Atonomi
For Trusted IoT

Authors

Vaughan Emery

Jason Gray

David Fragale

Contributors

Peter Kinnaird

Fil Capiral

Mike Mackey

Andrew Reading

James Stennett

Amy Skogen

Grant Fjermedal

Abstract

Atonomi provides a universal trust environment to enable billions of IoT devices to have trusted interoperability for data and commerce.

Atonomi registers the identity and reputation of devices on a blockchain-based immutable ledger. Atonomi accomplishes this by working with device manufacturers and other stakeholders facilitating an ecosystem of participants designed to maintain decentralized consensus for device identity and reputation. Combining on-chain and off-chain resources, and built on the Ethereum blockchain, Atonomi's architecture is extensible by developers across IoT verticals (for example, industrial IoT, healthcare, and smart cities) to help 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 and other bad actors to disrupt the services that are expected to control many aspects of our lives in the coming years.

Atonomi provides fundamental elements to enable interoperability and secure exchange of data and commerce at scale:

- Registration of immutable identity of devices through its device identity registration service.
- Reputation service to enable Atonomi and distributed third-party auditors to build systems to detect and deal with bad device actors.
- Token-based economy for the registration and activation of devices, facilitation of a reputation-scoring ecosystem among third-party auditors, and for transaction validation services.
- Fully extensible architecture designed for easy integration by vertical IoT application developers and manufacturers.

v0.9.4a

Atonomi leverages the experience of its parent company, Seattle-based CENTRI Technology. CENTRI is a provider in IoT data security solutions, with relationships with Arm, Flex, and STMicroelectronics.

The Atonomi trust environment is designed to be an integral part of securing the IoT and its rapidly growing world of applications. Homeowners, for example, can register smart home devices with Atonomi to validate on-premises devices and reduce exposure of personal information on their home network (e.g. online banking). Within industrial IoT, Atonomi reduces exposure to hackers trying to gain control of sensors, controllers, and other devices that measure, record and regulate the operation of essential infrastructure. Atonomi brings together the latest blockchain and cybersecurity technologies to create a trust environment to help safely unleash the power of IoT.

The information provided in this whitepaper is provided for illustrative and descriptive purposes only, and is subject to modification by Atonomi in its sole and absolute discretion.

Table of Contents

Table of Illustrations

1.0 Introduction

The Atonomi trust environment is designed to help secure the Internet of Things.

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 could propagate between a quadrillion and sextillion 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 securely and 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 interactions become foundational to our lives, it will present increasing and 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, because hackers and other bad actors will 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 its vending machines, smart light bulbs, and other campus IoT devices.[3]

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

---

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

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

[3] https://www.csoonline.com/article/3168763/security/university-attacked-by-its-own-vending-machines-smart-light-bulbs-and-5-000-iot-devices.html

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."[4]

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 adjusted accordingly.

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

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 consensus-based decentralized architecture to the IoT space. Atonomi records to the blockchain the immutable digital identity for each Atonomi-enabled device. In addition to recording trusted device identity, blockchain-based Atonomi also enables secure and immutable management of a device's reputation throughout its life. Atonomi envisions a world where blockchain technology allows humans to confidently govern autonomous devices and smart contracts secured through identity and reputation.

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 trust environment, to adopt scaling solutions as they become robustly available such as Plasma, Raiden, Sharding, Swarm, and other technologies currently in development.

1.3 How Atonomi Differs from Other Proposed Solutions

While the need for IoT security has triggered increased development efforts, 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 using blockchain have a limited and specific application-based focus, and lack interoperability, extensibility, and the ability to establish immutable identity and reputation tracking.

---

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

Atonomi's solution provides the following:

- **Low-level protection for secure IoT**. Atonomi enables secure interactions between IoT devices through our blockchain-based Identity Registry Network (IRN), which establishes root-of-trust using encrypted whitelist data from participating manufacturers using unique device identity and a cryptographic key pair for each device to be validated onto the Atonomi trust environment. 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 transactions of data and value, and are part of the Atonomi design, including our reputation tracking service. Reputation tracking allows for automated detection of, and response to, rogue or compromised devices. Other proposed solutions lack the capability of identifying and responding to untrusted devices, something that the Atonomi 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 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 or gigabytes—for deployment in even the most resource-constrained devices. This experience is integrated into the Atonomi Device SDK. 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 most powerful IoT devices.

