White Paper

blockchain Of Things

BCOT Global Holdings

Abstract

The Internet of Things (IoT) is not secure and we plan to fix that.

Blockchain of Things, Inc. aims to solve the IoT security problem with the official launch of Catenis Enterprise, an easy-to-use, web services layer encoded into the Bitcoin blockchain. By using a web services layer approach, Catenis can easily be adapted to support Ethereum, Hyperledger, and many other blockchains. Catenis is a live network (in beta) with several active corporate clients.

In this paper, we first characterize the nature of IoT security threats and the key hurdles they pose for enterprise IoT adoption. Then, we highlight the security advantages of the Bitcoin blockchain when compared to traditional IoT infrastructures. Next, we delineate the obstacles that have prevented organizations from using the Bitcoin network for secure IoT device communication. We describe how Catenis Enterprise addresses these obstacles while leveraging the security and trust of the Bitcoin blockchain. Finally, we introduce the concepts of true attestation and smart-assets, key attributes which expand the functionality of Catenis to include applications that go beyond the traditional scope of IoT.

Executive Summary

The Internet of Things (IoT) is not secure and we plan to fix that.

The IoT is Not Secure: A Bain-sponsored survey of over 500 corporate IoT buyers concluded that the #1 barrier to accelerating industrial IoT adoption is insufficient security.[1] Security concerns plague the traditional IoT market in large part due to the current reliance on centralized servers for IoT device communication. More specifically, IoT vulnerabilities can be grouped into three categories:

- **A Denial-Of-Service (DoS) Attack:** A DoS attack can indefinitely disrupt mission-critical IoT-enabled services.

- **Hacking:** Various methods of hacking such as device spoofing, man-in-the-middle, and replay attacks can lead to data theft or device hijacking.

- **Lack of Auditability:** The lack of an audit trail means device administrators can be oblivious to an intrusion for months or even years.

Bitcoin is Secure: The Bitcoin blockchain, the oldest and most battle-tested distributed ledger, inherently solves these security problems given that it has no central point of failure. The Bitcoin network has proven its resistance to a variety of hacking and DoS attacks, while also demonstrating its auditing capabilities given the irreversibility of ledger entries. As such, it is possible for an administrator to securely activate and communicate with an IoT device by linking the device to a Bitcoin address and using the Bitcoin blockchain to send messages (e.g. command-and-control signals) to that address.

Catenis Overcomes Bitcoin's IoT Limitations: Despite these security advantages, the Bitcoin blockchain suffers from many limitations which have prevented its use for IoT. Catenis Enterprise overcomes these hurdles, and does so in a way that retains Bitcoin's security advantages. This is possible since Catenis is a web services layer encoded into the Bitcoin blockchain. For industrial IoT applications, the limitations of the Bitcoin blockchain and the corresponding key features of Catenis can be grouped into six categories:

- **80-Byte Size Limit:** The Bitcoin message field is only 80 bytes which is limited and does not provide the ability to send large payloads of meaningful data between IoT devices. Catenis solves this issue by eliminating the size limit so that messages can include programming code or data files of any type or size.

- **Lack of Permissioning:** If an IoT device is connected to a public Bitcoin address, unauthorized actors could activate the device since the address it's connected to accepts messages from anyone. Catenis solves this issue through the creation of a permissioned network encoded into the open Bitcoin blockchain.

- **Lack of Encryption:** Messages sent through the Bitcoin blockchain are visible to the world since they are not encrypted. Catenis solves this issue by providing end-to-end encryption. The security features don't stop there since Catenis also automatically uses a brand-new Bitcoin address assigned to the IoT device every time the system sends a message to that device. As such, any messages sent to previously used Bitcoin addresses will have no impact on the device in question. This ensures Perfect Forward Secrecy[2] as messages travel through ephemeral tunnels that only exist for a blink of an eye. It also impedes unauthorized actors from conducting analytics to discover related messages.

- **Speed and Scaling Challenges:** Bitcoin confirmation times are slow and the blockchain suffers from well-publicized scaling challenges. Catenis solves this issue by running as a 2nd layer fabric akin to the Lightning Network,[3] which allows us to provide instant, scalable transactions. However, unlike the Lightning Network, we can function without counterparty risk since Catenis is a permissioned network.

- **Difficult to Use for the CTO:** The Bitcoin blockchain is difficult to use since most IT staff are not familiar with blockchain protocols. Catenis solves this issue by creating a web services layer and an easy-to-use API for customers.

- **Difficult to Manage for the CFO:** The Bitcoin blockchain can be difficult to manage for some CFOs since many are not experienced in managing cryptocurrencies. Catenis solves this issue by conducting the necessary cryptocurrency transactions behind the scenes, which abstracts the cryptocurrency from the perspective of corporate clients.

Catenis Facilitates Proof of Authenticity: Catenis' enhanced feature set enables applications that go beyond the traditional scope of IoT to include a system for true attestation (a.k.a. proof of authenticity). With Catenis, one can track the authenticity of real world products to mitigate both retail and supply chain product fraud, an estimated $1.9 trillion per year problem.[4] There are two key steps to the attestation process:

- **Confirm That the Product Manufacturer Has a Certificate of Authenticity:** A manufacturer can log the cryptographic fingerprint of a certificate of authenticity to the blockchain and provide the reseller/customer with a reference ID that allows for independent cryptographic confirmation that the manufacturer of the product owns the endpoint that logged the certificate of authenticity.

