Atonomi

The Secure Ledger of Things

Vaughan Emery
vaughan.emery@atonomi.io

David Fragale
david.fragale@atonomi.io

Andrii Zamovsky
andrey@ambisafe.co

Peter Kinnaird
peter@ambisafe-financial.com

Abstract

Atonomi provides a security protocol and infrastructure to enable billions of IoT devices to have trusted interoperability for both data and commerce.

The key innovation of the Atonomi low-level protocol is to root the identity and reputation of devices on a blockchain-based immutable ledger. Atonomi accomplishes this by building and deploying an ecosystem of participants designed to maintain decentralized consensus for device transactions on the Atonomi Network. Combining on-chain and off-chain resources, and built on Ethereum technology, Atonomi's architecture is extendible by developers across IoT verticals to secure the vast realm of IoT devices ranging from healthcare and home automation systems, to smart-city infrastructure, to industrial sensors and controllers.

This is required because vertically focused IoT companies are building diverse new applications for both controlled and autonomous device-to-device interactions, but the attack surface represented by billions of IoT devices—most of which are now unprotected or poorly protected—could enable hackers to disrupt the services that is expected to control many aspects of our lives in the coming years.

The Atonomi Security Protocol provides the following fundamental contributions to enable interoperability and secure exchange of data and commerce at scale:

a. Trusted immutable identity of devices through its device identity registration service
b. Reputation protocol to incent and enable Atonomi and decentralized third-party auditors to build systems to detect and remove bad device actors
c. Tokenized economy for the registration and activation of devices, and facilitation of a reputation-scoring ecosystem among third-party auditors, and for transaction validation services
d. Fully extensible architecture designed to be built on top of by vertical IoT applications for security

Atonomi is a project that leverages established technology of its parent company, Seattle-based CENTRI Technology. CENTRI is a leader in providing IoT data security solutions, with its technology integrated into IoT solutions produced by multi-billion dollar ecosystem players like Arm, Flex, and Intel, among others. CENTRI's security technology protects data for IoT devices and provides a solid foundation for Atonomi's security protocol. Further, CENTRI's patented security software currently available and on the market for secure communication services, multi-layer crypto

key management, and fast indexing and searching of encrypted data is integrated into the broader Atonomi security protocol stack to enable the Atonomi Network to uniquely operate at the high speed required by IoT.

The Atonomi Network is integral to securing the IoT and its real world applications. For example, homeowners could register smart home devices with the Atonomi Network to validate devices on the premises and help eliminate the risk of hackers accessing personal information. Within industrial IoT, the Atonomi Network can protect against hackers gaining control of the sensors, controllers, and other devices that regulate the operation of essential infrastructure, such as hydroelectric dams and utility grids. To unleash the power of IoT, cybersecurity is required.

Table of Contents

Table of Illustrations

1.0 Introduction

"Secure interoperability is essential for the Internet of Things to reach its full potential. The Atonomi blockchain technology vision for a global service that enables secure transactions and commerce through device identity and reputation is something Arm is excited to see realized."

- Ian Ferguson, VP Ecosystem Development, IoT Services Group, Arm

The Atonomi Network is designed to secure the Internet of Things.

That is, there are billions of IoT devices already deployed today and billions more coming. Gartner, the U.S. research and advisory firm, estimates there are already some 8.4 billion IoT devices deployed in the world as of 2017, up 31 percent from 2016, and further projects the number of IoT devices to increase to 20.4 billion by 2020,[1] with 5 million new IoT devices deployed each *day* in 2016.[2] Billions of connected devices will propagate between a quadrillion and sextillion of transactions of data and/or commerce over time.

Adding to the scale of IoT is the emergence of autonomous device-to-device commercial transactions and microtransactions, which are expected to play a growing role in how our world functions. As IoT becomes more robust, so will the interactions between devices, creating the need for devices to autonomously conduct transactions—such as devices in the field negotiating for and purchasing (using digital tokens) bandwidth, electric power, and other resources to most efficiently function.

As the growth in devices and their associated transactions become foundational to our lives, it could present increasing substantial security threats. The global IoT represents a huge attack surface for criminals and other bad actors, and IoT devices often exist outside the protective barriers of corporate firewalls and lack the computing and storage resources to host traditional security software. The need for security further intensifies as more and more IoT devices are given the ability to autonomously engage in financial transactions, as hackers and other bad actors could be attracted to the idea of devices having access to wallets and look for ways to digitally steal funds.

These potential security threats are a concern for everyone from homeowners to businesses, to municipal, state, federal, and international government agencies. For instance, IoT devices have already been hacked and harnessed for denial-of-services attacks, including the 2010 Stuxnet attack on an Iranian nuclear facility, and the 2016 Mirai botnet attack that disrupted U.S. Internet traffic. IoT-based attacks have also targeted Netflix, Twitter, the BBC, and other organizations, including a university that suffered a DDOS attack launched through one of its vending machines.

---

[1] https://www.gartner.com/newsroom/id/3598917

[2] https://www.gartner.com/newsroom/id/3165317

Gartner placed security at the top of its list of the top 10 IoT technologies for 2017 and 2018: "The IoT introduces a wide range of new security risks and challenges to the IoT devices themselves, their platforms and operating systems, their communications, and even the systems to which they're connected. IoT security could be complicated by the fact that many 'things' use simple processors and operating systems that may not support sophisticated security approaches."[3]

1.1 The Need for Device Identity & Reputation

The ability to establish IoT device identity and reputation is essential to enable the secure interoperability between devices without the need for human intervention. Such a service could prevent unintended consequences from hackers attempting to disrupt critical systems or benefit economically from actions that have become common in traditional computer networks.

Immutable device identity, much like our own fingerprints, can be obtained from the device through a function commonly referred to as root-of-trust, using either hardware or crypto certificates. Once the device identity is established, it can be written to the blockchain as a permanent record.

Device reputation would evolve over the lifetime of the device, much like personal credit scores. The device's dynamic reputation can also be written on the blockchain for public review. This provides for both a method to establish risk rating for the device and, in the event the device is compromised by hackers, the reputation could be set such that the device can no longer effectively function.

Validating device identity and managing reputation provides a foundation for securing the IoT as diverse application developers build on top of the Atonomi Security Protocol.

1.2 The Right Technology

Blockchain uniquely solves for fundamental vulnerabilities in data security, particularly focused on central authorities for data storage and access control rights, by bringing a decentralized architecture and consensus security protocol to the IoT space. As such, the Atonomi Network is able to establish an immutable digital identity for every device on its network using a decentralized architecture and consensus mechanism. In addition to a trusted device identity, blockchain also enables secure and immutable management of a device's reputation throughout its life. Moreover, as more devices begin to use the Atonomi Network for secure, trusted interoperability, network effects attract additional devices enabling the machine-to-machine economy to flourish. Further, Atonomi envisions a world where blockchain technology allows humans to confidently govern autonomous devices through not only identity and reputation, but also smart autonomous contracts.