1.4 Building Upon CENTRI's IoT Security Experience

CENTRI Technology (www.centritechnology.com), the parent company of Atonomi, was formed to address the growing cybersecurity need for data protection and optimization. CENTRI has been recognized as a leading developer of data security for the Internet of Things by technology research firms Frost & Sullivan[5], and Gartner Research.[6]

The following sections in this whitepaper provide additional detail regarding the purpose and functionality of Atonomi and the Atonomi Token. **Please note that the information provided in this whitepaper is provided for illustrative and descriptive purposes only, and is subject to modification by Atonomi in its sole and absolute discretion.**

---

[5] https://ww2.frost.com/news/press-releases/centri-earns-frost-sullivans-entrepreneurial-company-year-recognition-its-internet-things-security-solutions/

[6] https://www.prnewswire.com/news-releases/centri-technology-named-to-gartners-2013-list-for-cool-vendors-in-communications-service-provider-operational-and-business-infrastructure-207180691.html

2.0 Proposing a new IoT Environment 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 protection necessary for IoT devices to exchange information and engage in other transactions. IoT device manufacturers and solution providers have a vested interest in securing the products they sell. The starting point for the root-of-trust begins with the device manufacturer. Manufacturers participating in the Atonomi trust environment are assessed for their cybersecurity best practices and assigned a default reputation score for their devices. The process of qualifying manufacturers and assigning scores to their devices helps ensure the integrity of the network, and guards against rogue and hacked devices from entering the network.

Trusted manufacturers submit their list of devices, including a unique device ID and cryptographic public key for each device, to the Atonomi whitelist which is written to the blockchain, and referenced later during device activation. The registration service (covered in section 3.1) validates the integrity of the whitelist. Select manufacturers will run a limited number of Identity Registry servers. As Atonomi expands, the Identity Registry servers will publish to secondary Identity Registry servers. Once registered, the device is known and trusted by Atonomi and ready for the device owner to activate the device when placed in service.

2.2 System to Manage Reputation

Once device identity is established, the reputation of devices is managed to help ensure secure interoperability within the trust environment. A device's reputation consists of its unique behavioral signature representing varying degrees of security, commercial, and service quality measurements. The Atonomi Device SDK enables registered devices to validate a device's reputation, stored on the blockchain, to establish trust before exchanging data or engaging in 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 can initiate another request for validation of the peer device from the Atonomi trust environment.

Atonomi's reputation process 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, automated 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 will be collected, stored and managed by a distributed network of auditors.

Manufacturers can establish reward pools to encourage reputation monitoring by transferring Atonomi Tokens to the reputation function of the Atonomi smart contract, which rewards auditors for actively submitting device reviews. Manufacturers receive a part of the reward for maintaining reputable devices on the trust environment. The reward for submitting a reputation score is determined by the manufacturer of each device and pre-programmed into the reputation function of the Atonomi smart contract to facilitate autonomous execution of rewards. A device's reputation score is analogous to a FICO score but with 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).

The basic logic flow of reputation includes these steps:

- Device A interacts with Device B.
- Device A generates a transaction report about its interaction with Device B, sending it to the IRN.
- Device B generates a transaction report about its interaction with Device A, sending it to the IRN.
- A third-party reputation auditor collates transaction reports from the IRN and creates a new—or updates an existing—reputation score for each device and submits through the Atonomi smart contract for posting to the blockchain.
- The Atonomi smart contract issues Atonomi Tokens to the auditor, as well as to the manufacturer of the reporting device, pursuant to the parameters that were pre-determined by the manufacturer.

.