- **Confirm the Certificate of Authenticity is Genuine:** Catenis can display independent cryptographic identity verification. The owner of a given Catenis device endpoint can prove their identity by demonstrating access to or ownership of the appropriate website domain, government registration, or third-party certification. When these two steps are combined, it allows for a trustless proof of authenticity that can help mitigate fraud in a supply chain or retail setting.

Catenis Enables Customizable Smart-Assets: Catenis further expands its capabilities beyond the traditional scope of Internet of Things by empowering clients to digitize more things. This goal is accomplished by empowering customers to create smart-assets and transfer them from one user to another. Catenis smart-assets have all the robust functionality and smart contract capabilities of the Colored Coin Protocol,[5] but are even more powerful in four key ways:

• **Option to Deliver Actual Digital Payload:** A Catenis smart-asset coupled with its messaging capabilities can be configured to transmit the actual digital payload, which contrasts with many other crypto projects in which the digital asset is simply a representation of the payload backed by the promise of a third-party such that it has to be requested via an unrelated external system. A Catenis smart-asset can be configured to transmit the actual stock certificate, house deed, or MP3 file so that the actual payload can be transferred from one user to another.

• **Option to Encrypt the Digital Payload:** The digital payload that travels with the Catenis smart-asset can be encrypted with the public key of the destination endpoint so that only the destination endpoint can access the payload. This contrasts with crypto projects in which the payload is unencrypted and visible to the world.

• **Option to React to Messages:** Catenis smart-assets can be configured to react to messages from other endpoints, which contrasts with crypto projects in which the digital asset is nonresponsive. For example, a Catenis customer can program the automated creation and distribution of smart-assets conditional on the receipt of a message. This allows Catenis to be a platform for the efficient, transparent distribution of any digital asset, including but not limited to token sales.

• **Permissioned Network:** Since Catenis is a permissioned network, smart-assets will not react to messages from unauthorized endpoints. This contrasts with crypto projects that lack permissioning capabilities.

Catenis is a Platform for Third-Party Apps: Catenis is fundamentally a platform on which third-party developers will be able to build applications using Catenis' core functionality (e.g. secure messaging, smart-assets, etc.) as a building block. We highlight four of the many categories in which a third-party programmer could focus future development efforts:

• **Industry-Specific Apps for Securing the IoT:** Different industries and different parts of an operation will prefer to leverage Catenis' secure IoT functionality for different use cases. As such, a third-party developer could build an industry-specific app that leverages Catenis' security to bring tailored solutions to different segments of the IoT market.

• **Hardware as a Service:** Catenis enables secure, blockchain-based Hardware as a Service since digital keys in the form of a smart-asset can unlock functionality in remote hardware connected to a Catenis endpoint. A third-party developer could build industry-specific applications that leverage this functionality in different ways for different industries.

• **Ticket Marketplace:** Catenis will allow the original issuer of a smart-asset to earn a commission on resales of that asset (i.e. fee-based smart-assets). For example, concert ticket issuers could earn commissions if their tickets are resold on a secondary marketplace. A third-party developer could commercialize this functionality by building a ticket marketplace with smart-asset awareness that leverages the Catenis layer.

• **Equity Marketplace:** Delaware state law allows US corporations to trade shares on a blockchain to streamline the share settlement process. Catenis already has the functionality to encode smart-assets that can transfer the actual stock certificate. Catenis also has the functionality to abstract cryptocurrencies so that traditional equity investors could buy shares in companies from their regular brokerage firm without having to directly deal with cryptocurrency. A third-party developer could build an equity marketplace that would streamline the share settlement process.

Advanced IoT Architecture

Overview

Blockchain of Things, Inc. aims to solve the IoT security problem with the beta launch of Catenis Enterprise (see pages 2-5 for an overview of Catenis' key features).

In this section, we first set the proper context for understanding Catenis' architecture by providing an overview of the IoT market and its use cases. Then, we describe the standard (arguably unsustainable) architecture underlying most enterprise IoT systems. We contrast this with the decentralized, fault-tolerant architecture enjoyed by Catenis customers. We conclude this section by highlighting the importance of interoperability, and demonstrate how Catenis inherently solves the interoperability problems plaguing traditional IoT systems.