The ability of blockchain to scale to meet the transactional demands in the IoT space is an area in which Atonomi is keenly focused. Our architecture combines on-chain and off-chain resources to enable IoT to operate at scale. Further, as part of the Ethereum community, Atonomi intends to support, and to encourage other members of the peer-to-peer Atonomi Network to support and adopt, scaling solutions as they become necessary for the health of the Atonomi Network such as Plasma, Raiden, Sharding and Swarm, as well as alternative solutions currently in development.

---

[3] https://www.gartner.com/newsroom/id/3221818

1.3 How Atonomi Differs from Other Proposed Solutions

While the need for IoT security has triggered increased development efforts, many other proposed IoT solutions are incomplete or based on poor security designs. For example, many proposed solutions ignore blockchain, thereby lacking immutability while representing a centralized single point of failure. While others use blockchain, they have a limited and specific application-based focus, and lack interoperability, extensibility, and the need for establishing immutable identity and reputation tracking.

Atonomi's solution provides the following:

- **Low-level protocol for secure IoT**. Atonomi enables secure transactions between IoT devices through our blockchain-based Identity Registry, which establishes root-of-trust using encrypted whitelist data from participating OEMs/ODMs providing unique device identity and a public key for each device to be validated onto the Atonomi Network. Atonomi uses the Ethereum blockchain as part of our decentralized solution. Others generally don't address the critical element of security nor leverage the immutability of blockchain technology.

- **Trust and Reputation**. Trust and reputation are essential for autonomous devices to engage in transaction of data and value, and are part of the Atonomi Network design, including our Reputation Tracking service. Reputation tracking allows for automated identification of, and action against, rogue or compromised devices. Many other proposed solutions lack the capability of identifying and revoking access for untrusted devices, something that the Atonomi Network design addresses. Also, others leave the critical elements of trust and reputation to be handled by third parties, or simply omit them in their solutions.

- **Existing IoT Security Market Leadership**. IoT devices typically have limited computing, storage, power, and bandwidth resources. Atonomi's parent company CENTRI has pioneered the precision coding and engineering required to provide security solutions—with a footprint measured in kilobytes, not megabytes—for deployment in even the most resource-constrained devices. This past experience is being leveraged and deployed in the Atonomi Network, which accommodates the fact that autonomous devices, through multiple unique IoT stakeholders will need to negotiate new relationships, negotiate data structures, and interact. In contrast, some IoT solutions require participating devices to perform computationally complex peer-to-peer functions or simply require too large a footprint to be useful across any but the more powerful IoT devices.

1.4 Building Upon Years of CENTRI's IoT Security Experience

CENTRI Technology (www.centritechnology.com), the parent company of Atonomi, was formed as a technology transfer out of the University of Mississippi to address the growing cybersecurity need for data protection and optimization. CENTRI has been recognized as a leading provider of data security for the Internet of Things by technology research firms Frost & Sullivan, Gartner Research, and others.

CENTRI's patented security technology—currently available and on the market—is integrated into the full Atonomi security protocol stack to enable its solution to uniquely operate at the high speed required by IoT. As a result, the Atonomi product has a unique and competitive technical advantage over others that may offer an alternative IoT security platform. The technologies developed by CENTRI are protected by 10 issued patents and an extensive patent portfolio roadmap. Three of the technologies are integrated into the Atonomi services layer of its full protocol are:

1. Secure Communication Services—a lightweight communications protocol able to create a secure session in 3 milliseconds on average
2. Multi-layer crypto key management—a scalable crypto key management methodology that enables decentralization of encrypted data without centralized key management
3. Fast indexing and searching of encrypted data a method of searching and retrieving decentralized encrypted data without knowledge of the data storage

These technologies and others developed by CENTRI provide Atonomi with advanced data security capabilities to protect decentralized data and enable the scale and transaction speeds necessary for IoT.

CENTRI's data security products have been used successfully by leading technology companies, including: Arm, Flextronics, and Intel. This track record demonstrates that CENTRI's data security technology, as incorporated in the Atonomi Network, could be a powerful and effective technology for protecting the data of many IoT devices.

2.0 Proposing a new IoT Ecosystem with Trust at the Core

"Connected devices that think, transact and exchange sensitive and confidential data are the next evolution of IoT. There are a few impediments that must be overcome prior to the full utilization of this hugely disruptive technology. Initiatives like Atonomi which are marrying essential concepts of trust, identity, autonomy and security show great promise, and I look forward to using their platform."

- Gary Conktight, Chairman, CEO and Co-founder, physIQ

2.1 Service to Establish Identity

Trusted identity provides a level of insurance necessary for IoT device to exchange information, enable actions and buy and sell products and services. IoT device manufacturers and solution providers have a vested interest in securing the products they sell. The starting point for the root-of-trust (the lowest common denominator for device identity) begins with the device manufacturer. New manufacturers in the Atonomi Network are screened by existing members of the network and then provided with a unique manufacturer identifier used when registering devices submitted to the network. This screening process is used to assess their cybersecurity best practices and assign a default reputation score to the manufacturer. The process of qualifying the manufacturers

and assigning scores to their devices ensure the integrity of the network. This is an essential step to prevent rogue and hacked devices from entering the network.

Trusted manufacturers submit their list of devices through a whitelist (a list of devices that are known and trusted by the Atonomi Network) to the Atonomi Identity Registry service. The Identity Registry service is the Atonomi consensus service that validates the integrity of the whitelist. Select manufacturers of the Atonomi Network will run an instance of a limited number of Identity Registry servers. These manufacturers are highly qualified and trusted to maintain the integrity of the network. As the Atonomi Network expands, the Identity Registry servers will publish to secondary Identity Registry servers. The role of the Identity Registry servers are to ensure the whitelist is properly formatted, submitted from a trusted device manufacturer and all metadata in the whitelist is consistent with the manufacturer's profile maintained on the Identity Registry blockchain. Once registered, the device is known and trusted by the Atonomi Network and now ready for the device owner to activate the device when placed in service.

2.2 Protocol and System to Manage Reputation

Once device identity is established, the reputation of devices must be managed in order for secure interoperability to exist. A device's reputation consists of its unique behavioral signature representing varying degrees of security, commercial, social and service quality measurements as an example. The Atonomi Network enables registered devices to validate a device's reputation stored on the blockchain to establish trust before exchanging data or commerce.

Within a marketplace, there will be a provider and requester (of information/data and/or services). The device requesting services will be able to submit a request to the marketplace and the device providing the service will respond to the request. If the devices have a reputation score that verifies them as known trusted per the reputation auditors and the device manufacturers, the transaction can proceed. If the authorization for transaction has expired, then the devices initiate another request for validation of the peer device from the Atonomi Network.