2.3 Token to Facilitate Services

The Atonomi Token is used by participants of the decentralized Atonomi trust ecosystem to transact with each other. The Atonomi Token is used by Atonomi for device registration, activation, reputation management and commerce transactions. Key participants such as device manufacturers, distributors, device owners and auditors are anticipated to seek Atonomi Tokens in exchange for their participation in the Atonomi trust environment.
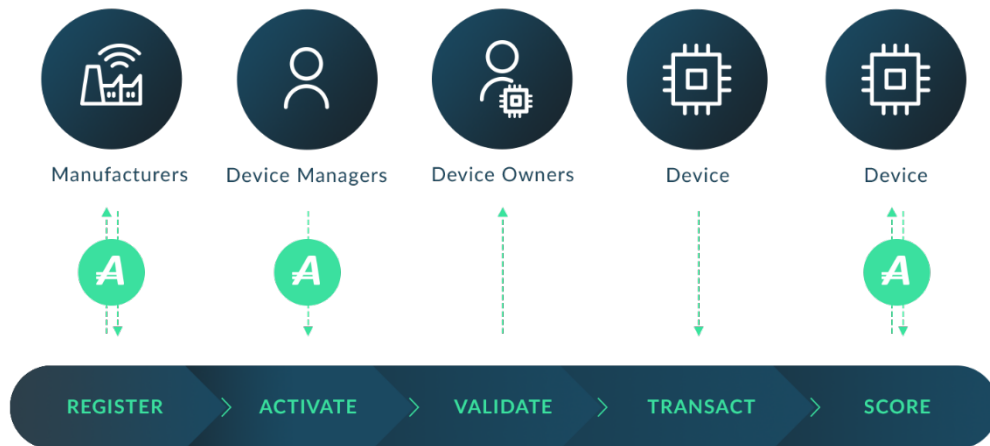
Figure 1. *Atonomi Token.*

Atonomi relies on the Atonomi Token to facilitate registration, activation, and reputation processes, Validation and transaction related services do not require Atonomi Tokens.

2.4 Extensible Architecture to be Built Upon

Atonomi has been designed for others to build upon and extend the services to meet the additional needs of new and existing market segments. Atonomi provides the essential identity registration and reputation tracking to enable third-party services with device trust and reputation. The Identity Registry 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 Device SDK 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 extensible architecture of Atonomi, non-security experts can build upon a network with the assurance of device identity and reputation.

v0.9.4a

139778950.10

3.0 Atonomi - Technical

Atonomi is designed to enable manufacturers to register devices with immutable, blockchain-based identity, enable users to activate registered devices, provide a mechanism for one Atonomi-enabled device to validate the blockchain-based identity of another participating device, and to assign and track device reputation. At the heart of all of these functions is the compact code of the Atonomi Device SDK.

Atonomi facilitates permanence of device identity and reputation by storing related data on the blockchain. Atonomi also incorporates off-chain components to support transactions at scale. This is intended to provide security for IoT devices immediately, while allowing flexibility for upgrades as distributed technology continues to develop. Atonomi includes the Atonomi Token, which is a utility token used to register and activate devices and provide reputation scores.

Basic elements of the Atonomi architecture include:

- Registration
- Activation
- Validation
- Reputation
- Atonomi Token

3.1 Registration

3.1.1 Overview

The Atonomi IRN identity registration is used to add manufacturers to the blockchain. Through registration, those trusted manufacturers can then register their devices to the Atonomi device whitelist, recorded onto the blockchain. Registration is driven by four components; device identity, registration service, manufacturer interface, and the registration function of the Atonomi smart contract.

3.1.2 Device Identity

Device identity is created during the device development or manufacturing process. The device developer or manufacturer registers the unique ID of each device onto the Atonomi whitelist, to be referenced later when the user activates the device with the IRN. The IRN uses device IDs, combined with the public key of an elliptic curve public/private key pair to activate the device.

3.1.3 Registration Service

The Atonomi registration service interacts with the IRN to register new Atonomi-enabled devices to the blockchain. Registration to the blockchain is required for later device activation by the user.

3.1.4 Manufacturer Portal

The device manufacturer interface is a graphical interface into the IRN where device manufacturers register devices with Atonomi before those devices enter the market. The interface is access-controlled, with credentials supplied to manufacturers that join Atonomi. The portal allows administrators to set up accounts for new member manufacturers.

3.1.5 Atonomi Smart Contract: Registration

The registration function of the Atonomi smart contract governs the writing of a new manufacturer member and its Ethereum address to the blockchain during manufacturer setup. It also governs the writing of new device IDs to the blockchain when the manufacturer adds new devices to the whitelist via the interface. It also facilitates the payment in Atonomi Tokens for the registration of devices.
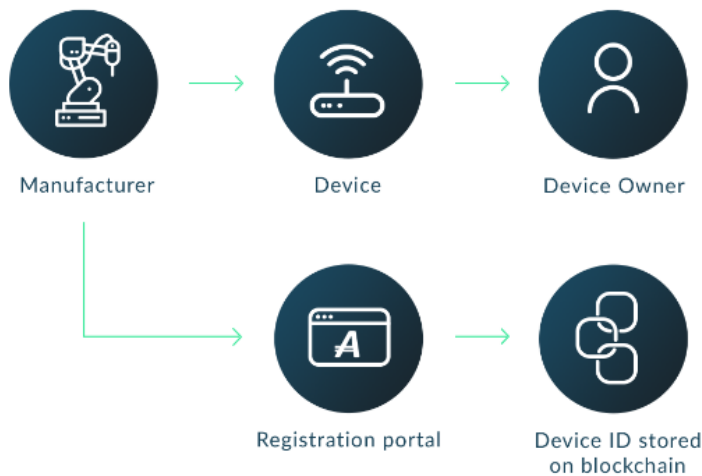