Internet of Things: The Backdrop

> **"The hype may actually understate the full potential of the Internet of Things"**
>
> **– McKinsey**[6]

The Internet of Things (IoT) refers to the practice of embedding internet connectivity into physical objects and software-based systems so that they can communicate with other Internet-enabled systems. Companies are increasingly implementing IoT solutions into their business to improve product quality, workforce productivity, operational efficiency, and product development processes.[7]

IoT Market Growth: Gartner, an IT research firm, estimates that the worldwide installed base of IoT units grew 26% in 2014 and 30% in 2016.[8 9 10] The same firm forecasts that growth will continue accelerating to 34% in 2018.[11] Furthermore, it's worth noting that these large growth rates are not occurring on a tiny base. Gartner estimates that in 2016, there were 6.4 billion units in the global installed base of IoT units and annual IoT endpoint spending reached $1.4 trillion.[12]

IOT Units Installed Base (Millions)						
	2013	**2014**	**2015**	**2016**	**2017E**	**2018E**
IOT Units (Millions)	3,032	3,807	4,903	6,382	8,381	11,197
y/y		*26%*	*29%*	*30%*	*31%*	*34%*
Source: Gartner estimates						

IoT Use Cases: A 140-page McKinsey report analyzed the realistic use cases for IoT and concluded that "the hype may actually understate the full potential of the Internet of Things." Based on a bottom-up analysis of the various potential IoT applications, McKinsey estimates that the Internet of Things will have a total potential economic impact of $4-$11 trillion by 2025.[13] In order to provide context for the many ways Catenis-secured IoT systems can be used in practice, we highlight a small sample of the many uses cases for IoT:

- **Manufacturing Optimization:** IoT sensors in factories are being used to increase workflow visibility and reduce the time between identification and remediation of a problem. For example, if a process anomaly is detected, managers can take preemptive action to avoid costly bottlenecks and defective parts.[14]

- **Predictive Maintenance in Gas Pipelines:** If a gas pipeline suffers a spill, it can cause large economic and environmental loss. Operators are increasingly combining IoT data from pipeline sensors with third-party data on weather/flooding events to identify high-risk areas of the pipeline that require manual inspection.[15]

- **Minimizing Costly Hospitalizations:** Wearable and non-wearable IoT devices have already demonstrated the ability to reduce healthcare costs in acute forms of chronic heart failure, diabetes, and COPD.[16] Continuous data from these devices enables early warning signals to allow for prompt interventions that reduce hospitalization risk.

- **Clinical Trial Cost Reduction:** IoT-enabled devices can be used to lower the cost of expensive pharmaceutical clinical trials by an estimated 10 to 15%.[17] By collecting patient health data more frequently, it becomes possible for pharma companies to more quickly identify failing trials, which saves money.

- **Precision Farming:** Many farms have embraced IoT systems by combining data from soil sensors, tractor sensors, satellite imagery, and weather data analytics platforms. These farms can optimize yields by calibrating water and fertilizer usage based on the precise productivity of every few square yards of corn.[18]

- And Many More: The above discussion of use cases was merely illustrative, as there are many more potential applications for Catenis-secured IoT systems.

Traditional Internet of Things Architecture

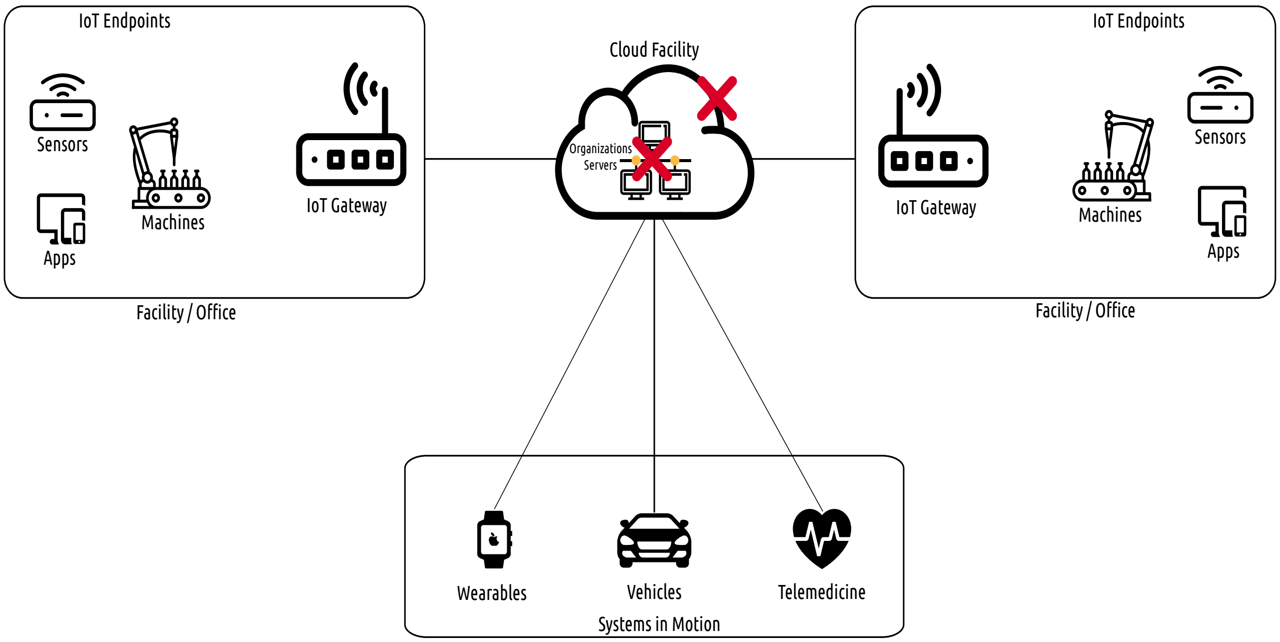
Devices & Gateways: In standard IoT architectures, IoT gateways function as the key communication bridge between IoT edge devices and external systems. Edge devices such as sensors, actuators, and software applications use the local corporate intranet to speak to the on-site IoT gateway. The gateway also connects to the external Internet and offsite data systems (e.g. the cloud). As such, IoT gateways negotiate all communications between IoT edge devices and the cloud. More than just relay points, IoT gateways offer local processing and storage solutions, as well as the ability to autonomously control edge devices based on sensor data.