Atonomi's reputation protocol is a key enabler of a future consisting of trusted devices securely interacting in an autonomous manner. If a device begins to operate outside of predetermined parameters, auditors write low reputation scores to the device reputation data store and other devices can refuse interactions. Conversely, if an autonomous device has developed a positive reputation for effectively servicing others, the reputable device may attract more business as a service provider and might be able to increase its pricing for service. Reputation data is collected, stored and managed by a distributed network of Audit partners. Audit partners are paid through fees with Atonomi Tokens, to track device behavior on the Atonomi Network in order to score the reputation of each device, analogous to a FICO score but with the parameters for the machine economy. Scores are vectors with both magnitude and direction, similar to how FICO scores with a number (e.g., 740) and a direction (credit worthiness). Reputation scores can also relate to nonfinancial information such as a device's trustworthiness with respect to posting on social media or on reporting accurate weather, health data, and more.

2.3 Token to Facilitate Services in the Atonomi Network

Atonomi intends build a global ecosystem to enable the secure, trusted interoperability of IoT devices through identity and reputation. As such, Atonomi is introducing the Atonomi Token for participants of the decentralized ecosystem to transact with each other. The Atonomi Token is used by the Atonomi Network for device registration, activation, reputation management and commerce transactions. Key participants such as OEM/device manufacturers, distributors, device owners and auditors are anticipated to seek Atonomi Token rewards for participating in the Atonomi Network.

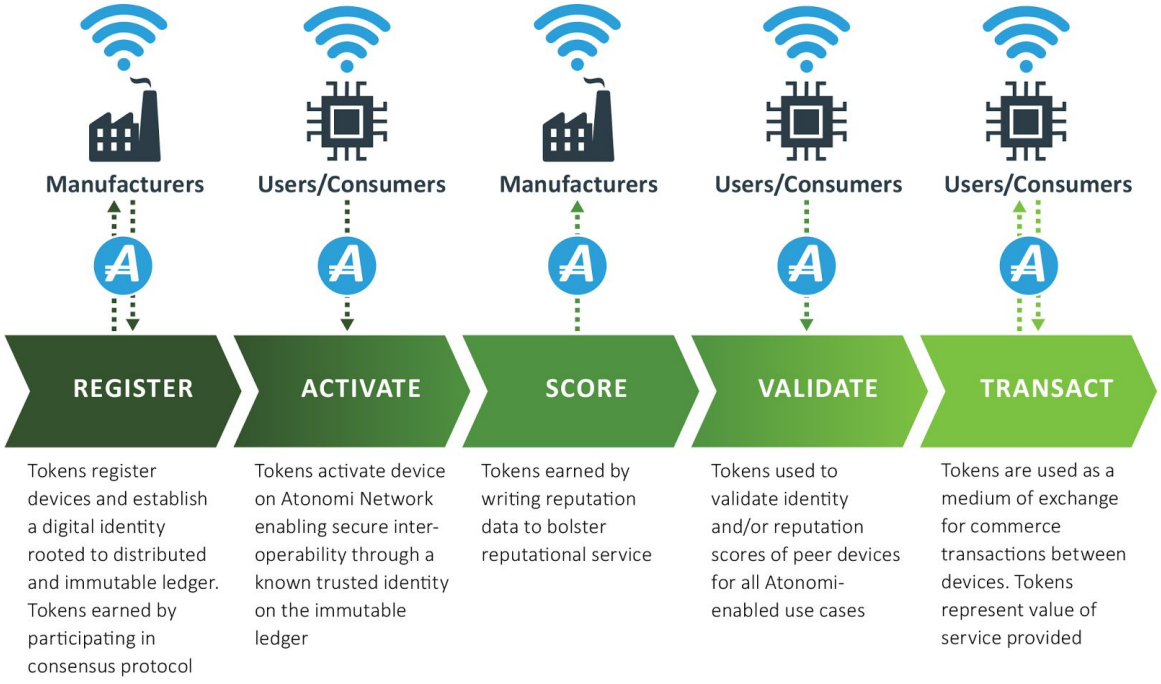

Figure 1. *Atonomi Token.*

The Atonomi Network relies on the Atonomi Token in order for it to function: the token acts as a utility to operate the Atonomi smart contracts, serves as a digital unit of value that can be used to facilitate the operation and expansion of the system by its ecosystem participant; and as our architecture tokenizes the identity and reputation management of devices on the Atonomi Network, it drives continually increasing ecosystem participation.

2.4 Extensible Architecture to be Built Upon

The Atonomi Network has been designed for others to build upon and extend the services to meet the additional needs of new and existing market segments. The security protocol and infrastructure of the Atonomi Network provides the essential identity and reputation security to enable third-party services with device trust and reputation. The Identity Registry and Transaction Ledger can be integrated into services such as healthcare, industrial IoT, and home automation to enable devices

from different manufacturers to interoperate without the complexity of custom API development or the security risks associated with open communications between unknown devices.

A third-party service provider could extend their solution by using the Atonomi Network to validate the device identity and reputation before a transaction occurs. The devices in the transaction, once validated, could save specific transaction and metadata plus Atonomi identity and reputation data within their private database or submit the transaction to another third-party public blockchain. These transactions create an immutable record between trusted devices that provide a level of certainty not possible before. Getting security right has proven to be difficult for companies and experts focused on cybersecurity. Through the extendible architecture of Atonomi, non-security experts can build upon a network with the certainty of the device identity and reputation.

3.0 The Atonomi Network - Technical

The Atonomi Network is designed to validate device identity, provide extensible capacity for leveraging device reputation in transactions, and provide protocol hooks for recording arbitrary device transactions. Further, the Atonomi Network provides an SDK to facilitate OEM integrations for device and device reputation lookup. By recording lookups and metadata about subsequent transactions sent through software services that are called from the SDK, the Atonomi Network serves an additional role as an auditor.

Devices performing anomalous lookups will have their reputations downgraded and those which continuously display ordinary performance will have their reputations upgraded. The Atonomi Network's use of the public Ethereum blockchain is intended to ensure the permanence of Atonomi functionality, providing security for IoT devices into the foreseeable future. The Atonomi Network includes the Atonomi Token, which is a utility token used to activate devices onto the Atonomi Network and can also be used for secure device-to-device commercial transactions.