Figure 2. *Atonomi Registration.*

3.2 Activation

3.2.1 Overview

The Atonomi activation functionality occurs after the Atonomi enabled device has been sold to an end user. The end user receives activation instructions directing them to a web portal, where they enter a device identifier (provided in the instructions) and pay for the activation in Atonomi Tokens via a cryptocurrency wallet. Devices that have been Atonomi enabled via the Atonomi Device SDK contact the Atonomi activation service upon first production boot, sending their signed identifier. Because the device underwent the registration process, the IRN's activation service finds the device in its whitelist, verifies its signature, and clears the activation payment, officially activating the device within the Atonomi trust environment.

3.2.2 Device SDK

The Atonomi Device SDK has enables the device manufacturer to 'hook' into the device's initial boot up. The activation function autonomously (without end user interaction) signs the device ID with its own private key and the Atonomi activation service public key and submits the device ID to the activation service for verification.

v0.9.4a

3.2.3 Activation Portal

Device owners receive activation instructions, which include a URL for a device activation portal and the public device ID. The portal includes a plugin that takes in the device ID and sends a request to a cryptocurrency wallet to transfer an activation transaction fee if applicable. (This process can also be provided by the manufacturer to simplify device deployment for the consumer.)

3.2.4 Activation Service

The Atonomi activation service is a cloud-based, globally accessible, highly available, high-volume service that provides the second step in the Atonomi process. The IAS provides several key functions to the overall Activation functionality; it provides a device interface that newly booted devices communicate with to finalize the activation process. The device ID is written to the blockchain.
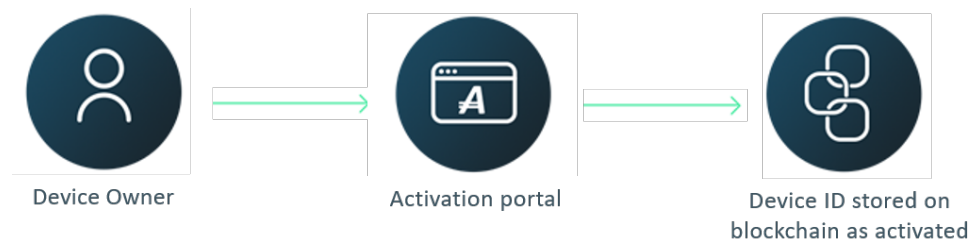

Figure 3. *Atonomi Activation.*

3.2.5 Atonomi Smart Contract: Activation

The activation function of the Atonomi smart contract governs the writing of newly activated device IDs to the blockchain when the device owner boots the device and activates it via the interface. It also facilitates the payment in Atonomi Tokens for the activation of devices.

3.3 Validation

3.3.1 Overview

Atonomi-enabled devices can begin to utilize the Atonomi validation functionality. Devices exchange their signed device identifier with other devices that they want to transact with. Each device can then call the Atonomi validation service, with its counterpart's signed device identifier and receive back an indicator of whether or not the device is an Atonomi 'member' or not. If the other device is a member of the Atonomi, the validation service sends back the current reputation for that device.

3.3.2 Device SDK

The Atonomi Device SDK has two additional methods for validating another device's identity. The first method produces a handshake package to be sent to another device for validation. The second method takes in a signed device identity (from another device via handshake) and submits it to the validation service to be validated. The latter method returns a reputation score if the other device is valid.

v0.9.4a

3.3.3 Validation Service

The Atonomi validation service is a primary component, that when globally distributed, becomes part of the central hub of the Atonomi IRN. The validation service is a cloud-based, highly available, high-volume service that essentially provides the third step in the Atonomi process. The validation service provides a key function to the overall validation functionality; it provides a device interface that devices communicate with to validate another device and it includes a module for reading the device identity from the blockchain as validation that it has registered/activated on the Atonomi trust environment.