A typical gateway connects directly to central control systems in a hosting cloud infrastructure.

These clouds systems are susceptible to hacker attacks based on two central points of failure:

- The organization's own servers within the cloud
- The hosting providers of the cloud infrastructure i.e.: AWS, Azure etc.

A breach at either point of failure would affect all systems that rely on the cloud. The diagram below depicts the traditional IoT cloud architecture and its two central points of failure.



Traditional IoT Cloud Architecture

A House of Cards: As devices become more intelligent and connected, the consequences of a successful hacker attack are increasingly dire. The ramifications extend beyond data theft to include hijacking of real-world IoT-enabled machines, putting industrial operations and human safety in jeopardy. Traditional IoT architectures increasingly resemble a house of cards in which one successfully attacked server can compromise a company's entire IoT network. It's no wonder that security is the top concern for corporate IoT buyers.[19]

New Blockchain of Things Architecture

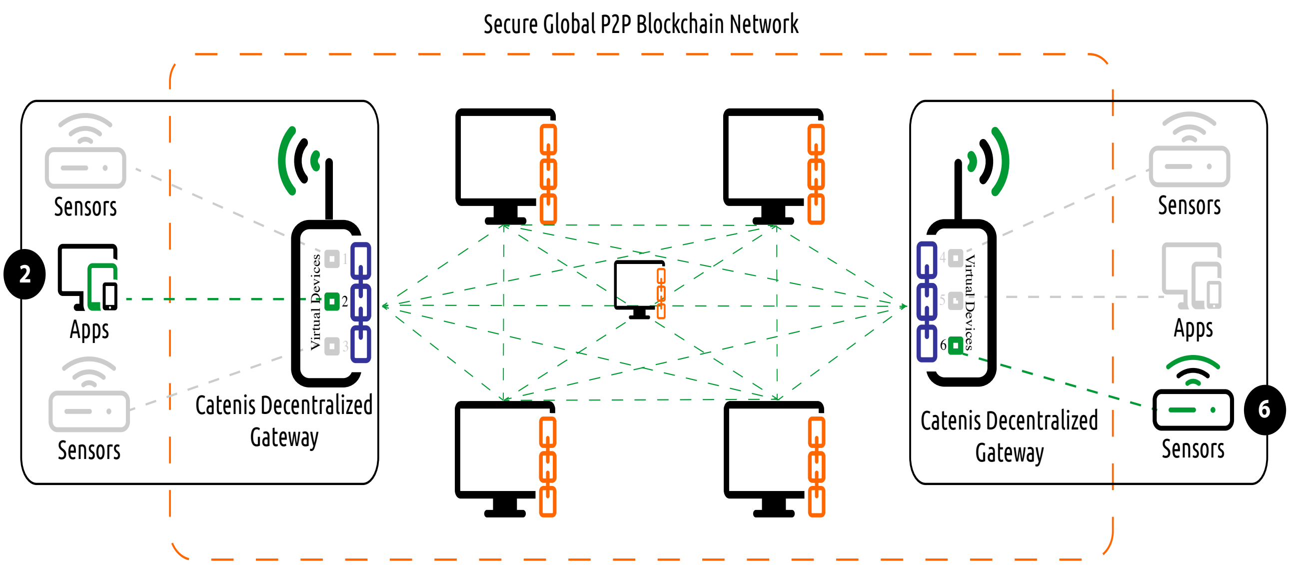
Blockchain of Things, Inc. decentralizes and secures the IoT infrastructure by enabling edge devices such as sensors, actuators, and software applications to communicate with each other on a peer-to-peer basis through Catenis.

Virtual Devices: In Catenis, every real-world IoT device will communicate with and will be represented by its own Catenis virtual device, which is a logical unit that sits in the local Catenis Gateway or the offsite Catenis Hub (see below). Each virtual device will manage a host of Catenis services for the IoT device it represents. These services include Bitcoin address generation, message transmission, data logging, smart-asset creation, smart-asset transfer, fees, encryption, permissioning, ephemeral tunnel creation, public-private key cryptography, etc.

Catenis Gateways: Similar to the traditional IoT architecture, the new Blockchain of Things architecture will be structured so that real-world devices use the local corporate intranet to speak to the on-site gateway. However, unlike traditional IoT gateways, Catenis Gateways will be powered by Catenis software which uses a web services layer to manage communications between real-world devices and virtual devices. In addition, each Catenis Gateway will run a full node (or pruned node) on the Bitcoin blockchain, which will establish its ability to communicate through the blockchain.[20]

Catenis Hub: The Catenis Hub is Catenis' cloud offering. Catenis Hub is a node that clients can connect to if they don't need a Catenis gateway installed onsite. Since it is a cloud offering, clients who use the Catenis Hub do not get the full security benefits of Catenis Gateways. However, these customers can still benefit from security features such as inherent message auditing for all devices and enhanced security for messages in flight across the blockchain. The convenience of Catenis Hubs can be a worthwhile trade-off for IoT devices where maximum decentralized security is not as significant of a concern.