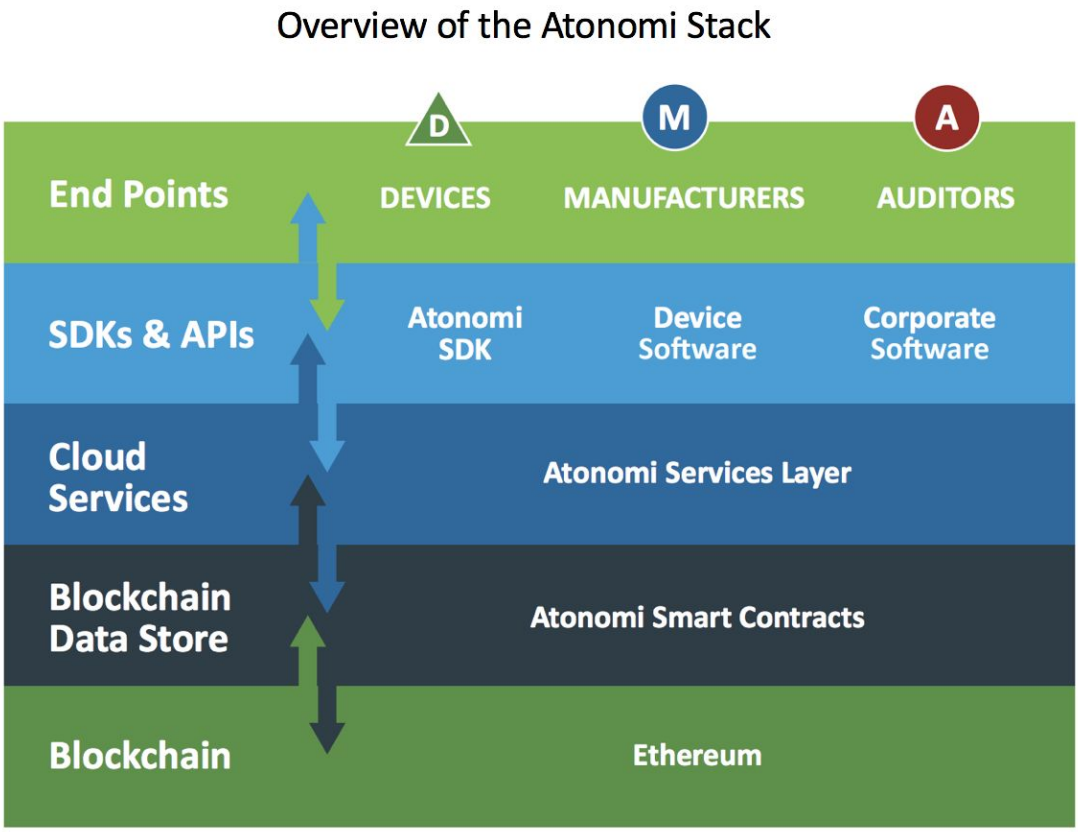

Figure 2. *Overview of the Atonomi Stack.*

3.1 Atonomi Smart Contracts

The Manufacturer Registry is a smart contract which can only be written to by Atonomi and participants in the consensus network. Atonomi and its consensus partners will add partner manufacturers to this registry and maintain their state. Each smart contract lists data tuples referenceable by public unique identifiers. In this way, the Identity Registry can be conceptualized similarly to a relational database (see Figure 2). Write control to these smart contracts is strictly maintained by whitelists controlled by Atonomi. Read control is maintained by encrypting or salting and hashing data in order to obfuscate the data from arbitrary third parties. The Atonomi Network includes a metadata field in each tuple for extensibility.

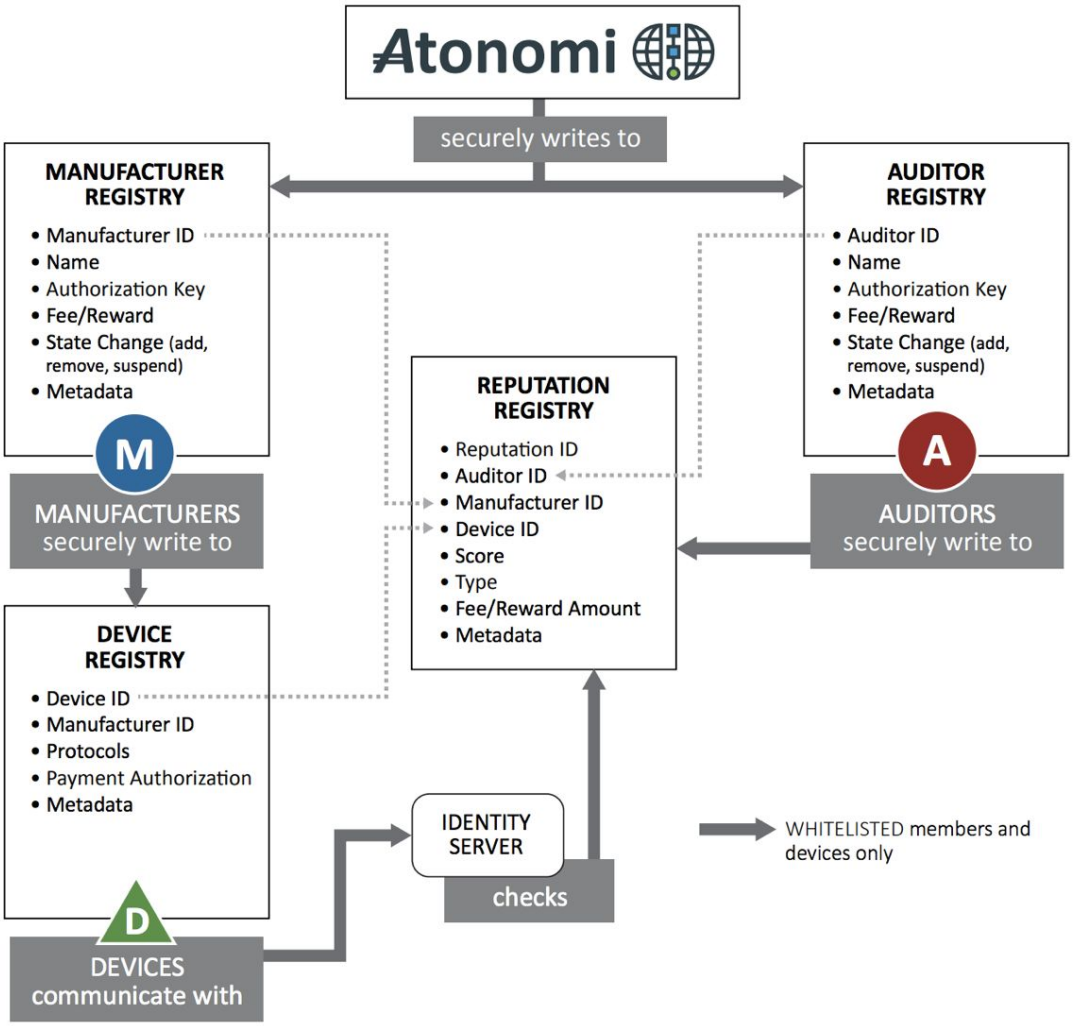

Figure 3. *Architecture describing the different smart contracts and how they interact with each other and external devices and services.*

3.1.1 The Manufacturer Registry

The Manufacturer Registry is a smart contract which can only be written to by Atonomi. Atonomi will add partner manufacturers to this registry and maintain their state. Each tuple in this registry contains a unique id, a human readable name, a salted and hashed authorization key, a field maintaining the fee or reward of Atonomi Tokens collected from or distributed to this manufacturer when the manufacturer adds new devices to the registry. The smart contract allows Atonomi to Add, Remove, or Suspend a partner manufacturer.

3.1.2 The Auditor Registry

The Auditor Registry is a smart contract which can only be written to by Atonomi. Atonomi will add partner auditors to this registry and maintain their state. Each tuple in this registry contains a unique id, a human readable name, a salted and hashed authorization key, a field maintaining the fee

or reward of Atonomi Tokens collected from or distributed to this manufacturer when the manufacturer adds new devices to the registry. The smart contract allows Atonomi to Add, Remove, or Suspend an audit partner.