A 'ledger' of validation transactions is maintained for future reference during the reputation recording process. Each mutual validation (two devices validating each other) results in two records for referencing.

3.4 Reputation

3.4.1 Overview

The Atonomi reputation functionality is used after the Atonomi-enabled device has been activated by an end user and begins to transact with other devices. Devices that have been Atonomi-enabled via the Atonomi Device SDK are able to submit a reputation report concerning other devices they have transacted with. The Atonomi Device SDK contains a method that produces the report from input criteria. Once submitted, the reputation service receives the report, validates it against the validation database and logs it into the reputation database for additional processing.

3.4.2 Device SDK

The Atonomi Device SDK has one reputation report method. The intent is that the device manufacturer codes their application to generate the report based on criteria specified in the SDK documentation and then submits the report as input to the reputation report method.

3.4.3 Reputation Service

The Atonomi reputation service is a cloud-based, highly available, high-volume service that essentially provides the third step in the Atonomi process. The reputation service provides a device interface that devices communicate with to provide reputation feedback on another device. Reputation reports are submitted by devices. The reports are periodically audited by reputation auditors to produce updated reputation scores for devices.
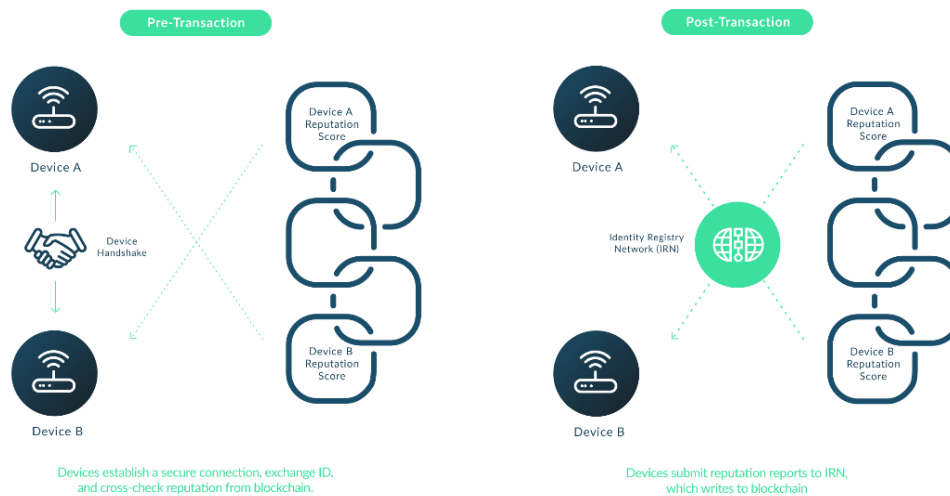
Figure 4*. Atonomi Reputation.*

3.4.4 Atonomi Smart Contract: Reputation

The reputation function of the Atonomi smart contract governs the writing of updated device reputation scores to the blockchain after the reputation auditors have processed the reports. It also facilitates the payment in Atonomi Tokens for the reputation score updates, and disburses these as fees to reputation auditors on a pre-programmed and autonomous basis.

3.4.5 Reputation Auditor

The reputation auditor is a node/service that processes reputation reports using the Atonomi reputation model and updates the reputation scores of affected devices. The updated reputation scores are then written to the blockchain and to the reputation database. For purposes of utility the initial reputation auditor node is within the IRN. Eventually, this will be broken out into a separate node so that hosting may be distributed among Atonomi reputation service providers.

3.5 The Atonomi Token

The Atonomi Token, which functions in compliance with ERC-20 standards, is a utility token used during device registration, device activation, and to reward reputation auditors. The Atonomi Token can also be used to pay processing fees for secure device-to-device commerce between devices registered onto the Atonomi trust environment.

3.6 Additional Elements

The extensible design of the Atonomi architecture was created to support deployment of future elements and services. **Note that these potential elements and services are provided for illustrative**

purposes only, and Atonomi assumes no responsibility for the function or availability of these or any other potential elements or services in the Atonomi trust environment.

3.6.1 Transaction Service Creation and Maintenance Services

The Atonomi Device SDK could support 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 Token-compatible wallets could be used to store Atonomi Tokens which will deduct a small percentage for some transactions taking place over the Atonomi trust environment.