Communication through the Blockchain: Communication between real-world IoT devices will take place through the following steps: 1) The Sending IoT Device will send a message through to the corresponding Sending Virtual Device which sits in the on-site Catenis Gateway or in a Catenis Hub. 2) The Sending Virtual Device will send the message through the Bitcoin blockchain to the Receiving Virtual Device. 3) The Receiving Virtual Device will send the received message to its corresponding Receiving IoT Device. As such, two real-world devices can communicate with each other through the blockchain. See diagram below for a schematic of how communication flows when IoT Device #2 sends a message to IoT Device #6.

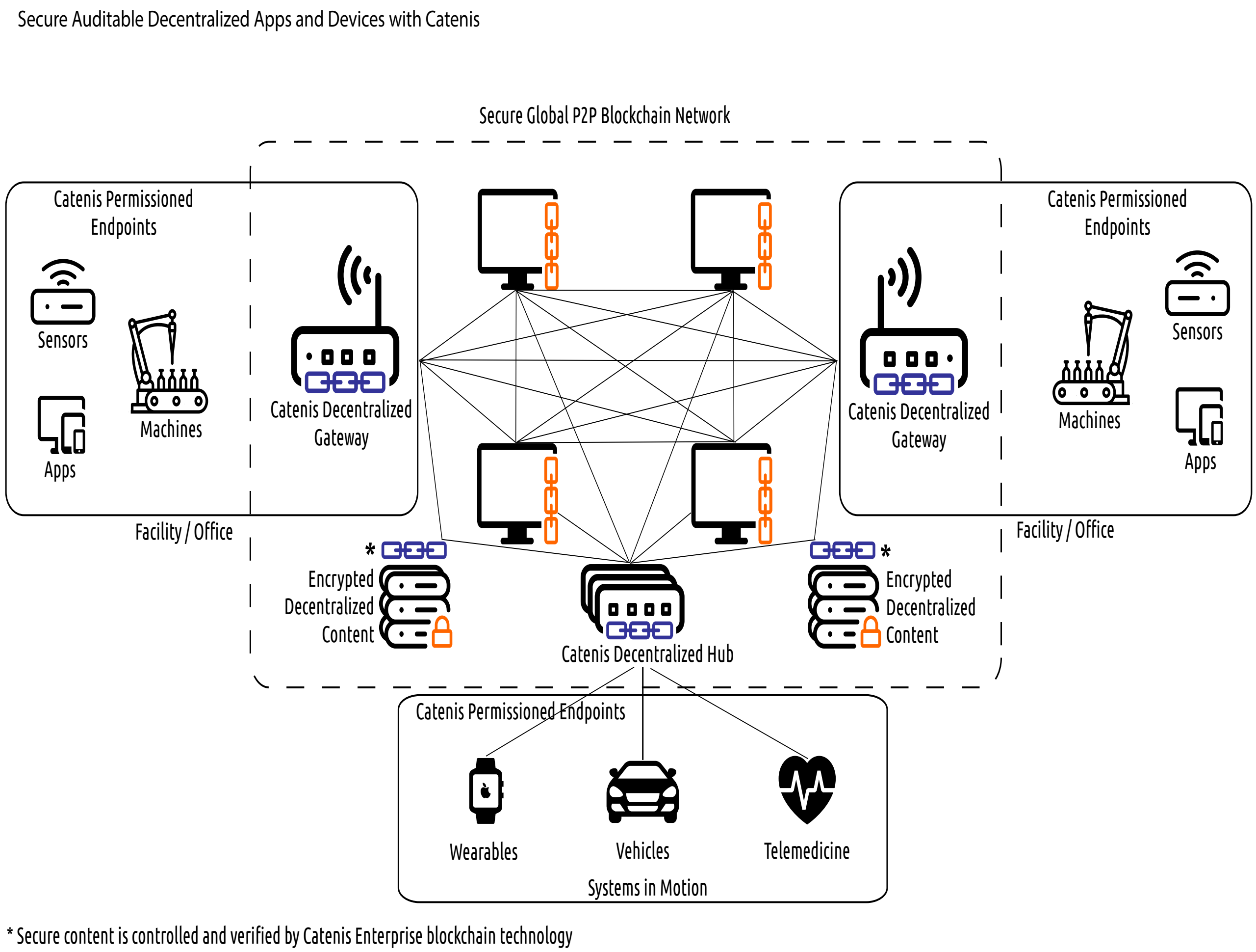


Communication Flow in Blockchain of Things' Ecosystem of Catenis Enterprise

IoT Becomes BoT: Once data from the IoT device reaches its corresponding Catenis virtual device, all communication will occur through the Bitcoin blockchain via Catenis virtual devices. As such, we refer to this new paradigm as the Blockchain of Things (BoT). The advantage of channeling IoT communications through the Bitcoin blockchain is that it's a global, peer-to-peer network that replaces the centralized points of failure that exist in the traditional IoT architecture. Given the lack of a centralized point of failure, the Bitcoin blockchain is inherently more resistant to hacking and DDoS attacks than the traditional IoT architecture. With over $200 billion dollars transacted on the blockchain over the last 2 years,[21] there is plenty of financial motivation for a hacker to attack the network, and yet the blockchain remains secure.