3.1.3 The Device Registry

The Device Registry is a smart contract which can only be written to by authorized manufacturers listed in the Manufacturer Registry. Writing an entry to the Device Registry may require or award Atonomi Tokens based on the appropriate entry in the Manufacturer Registry. In this way, tokens can be used to facilitate participation in accordance with maintaining a healthy network and can be thought of as a license for participation. Each tuple in the Device Registry will contain a unique identifier, a reference to the unique identifier in the Manufacturer Registry, a field listing protocols the device supports, and an optional reference payment authorization identifier.

3.1.4 The Reputation Registry

The Reputation Registry is a smart contract which can only be written to by authorized auditors listed in the Auditor Registry. Writing an entry to the Device Registry may require Atonomi Tokens to update the ledger for the Manufacturer Registry. In turn, participating consensus partners can earn token rewards for validating entries to the Manufacturer Registry. In this way, Atonomi Tokens can be used to facilitate participation in accordance with maintaining a healthy network and can be thought of as a license for participation. Tuples in the Registration Registry maintain a unique identifier, a reference to the auditor who wrote the entry, a score stored as an unsigned 32 bit integer (capable of storing a value from 0 to 2,147,483,647), a reputation type, and a reference to a device ID or a manufacturer ID. Reputation types are plain text that auditors determine. For example, a particular auditor might maintain a financial reputation (trustworthiness of the device for purchases in a given price range) for a given device as well as a social reputation (trustworthiness of the device to make social media posts on behalf of its owner).

3.2 The Atonomi Token

The Atonomi Token, which functions in compliance with ERC-20 standards, is a utility token used to register devices onto the Atonomi Network during the device registration process and to write reputational data to the network. As noted earlier, the Atonomi Token can also be used as a reasonable default for secure device-to-device commerce between devices registered onto the Atonomi Network. Moreover, the token serves as a reward mechanism to facilitate and attract ecosystem participants to the Atonomi Network.

3.3 The Atonomi OEM/ODM SDK

To simplify manufacturer and auditor interactions with the Ethereum blockchain, Atonomi includes shared-source services for all of the described interactions with the smart contracts and provide SDKs for free to OEMs and ODMs to allow them to easily participate in the Atonomi Network. Atonomi provides sample code and an SDK for OEMs and ODMs to use in embedding basic device wake-up and handshake code for devices to use upon initial activation. The embedded code directs the device to the Atonomi Network where its unique device identity and private key is matched to the whitelist data stored on the Identity Registry blockchain. These SDKs rely upon services run by the Atonomi

Network in order to further facilitate connections between manufacturer data centers, IoT devices, and the Ethereum blockchain.

3.4 Reputation Registry

Reputation is tracked for each device and can also be tracked for device owners, or devices sharing a common wallet. Reputation provides an additional layer of security, enabling misbehaving devices to be decremented to the point of exclusion. Reputation can also be used as a qualifying element in transactions. Reputation can be based on a number of factors (customizable to meet the needs of different verticals) including: device performance, service delivery, device owner, device manufacturer. Advanced reputation management capabilities could be informed by emerging AI and machine learning.

3.4.1 Atonomi's Audit and Reputation Service

While the Atonomi Network and security protocol are designed to support any number of 3rd party auditors who can analyze their partners devices and those devices' transactions, the Atonomi Network also serves as an initial auditor and Reputation service provider. The OEM SDK includes calls to Atonomi service layers to record transaction logs when devices are registered, activated, and perform lookups to the Atonomi Network. The SDK supports the easy addition of other network calls to support the sending of high granularity device-specific log data to third party audit services as specified by manufacturers.

As part of ongoing development contributions, Atonomi intends to bootstrap the network with reputational data based on manufacturer security best practices. The Atonomi Network will dynamically adjust device reputation based upon artificial intelligence-based analysis of device-to-device behavior. Transaction logs are stored within the Atonomi Network where design classifiers will identify aberrant behavior and modify device reputation accordingly.

.

3.5 Atonomi Services

The Atonomi Network is intended to include a number of cloud-based services intended to make it simpler for OEMs to embed Atonomi functionality into their devices.

3.5.1 Identity Registration Service

The Identity Registration service of the Atonomi Security Protocol is designed to interact with devices seeking to validate to the Identity Registry. The Identity Registration service handles key negotiation and validation of unique hardware identification against the OEM/ODM-provided whitelist. Upon validation, the service sends an ADD function to the Identity Registry blockchain with unique device identification and other metadata. Once a given device has been added to the registry it cannot be re-added, preventing its credentials from being reused. Each validated device may be associated with a transaction authorization, such as a wallet with a public-private key pair associated with it. Similarly, devices may be de-registered or suspended as needed. This service is dependent on an appropriate number of Atonomi Tokens being transferred between transaction service providers.

3.5.2 Device Activation Service

The Device Activation service supports device ownership transfer with the validation of public/private key pairs and encrypted unique device identifier from the OEM/ODM whitelist to activate new devices onto (or reject invalid devices from) the Device Registry. Additionally, this service can generate validation failure alerts to external services in order to provide notifications to relevant parties. After successful identity validation and activation of the device into the Atonomi Network, the transaction authorization/wallet associated with the device, generally that of the device owner or an organization's IoT network manager, is decremented a partial Atonomi Token amount.

3.5.3 Attributes Registration Service

The OEM/ODM stack provides APIs for integration with a manufacturer's existing device application stack where attributes and other user-defined metadata are assigned to devices. The Atonomi Transaction Validation service provides metadata as part of its transaction permissioning.

Attributes could include:

- Per-transaction spending limits
- Transactions per-minute (hours or days) spending limits
- Geographic limitations on transactions
- Counter-party reputation requirements
- Attributes can also be ascribed for non-financial transactions, for example:
- Data exchange only with Identity Registry-validated devices
- Data exchange with any device
- Data exchange with any device within scope of geofencing
- Whitelisted smart contracts can receive payments from a device used as a gateway/firewall for additional auditing and permissions purposes

The above attributes aren't intended as a complete list, but as an example of the ways in which device owners can use the OEM/ODM application stack to ascribe attributes which will have meaningful use for their own vertical and specialized needs.

3.5.4 Transaction Service Creation and Maintenance Services

The OEM stack supports use of existing—or creation of new—digital wallets or related transaction authorizations for devices that may need to support commercial transactions. Transaction authorizations or wallets can be created by device owners on either a device-by-device basis, or on a department-wide, company-wide, or other group basis. Atonomi intends to work with third-party services to support credit card and bank account authorizations. Atonomi Token-compatible wallets will be used to store Atonomi Tokens which will deduct a small percentage for some transactions taking place over the Atonomi Network. Wallet creation isn't required for devices not anticipated to be involved in commercial transactions and not performing charged transactions in the Atonomi Network. Should a need for a wallet later arise, device owners can return to the OEM/ODM device application to create a wallet.