3.6.2 Device Ownership Transfer Service

Atonomi could support ownership transfer of IoT devices—with or without wallet contents. Upon device transfer, a transaction log entry of the transfer would be broadcast to the Atonomi reputation service which would update device reputation as needed.

3.6.3 Reputation Caching and Lookup Services

Atonomi could facilitate a cloud-based service giving devices the ability to perform a fast lookup of reputational data prior to engaging in peer-to-peer transactions—while also providing manufacturers the option of opting out of the service if not deemed necessary for anticipated device usage. Services to write to the reputation registry for whitelisted auditors could also be provided through Atonomi.

3.6.4 Transaction Validation and Facilitation Services

Atonomi could support services to facilitate off-chain inter-device transactions. The data from these services would be used for reputation analysis. The extensible nature of the Atonomi Device SDK means that different verticals can define which non-commercial transactions are stored off-chain. Atonomi Tokens may be used to pay network fees for inter-device commercial transactions, and eventually, they may be a useful default payment method for such inter-device commercial transactions. Though Ethereum network transaction processing might become cost- or speed-prohibitive, the network should be sufficient for immediate use. If and when necessary to maintain a healthy ecosystem, Atonomi and other users of the Atonomi trust environment can evaluate migration or simultaneous use of alternative blockchain technologies for these transactions, such as Ethereum Raiden, Plasma, HashGraph, or others.
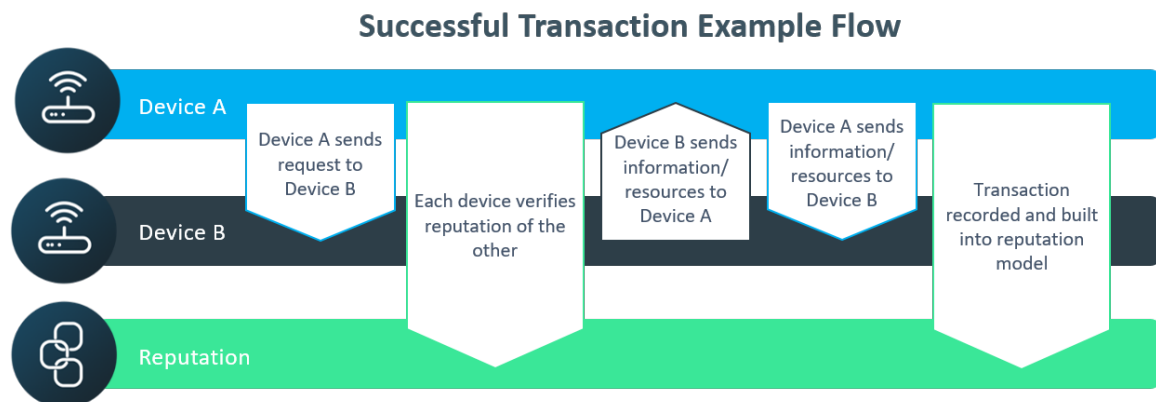
Figure 5. *Transaction Flow.*

3.7 Scalability

Atonomi 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 price and performance. We will monitor new developments to ensure that the Atonomi's decentralized services can serve the necessary use cases. Note, however, that many of the operations supported by Atonomi do not require high throughput writes to the blockchain.

4.0 Simple and Secure Authentication

The Atonomi Device SDK provides security-enhancing single-stage handshake for securing initial contact between a newly activated device and our Identity Registry.

4.1 Small Footprint

The Atonomi Device SDK has a minimal footprint, making it easy to include the code in applications. The SDK only requires about 100 KB of RAM (50 KB on most devices) for efficient performance on typical IoT devices. Our experience in creating tight code and embedding key seed data has informed our creation of the small code footprint of our Atonomi Device SDK, which we see as essential for integration with IoT devices that can be resource-constrained.

4.2 Device Agnostic

Developers can use the Atonomi Device SDK as a foundation for creating libraries and tools for devices and custom network stacks and other code that organizations might want to use in creating IoT solutions. Atonomi uses this same device agnostic approach in creating an extensible development platform that can be customized to the exacting needs of different verticals.

4.3 Secure Data

Atonomi security 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.

5.0 The Atonomi Trust Environment

"The number of connected devices is 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 environment that is designed to maintain and expand IoT security and interoperability. Atonomi plans to accomplish this in multiple ways.