Catenis Decentralized: Not only will an IoT device's message propagate through the blockchain, but so will the Catenis system state itself. The entire Catenis system state will be encoded into the Bitcoin blockchain. This will provide fault-tolerance because the system state could be recreated from the blockchain, providing a fully decentralized reliable system for customers. Since Catenis' architecture will be tightly coupled to Bitcoin, Catenis Enterprise gateways won't rely on any central databases, secondary blockchains, or side chains. This will make connected systems resistant to central points of failure for all critical applications and systems. Furthermore, an edge device's full transaction history can be audited outside of our system, providing confidence to customers, auditors, and regulators.[22]

The diagram below depicts the Catenis Enterprise Decentralized architecture which will liberate customers from the central points of failure that exist in traditional IoT frameworks.



Catenis Enterprise Decentralized Architecture

Functionality Beyond the Internet: Nearly 4 billion people do not have Internet access.[23] For remote locations where the Internet is not accessible or for non-stationary devices where connectivity can be intermittent, it will be possible to configure Catenis Gateways to use secondary means of accessing the blockchain to guarantee uptime for critical systems. In such scenarios, SIM cards or Blockstream Satellite technology can be used to receive information from the blockchain. Blockstream Satellite plans to cover 99.99996% of the world's population, which excludes the few thousand-people living in Antarctica.[24] Not only will this make the Blockchain of Things accessible to over 99% of the global population, but it will also bring fault tolerance for critical systems when the Internet goes down. Fault tolerance and expanded coverage address a critical need for many industrial implementations (e.g. offshore oil rigs, remote research facilities, etc.).[20]

Interoperability of Disparate IoT Systems

> **"Interoperability is critical to maximizing the value of the IoT. On average, 40 percent of the total value that can be unlocked requires different IoT systems to work together."**
>
> **– McKinsey**[25]

IoT's Interoperability Challenge: To unlock the full potential of the IoT, heterogeneous platforms that run different operating environments, languages, and protocols need to be able to communicate with each other. Corporations typically have an unwieldy number of software platforms that are incompatible with each other. This causes many firms to squander a large portion of the potential value that can be unlocked from IoT systems.[26]

BoT's Interoperability Solution: Catenis inherently solves the interoperability issue because Catenis' web services API accepts read/write requests from any software platform in any modern language. IoT devices on disparate platforms can send data to each other via each platform's Catenis endpoint. Each platform can then access/analyze the data through its respective Catenis endpoint using whatever protocols and languages are native to that platform. For example, equipment manufacturers for offshore oil rigs frequently enable their machines with IoT sensors to provide their customers anomaly detection and predictive maintenance services. However, more than half of the potential failure modes can only be predicted by combining IoT data from different equipment suppliers.[27] By using Catenis, an offshore oil rig can incorporate data from these disparate IoT systems and significantly increase the value derived from its IoT initiatives.

BoT Streamlines Inter-Company IoT Coordination: In addition to addressing interoperability issues, Catenis also streamlines inter-company data sharing by relieving companies of the cost and responsibility of securing a shared database. Catenis accomplishes this goal by allowing companies to log data to a secure, decentralized network (e.g. Bitcoin or IPFS; details on page 14). This capability helps firms address the security vulnerabilities that can limit inter-company IoT coordination. For example, in the prior offshore oil rig example, neither the company nor its suppliers needs to worry about securing a shared database. This is a key advantage since many CTOs are particularly reluctant to host inter-company shared databases that connect to internal systems since it increases the surface area of attack on the company's core IT infrastructure.

Overview

The Attack Vector of Things: Numerous IT research organizations have studied the IoT security challenge and identified security as the key challenge facing the IoT.[28 29] Based on a survey of its members, The Global Digital Infrastructure Alliance concluded that the top four IoT related security concerns can be categorized into the following four areas:[30]

- Network: Vulnerabilities in the IoT network
- Application Layer: Application security vulnerabilities within IoT systems
- Authentication: Poor authentication of IoT endpoints
- Physical: Physically unsecure endpoints

In this section, we survey key attack vectors[31] from each of the above four categories and explain how Catenis mitigates each vulnerability.

Network Attacks

Network-Based Man-in-the-Middle (MITM) Attack: Hackers could manipulate network communication protocols by posing as a legitimate node which could allow them to maliciously intercept and alter data flows.

- **Catenis Defends the Attack:** Unlike the traditional IoT architecture, in the Blockchain of Things, communication between nodes occurs through Catenis on the Bitcoin blockchain. As such, to conduct a network-based MITM attack on the Blockchain of Things, one would need to successfully conduct a MITM attack on Bitcoin. With over $200 billion of value transacted on the Bitcoin blockchain over just the last two years,[32] there has been ample financial motivation, yet no evidence that the network is vulnerable.

Remote DDoS Attack on the Network: An attacker could overwhelm network devices with excessive requests so that legitimate users can't access the system. In the Blockchain of Things, there are multiple lines of defense against this attack.

