners. Moreover, SDKs will be created to register the 8 Billion devices that are already deployed into our world. These SDKs will manage OCK balances for the machine, directly interface with dApps, register devices to the Ockam Registry, and engage other smart contracts on the network.



dApps Ecosystem

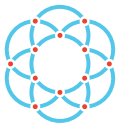
Ockam plan to produce several dApps. We also plan to enable and encourage others to build dApps that leverage the Ockam Blockchain network.

Some dApps that we envision include:

- Identity Applications that link owner and device identities.
- Staking applications that allow people to manage their stake in devices.
- Applications that codify SLAs for devices.
- 'Mining' applications for Type II Sensor devices that fail their SLAs and then recoup the rewards of the stake behind the sensor.
- Applications that curate specialized Whitelists / Blacklists of devices that are in the Ockam Registry.
- Applications that link the Ockam Blockchain to other blockchain networks. Ockam is designed to work with, not against, other networks.
- Governance proposal and voting tools.

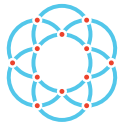
Ockam Enterprise

Existing device manufacturers have pre-existing device management, identity, and user systems. We plan to build cloud services that link the Ockam Blockchain network to these Enterprise systems. This will serve to widen the addressable market for organizations that want to utilize the benefits of the Ockam Registry, and the Blockchain more broadly. Ockam Enterprise will also manage OKM for the Enterprise, handle role based access controls for their internal teams, and sync with the Ockam SDKs in the devices they produce.



Ockam is committed to partnerships

Ockam is fanatical about team culture. It's part of why we love the open source and the decentralized communities within blockchain development. Ockam is committed to lead, enable and participate in the broad ecosystem. To that end, we highly value partnerships as a critical component of our shared mission to change the world of connected devices.



Thank You

Ockam.io

DISCLAIMER OF LIABILITY:

This white paper is meant to describe the currently anticipated plans of Ockam Inc. (“Ockam”) for developing a new blockchain token mechanism (“Token”) that will be used on the platform/network sponsored by Ockam (the “Platform/Network”). Nothing in this document should be treated or read as a guarantee or promise of how Ockam’s business, the Platform/Network, or the Tokens will develop or of the utility or value of the Platform/Network or the Tokens. This White Paper outlines Ockam’s current plans, which could change at its discretion, and the success of which will depend on many factors outside Ockam’s control, including market-based factors and factors within the data, internet-of-things and cryptocurrency industries, among others. Any statements about future events are based solely on Ockam’s analysis of the issues described in this document. That analysis may prove to be incorrect.

This document does not constitute an offer or sale of the Tokens or any other mechanism for purchasing the Tokens (such as, without limitation, a “simple agreement for future tokens” related to the Tokens). Any offer or sale of the Tokens or any related instrument will occur only based on a disclosure statement, risk factors, and purchase agreement for the Tokens or the applicable instrument.

Purchasing the Tokens or any related instrument is subject to many potential risks. Some of these risks will be described in the offering documents. These documents, along with additional information about Ockam and the Platform/Network, are available on our website at www.ockam.io. Purchasers of Tokens and related instruments could lose all or some of the value of the funds used for their purchases.