First, unlike other IoT device security platforms, Atonomi begins at the source of the IoT value chain by flashing code onto the chip with the Atonomi Device SDK. The chip-first solution is relevant to the Atonomi architecture because a small number of chip manufacturers create the foundation for a universal trust environment that could be widely used by smart device manufacturers, and then built on by application developers.
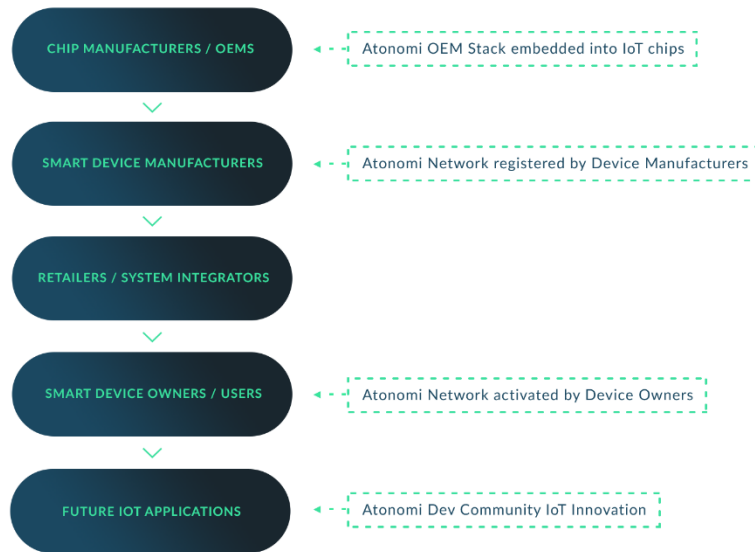
Figure 6. *End-to-End Security Value Chain.*

The Atonomi trust environment 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, and device manufacturers may elect to audit data and publish reputation data, provide service layers to interact with Atonomi's smart contract, or validate and process transactions between devices. The Atonomi trust environment will enable a community of developers to build the next generation of IoT applications and platforms. By facilitating trusted interoperability between devices, Atonomi solves a fundamental problem of security in IoT and facilitates an innovation hub for the developer community.

Atonomi is engineered to support extensibility. We provide known and trusted device identity and reputation, and other companies and organizations 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.

Auditors are anticipated to seek fees in Atonomi Tokens to serve as validators on the Atonomi trust environment. 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 the smart contract, auditors (run by OEMs and other stakeholders) could validate this transaction and, in return, receive a reward fee in Atonomi Tokens. Manufacturers may elect to create reward pools of Atonomi Tokens to encourage auditing of their own devices.

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 identity and reputation-based trust environment for the IoT industry.

Below are applications that may be of immediate relevance to potential users of the Atonomi. The healthcare, industrial, smart city and home device markets are considered to be current movers in the IoT space. **Note that these potential applications are provided for illustrative purposes only and Atonomi users are solely responsible for their use of such applications, if any. Atonomi assumes no responsibility for the function or availability of these or any other applications of the Atonomi.**

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-enabled 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 trust environment.
- 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 Atonomi.

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 execution 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 require 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, Atonomi is architected so that diverse verticals can integrate our Atonomi Device SDK to create innovative solutions. Examples of how the Atonomi trust environment can provide value include:

- 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, a standard ERC20 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. IoT 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 Token-based Identity & Reputation

Atonomi Tokens serve as a multi-use token for the internal mechanics of Atonomi. Specifically, tokens can be used to pay fees when new devices are registered and activated onto the Atonomi trust environment. Additionally, tokens are designed to be a key component of Atonomi's reputation service by rewarding auditors for capturing, analyzing, and scoring reputation data. 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 for digital payments to enable device-to-device autonomous transactions. This token-based economy enables devices to securely engage in peer-to-peer autonomous

transactions. While Atonomi doesn't charge for data exchanges, and Atonomi is agnostic as to the particular token used for device-to-device transactions, Atonomi Tokens could be used 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 and activation, with a future release facilitating commercial transactions. For instance, Atonomi may elect to charge a minimal processing payment for handling commercial transactions between IoT devices. Nothing is charged for data exchange, as noted above. 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 with the trust environment, including device registration, activation, 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 through customer acquisition programs.

Atonomi aims to unlock many new use cases and future innovations such as a marketplace for IoT commerce. The developer community can build on Atonomi to innovate new projects and service offerings leveraging Atonomi 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 Atonomi to secure the end points on Swytch's network and enable trusted interoperability.

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