- **DDoS Protection at the Device Level:** Catenis inherently defends against this type of DDoS attack since devices can be purposely built to only communicate through the Catenis API. A device level DDoS attack would be thwarted due to Catenis' permissioning & ephemeral tunnel protection layers which only allow permissioned endpoints to communicate with the device (see pages 14-16).

- **DDoS Protection at the Central Server Level:** An attack at the central server level is the most critical DDoS vulnerability since if it is exploited, a company's entire IoT system can be brought down. Catenis inherently defends against this type of DDoS attack since the central server is decentralized onto the Bitcoin network, which has proven itself resistant to a DDoS shutdown over its 8-year history.[20]

- **DDoS Protection at the Gateway Level:** Catenis customers can protect themselves from a DDoS attack at the gateway level through two lines of defense: 1) Customers can conceal their gateway behind the Tor network to anonymize their gateway's IP address. Without the IP address, an attacker would not know where to direct his DDoS attack. 2) If a DDoS flood is detected over internet lines, Catenis Gateways can be configured to automatically switch over to a secondary means of receiving information (e.g. SIM cards or Blockstream satellite). This creates resilience at the gateway level as well.[20]

Traffic Analysis Attack: Hackers can analyze communication patterns between devices to infer information about encrypted messages. This can be accomplished without ever cracking the encryption code.

- Catenis Mitigates the Risk: Traffic analysis is very difficult on Catenis because of the use of ephemeral tunnels (see page 15-16). If the customer places their gateway behind the Tor network, that would obfuscate the IP address of their Bitcoin node and would further complicate any traffic analysis attack. We expect traffic analysis will become even more difficult when Bitcoin implements the Dandelion Anonymization Protocol.[33]

Application Layer Attacks

Malware/Viruses: Attackers can use malware / viruses to hack and disrupt key systems.

- **Catenis Mitigates the Risk:** Most malware/viruses rely on open connections to the Internet. However, in Catenis, communication channels are isolated since only permissioned endpoints can communicate with IoT devices (see page 14).

DDoS Attack on the Application Layer: In an application layer attack, a hacker amplifies the impact of a relatively small number of external requests by causing the application to execute a large number of unnecessary internal requests so that it can't fulfill legitimate requests.

- **DDoS Protection at the Application Layer:** In Catenis, an attacker can't conduct an Application Layer DDoS attack since Catenis devices only communicate to permissioned endpoints through the blockchain (see page 14).

Authentication Attacks

Cryptanalysis Attacks: A hacker could identify weaknesses in the cryptographic algorithm to gain unauthorized access to a device.

- **Catenis Defends the Attack:** Catenis relies on Bitcoin's cryptography, which has successfully protected billions of dollars' worth of bitcoin for nearly 7 years.

Man-in-the-Middle Attack for Encryption: A hacker could use a man-in-the-middle attack to intercept the private keys shared between two users.

- **Catenis Defends the Attack:** In Catenis, private keys are not shared between endpoints. Instead, the sender encrypts each message with the public key of the destination endpoint. After that point, the message can only be decrypted by the private key of the destination endpoint, so that not even the sender can read the message after he encrypts it. As such, the private key never needs to be shared between two users.

Physical Attacks

Physical Man-in-the-Middle Attack: An attacker can physically tamper with an unsecured node (i.e. edge device) and inject malicious code into it to gain access to the rest of the IoT network. While physical attacks are best addressed through physical defenses, Catenis can still help mitigate the consequences of a breach at an unsecured node.

- Permissioning Limits the Damage: Administrators can use Catenis' permissioning system so that remote, physically unsecured nodes are limited in terms of what parts of the IoT network they can access. IT departments can configure the Catenis system so that the most sensitive devices are only accessible by physically secured nodes.

- Inherent Auditability Enables Rapid Detection: Catenis inherently provides auditability for every device. Every message is logged to the Bitcoin blockchain and is visible to the administrator. IoT systems managers can set up alerts so that if a device is active more frequently than normal or during off hours, the anomaly is quickly noticed and corrective action can be taken. This contrasts with traditional IoT systems in which auditability is not inherent at the device level, but has to be installed separately for each device using third party solutions. This is a costly and complex process given the billions of IoT devices in the worldwide installed base. Fortunately, Catenis customers can avoid this complication.

Breaking Through Bitcoin's IoT Limitations

Overview

Despite the many security advantages of the Bitcoin blockchain, there are many obstacles that have prevented its use in IoT applications. In this section, we examine Bitcoin's limitations and the corresponding Catenis product features that break through those limitations.

Data, Documents and Information of Any Size

Bitcoin's 80-Byte Limitation: The 80-byte limit on Bitcoin transaction messages allows for only rudimentary messages to be transmitted. This may not be enough for meaningful communication between IoT devices.