3.5.5 Device Ownership Transfer Service

The Atonomi Network will support ownership transfer of IoT devices—with or without wallet contents. Upon device transfer, a transaction log entry of the transfer will be broadcast to the Atonomi

Audit service which will incorporate this data into its artificial intelligence models and update device reputation as needed.

3.5.6 Reputation Writing and Lookup Services

The Atonomi Network will maintain a cloud-based service that may be optionally incorporated into device software by OEMs to facilitate lookup of reputational data prior to engaging in peer-to-peer transactions. Atonomi also maintains services to write to the Reputation Registry for whitelisted auditors.

3.5.7 Transaction Validation and Facilitation Services

The Atonomi Network maintains services to facilitate off-chain inter-device transactions (especially commercial transactions). The data from these services are used for reputation analysis. The extensible nature of the Atonomi Network OEM stack means that different verticals can define which non-commercial transactions are stored off-chain. Atonomi Tokens may be a useful default token for inter-device commercial transactions. Though Ethereum network transaction processing might become cost- or speed-prohibitive, we believe the network is sufficient for immediate use. If and when necessary to maintain a healthy ecosystem, Atonomi and members of the Network will evaluate migration or simultaneous use of alternative blockchain technologies for these transactions, such as Ethereum Raiden, Plasma, HashGraph, or others.

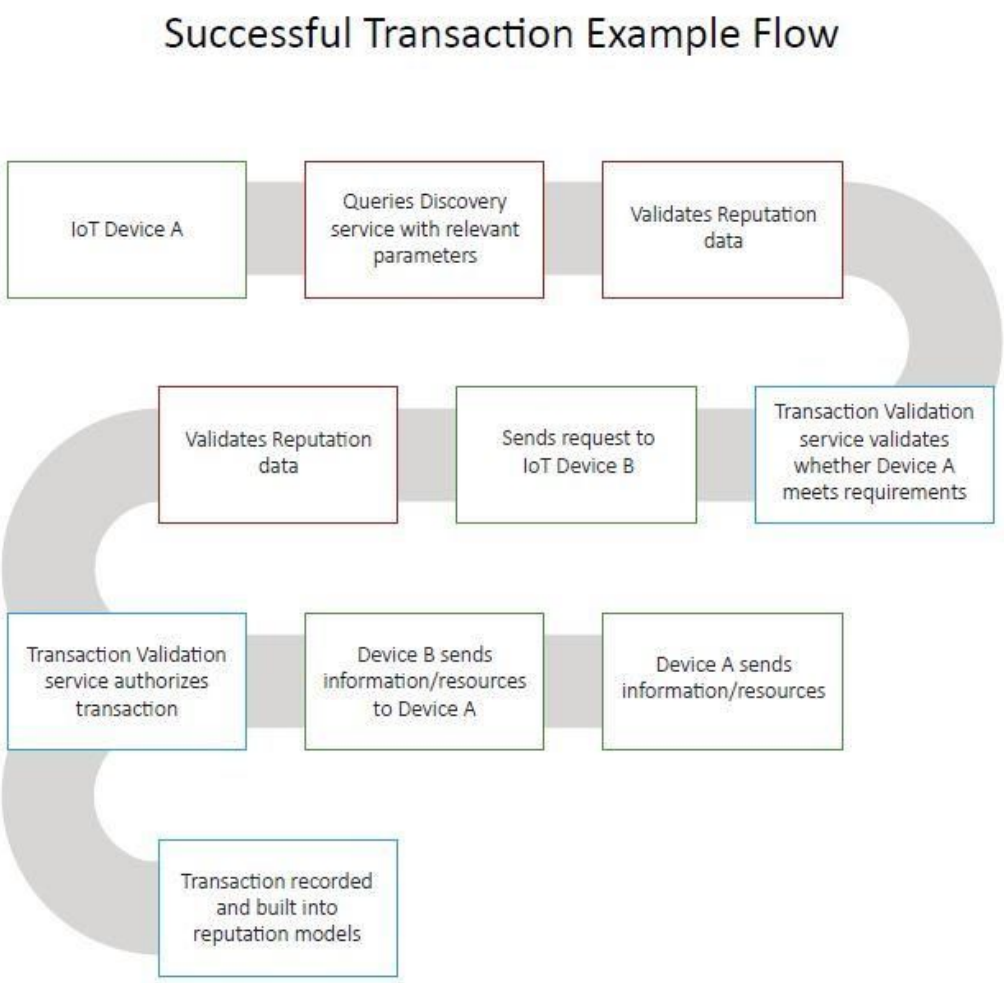

Figure 4. *Transaction Validation Service.*

3.5.8 Service Discovery Service

Atonomi's Service Discovery service allow devices to connect to Atonomi's database of services provided by other devices and return a device ID from the Identity Registry. A device seeking to locate electricity for purchase, for example, can query this service with its requirements. A list of device IDs and relevant information about the services available will be returned alongside relevant reputation data. Service-specific metadata is cataloged based on device- and manufacturer-specific metadata registered with the device in the Identity Registry.

3.6 Scalability

The proposed architecture leverages centralized cloud services scalable through traditional means as well as the Ethereum public blockchain. We recognize industry-wide concerns about the scalability of the Ethereum blockchain and will benchmark and forecast key performance metrics to ensure that our services and protocol can serve the necessary use cases. Note that many of the operations we

support do not require high throughput writes to the blockchain. We will continue to monitor new developments in the space and prepare a migration path if and when scalability becomes a significant concern.

4.0 Faster and More Secure Services Stack

Integrated into the services stack of the Atonomi solution is the Centri IoTAS technology. As device performance and blockchain data security are essential elements to secure IoT, the Atonomi Agent includes advanced security technology developed by CENTRI. Atonomi has integrated the high speed communications technology described below to allow IoT devices to operate at real-time data speeds. Further, data posted to the public blockchain is protected by multi-layer crypto key management to allow devices owners and Atonomi Auditor Server to analyze device transaction history without exposing the data to public review.

4.1 Fast and Secure Authentication

CENTRI IoTAS has a process for assigning secure device identifications upon registering a new device into an IoT environment. This allows for immediate, and encrypted, single-stage handshake communication between IoT devices using the CENTRI Secure Communications library, and the Cloud infrastructure side using the CENTRI Secure Communications Service. With CENTRI IoTAS, there's no need to exchange certificates or employ a third-party certificate authority solution. We plan to use technology similar to our security-enhancing single-stage handshake within our OEM stack for guiding initial contact between a newly activated device and our Identity Registry.

4.2 Small Footprint

The CENTRI IoTAS platform has a minimal footprint, making it easy to embed the code into applications. IoTAS only requires about 16 kB of RAM for efficient performance on typical IoT devices. CENTRI developed "vault-less" technology—a patented process to embed key seed information within the data, to eliminate the need for hardware key storage systems. The seed data used to generate each one-time key is protected with asymmetric encryption. The result is unlimited key management, which is essential for IoT security to scale. Our experience in creating tight code and embedding key seed data will inform our creation of the small code footprint of our OEM stack, which we see as essential for integration with IoT devices that can be resource-constrained.

4.3 Device Agnostic

Developers can use the C-based libraries and tools across a spectrum of operating systems, including Android, iOS, Windows, Linux, RTOS, and custom network stacks and other code organizations might want to use in creating IoT solutions. Atonomi uses this same device agnostic approach in creating an open and extensible development platform that can be customized to the exacting needs of different verticals.

4.4 Secure Data

The CENTRI IoTAS technology protects data during transport, in use, and at rest through standards-based, leading edge cryptography, including Elliptic Curve Diffie-Hellman Cryptography

(ECDH) 25519, Salsa20 Symmetric key cipher data encryption, and SHA-512 cryptographic hash function for key derivation. Atonomi will be guided by this same approach to protecting data with leading-edge cryptography.

4.5 Intellectual Property and Patents

CENTRI's IoTAS is protected via multiple patents:

- Single-Pass Data Compression and Encryption, U.S. Patent 8,886,926 which compress and encrypt data in a single pass to reduce inefficiencies that occur from compression and encrypting data separately.
- Single-Pass Data Compression and Encryption (Broadening), U.S. Patent 9,503,434
- Seeding of a Workspace to Optimize CODEC Operations, U.S. Patent 8,804,814 which improves codec performance by seeding the computation workspace that may be used by various codec processors.
- Seeding of a Workspace to Optimize CODEC Operations (Broadening), U.S. Patent 9,025,657
- Secure Storage for Shared Documents, U.S. Patent 9,298,940 which improves management of data storage for secure storage of shared documents, using an encryption key based on instruction set and header information.
- Secure Storage for Shared Documents (Broadening), U.S. Patent 9,584,321
- Transparent Denial of Service Protection, U.S. Patent 9,210,187 which uses instruction set information that references a seed file communicated to a client computer and a network packet key generated by the instruction set information encrypted and provided by a server.
- Transparent Denial of Service Protection (Broadening), U.S. Patent 9,503,262
- Fast Indexing and Searching of Encoded Documents, U.S. Patent Application 15/453,853
- Big Data Markers for Stream Labeling, Identification and Decoding, U.S. Patent Application 15/402,122
- Process for Distributing Computing Datasets, U.S. Patent applied for.

5.0 The Atonomi Secure IoT Ecosystem

"The number of connected devices are growing exponentially driving up the value provided by IoT solutions. The Atonomi blockchain initiative offers intriguing possibilities to secure this world of automated device-to-device transactions and exchange of data."

- Mrinalini Lakshminarayanan, Director of Products and Services, Gogo Inflight

An important part of securing IoT is building an ecosystem that is designed to maintain and expand IoT security and interoperability. Atonomi plans to accomplish this in multiple ways.

First, unlike other IoT security offerings, Atonomi begins at the source of the IoT value chain by embedding the Atonomi OEM Stack into the chip/OEM software code (see Figure 5). The chip-first

solution is relevant to the Atonomi architecture because the small number of chip manufacturers create the foundation for an end-to-end security protocol that could be widely used by smart device manufacturers, and then built on by application developers.

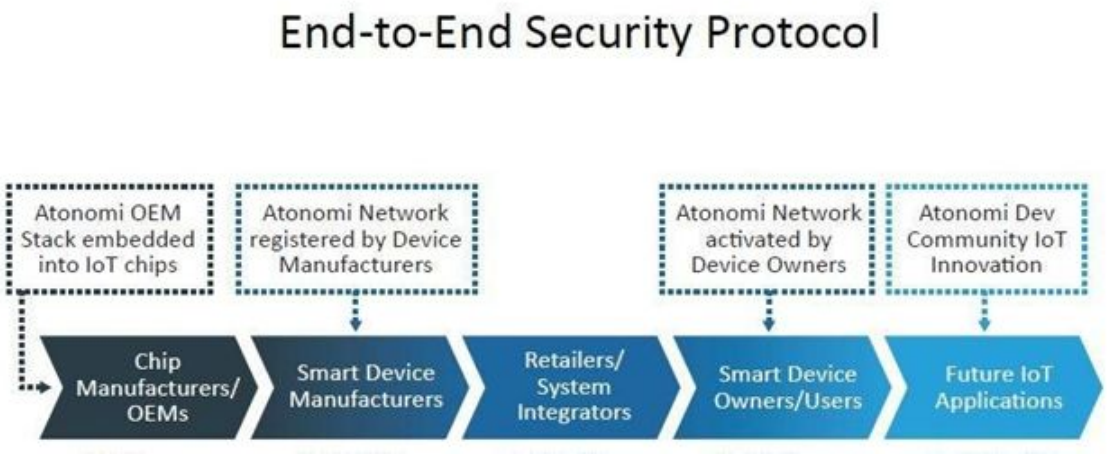

Figure 5. *Atonomi Network provides an end-to-end security protocol for the IoT value chain.*

Next, the Atonomi ecosystem is designed to serve as a decentralized network of IoT stakeholders who act as key participants in Atonomi's identity and reputation service. For instance, participants such as utilities, smart cities, industrial IoT participants, and OEM and device manufacturers may elect to audit data and publish reputation data, provide service layers to interact with Atonomi's smart contracts, or validate and process transactions between devices on the Atonomi Network. As a low-level protocol for secure IoT, Atonomi will also enable a community of developers to build the next generation of IoT applications and platforms. By securing the end points of IoT devices and facilitating trusted interoperability between devices, Atonomi solves the fundamental problem of security in IoT and facilitates an innovation hub for the dApp developer community.

The Atonomi Network is engineered to support extensibility. We provide known and trusted device identity and reputation, and other companies and organizations that will be able to extend the definition based on their own future needs. For example, builders of IoT devices for the HVAC industry may identify new transaction types, as could participants in IoT for industrial controllers, the power grid, agricultural devices, healthcare, retailing, shipping, and a world of other areas. Creating an extensible platform, open to all, will foster new—and secure—ways to derive benefit from the Internet of Things.

Audit partners are anticipated to seek fees in Atonomi Tokens to serve as validators on the Atonomi Network. For instance, a smart device such as an electric vehicle may enter into a service transaction with a charging station to recharge its battery. While Atonomi secures identity and reputation of these devices enabled by smart contracts, Audit partners (run by OEMs, Smart Cities, PwC, etc.) could validate this transaction and, in return, receive a reward fee in Atonomi Tokens.

Expanding upon CENTRI's established record in data security products, and building upon CENTRI's existing partnerships with Arm, Flex, and Intel, Atonomi intends to attract the key

stakeholders in the IoT value chain to facilitate adoption and participation in the Atonomi Network through business development and customer acquisition activities.

6.0 Atonomi Use Cases

According to Gartner, an estimated 5 million connected devices are being added per day to the IoT. The burgeoning IoT market can be viewed as a continuum, with early adopters that will over time drive future market opportunities. Atonomi seeks to be the standard low-level security protocol for the IoT industry. With a chip-first strategy, Atonomi intends to work with chip manufacturers who may choose to embed our software, which is the greatest possible leverage point in the ecosystem.

Below are applications that are of immediate relevance to potential users of the Atonomi Network. The healthcare, industrial, smart city and home device markets are considered to be current movers in the IoT space.

6.1 Early IoT adopters in Healthcare

Given the aging baby boomer generation and the many use cases IoT can provide for healthcare, the healthcare industry can derive substantial benefits from Atonomi Network products. For example, consider the case of adding Atonomi security into an IoT solution, used for a proprietary health application platform, which is then built upon by application companies creating connected monitoring products, analytics tools, trackers, and other innovations.

At the application level, for instance:

- An inventory sensor inside a hospital emergency room blood-storage appliance could autonomously order re-stocks of specific blood types from regional suppliers based upon existing inventory, anonymized electronic health record reports of scheduled surgeries, and day-of-week historical ER needs. This system could be secured with the Atonomi Network.
- A diabetic patient wearing an insulin pump could allow the pump to share anonymized blood chemistry data with researchers to advance the science, or with healthcare monitoring systems that could intercede to prevent adverse events. This system could also be secured with the Atonomi Network.

6.2 Innovation in Industrial IoT, Smart Cities, and Home Devices

Industrial IoT requires a secure ecosystem within which a wide array of device types can seamlessly operate together to help manage the consistent flow and monitoring of workflow across multiple processes. Additionally, industrial IoT devices often need to extend autonomous interoperability to include resources beyond the domain of the manufacturing facility. The result is a need for trusted identity, reputation, and the ability to ledger user-defined key events.

Regarding smart cities, municipalities are finding ways to employ automation to seamlessly connect IoT devices and resources to lower power consumption, reduce traffic congestion, enhance air quality, increase safety, and improve overall livability. IoT will be at the core of many of these efforts, and providing security across this broad array of attack surfaces will be essential.

Further, the IoT is already playing an increasingly relevant role in home automation, smart appliances, and an array of other devices designed to make life easier and more convenient. A consumer, concerned about Internet security, can requires all IoT devices within the home to be identity-validated and secure to help eliminate attack surfaces.

6.3 Supporting Diverse Use Cases

While particular industries might be early adopters, the Atonomi Network is architected so that diverse verticals are able to build using our protocol over time. Consider additional use cases to illustrate the ways security is required as a core building block of IoT applications, and the way the Atonomi protocol could be integrated into various third-part applications:

- An electric vehicle recharges its batteries from a charging station, autonomously conducting the payment transaction through the owner's electronic wallet. The vehicle **securely** negotiates for the lowest-cost power available, while the owner is spared the hassle of plugging in a credit card and paying a service charge.
- A home with solar panels and a wall of storage batteries could use an IoT device to **securely** sell excess power to a neighboring home with a smart meter looking for cheap power while running the clothes dryer.
- Moisture sensors in an industrial greenhouse could detect low soil nitrogen and **securely** transact with irrigation devices to add nitrogen from automated feeders.
- An office building with an IoT-equipped HVAC system could **securely** negotiate just-in-time electric power from local or regional providers based on availability, time of day, and lowest cost.
- A remote sensor **securely** negotiates just-in-time wireless services from a low-cost provider to facilitate periodic data transmission.

7.0 Atonomi Token

The Atonomi Token is central to the entire Atonomi Network. The use of a token is ideally suited to secure IoT devices, which typically have constrained memory and CPU resources, because the token can link the identity between the device and device owner through a crypto wallet. Devices can't be expected to carry a PCI stack for credit card purchases, nor are credit cards suitable for the kind of autonomous device-to-device micro-transactions required in many use cases which may involve purchases of less than $1 and in some cases less than one cent.

7.1 Tokenized Identity & Reputation

Atonomi Tokens serve as a multi-use token for the internal mechanics of the Atonomi Network. Specifically, when new devices are registered and activated on the Atonomi Network, Atonomi Tokens can be used as fees for creating a device's digital identity through the use of smart contracts. Additionally, tokens are designed to be a key component of Atonomi's Reputation Tracking service by enabling reputation data to be captured, analyzed and scored. Atonomi Tokens also enable devices to validate other device identities that are stored on the blockchain encountered throughout its lifecycle.

7.2 Commercial Transactions and Data Exchange

Atonomi Tokens can be used as a digital token to enable device-to-device autonomous transactions. Third-party tokens can also be used. This token-based economy enables devices to securely engage in peer-to-peer autonomous transactions. While Atonomi doesn't charge for data exchanges, Atonomi Tokens provide a digital token to enable devices to engage in commercial transactions with each other. For example, a smart meter on a home or building may autonomously negotiate with the power company or a micro grid to acquire electricity and pay for services using the Atonomi Token.

7.3 Processing Commercial Transactions

Atonomi plans to enable fees to be structured into the smart contract and blockchain-based transactions, including device registration, activation, validation of other devices, reputation management and commercial transactions. For instance, Atonomi may elect to charge a processing payment of 1% for handling commercial transactions between IoT devices. Nothing is charged for data exchanges. It is anticipated that these transaction fees would be shared between reputation auditors in relation to the auditing services they perform, and Atonomi.

7.4 Ecosystem Partners and Innovation

Atonomi anticipates that ecosystem partners will seek to participate in key functions on the network, including device registration, activation, validation of other devices, reputation management and commerce transactions. For instance, as explained above, device manufacturers may elect to serve as auditors to write reputation data to the reputation service, and receive Atonomi Tokens as a reward for their service to the network. Additionally, Atonomi Tokens may be used to attract new chip/device manufacturers and end users to the network through customer acquisition programs.

Lastly, as a low-level security protocol, Atonomi aims to unlock many new use cases and future innovations such as a marketplace for IoT commerce. The developer community can build on the Atonomi protocol to innovate new projects and service offerings leveraging the Atonomi Token as fuel for their initiatives. For example, Swytch.io is a new blockchain-based project intending to disrupt the energy market by democratizing access to electricity through encouraging local, micro-grid production. In this case, Swytch may leverage the Atonomi security protocol (and the Atonomi Token) to secure the end points on Swytch's network and enable trusted interoperability.

8.0 Leadership

Leadership for the Atonomi Network includes:

- Vaughan Emery, Founder and CEO
- David Fragale, Co-Founder and VP of Product
- Mike Mackey, CTO and VP of Engineering
- Dr. Luis Paris, Chief Scientist
- Andrii Zamovsky, Technical Development Partner

Advisors to Atonomi include:

- Dr. Paul Clippinger, Senior Advisor; MIT Media Lab
- Peter Kinnaird, Technical Development Partner; Ambisafe
- Dr. David Kravitz, Vice President, Crypto Systems Research at DarkMatter
- Dr. Ulf Lindqvist, Program Director at Stanford Research International (SRI)
- David Jevans, CEO, CipherTrace
- Rob May, CEO, Talla and Botchain

For brief biographies of our Leadership Team, please visit the Atonomi website.