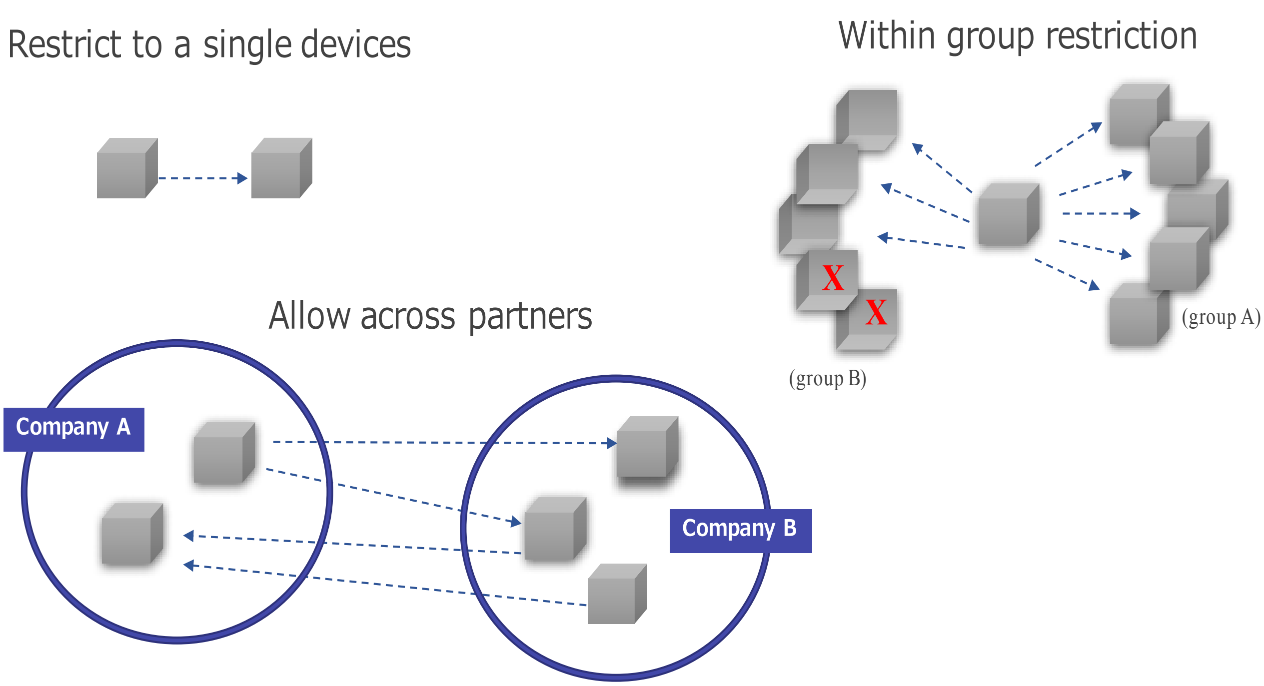
- **Catenis Allows Data of Any Size:** Catenis removes the 80-byte size limit and enables the transmission of data of any size. This includes command-and-control signals to IoT devices, programming code, or files of any size or type (e.g. DLLs, Source Code, PDF, MP3, CAD, etc.). Catenis liberates users from the constraints of the 80-byte Bitcoin messaging field size by supporting integration with an unlimited number of storage platforms. We default to using IPFS as the storage platform since it is a decentralized storage protocol with the ability to store unalterable data.[34] That said, any storage provider can be quickly integrated with Catenis to provide additional storage locations. Catenis has an extensible payload storage layer specifically designed to allow pluggable add-ins for alternative storage providers such as Amazon Web Services (AWS) Object Storage Service, Simple Storage Solution (a.k.a. S3 Buckets), and Azure Blob Storage.

Control and Permissioning On a Global Open Ledger

Bitcoin's Lack of Permissioning: If an IoT device is connected to a public Bitcoin address, unauthorized actors could activate the device since the Bitcoin address it's connected to accepts messages from anyone. This problem is a deal-breaker for most IoT applications.

- **Catenis is a Permissioned Network:** We solve this issue by creating a permissioned network encoded into the open Bitcoin blockchain. In Catenis, a real-world IoT device isn't directly connected to a Bitcoin address. Instead, it speaks through its corresponding virtual device, which includes a Virtual Device Permissioning Broker technology layer that only allows permissioned messages to be received. Permissioning is accomplished by using Bitcoin's transaction signature verification on every outbound transmission to identify the sender's Bitcoin address. Only messages from authorized virtual devices are permitted to reach the real-world IoT device.

- **Flexible Permissioning Model:** Customers can use Catenis' permissioning system to restrict communication to a single device, group, or company. Walled gardens can be built to include outside partners and customers as well. Permissions are set with a few mouse clicks and can be configured at four levels: 1. System Wide 2. Node (hub or gateway) level 3. Client level and 4. Device level.



Permissioning in Catenis Enterprise

Ephemeral Tunnels & End-to-End Encryption

Bitcoin Lacks Privacy: In Bitcoin, messages sent through Bitcoin are unencrypted and visible for the world to see. Even if that weren't the case, unauthorized observers could still deduce information about an endpoint by correlating activities over time between Bitcoin addresses. Both issues combine to create significant privacy and security challenges for enterprises.

- **Catenis Messages Can Be Encrypted:** In Catenis, messages are encrypted by default with the public key of the recipient's Bitcoin address. The only way the message can be decrypted is with the private key of the recipient's Bitcoin address. Not even the sender can read the message after it is encrypted, only the recipient can. Furthermore, if an application requires messages to be unencrypted, customers can override the default and send messages unencrypted.

- **Catenis Messages Travel through Ephemeral Tunnels:** Every time Catenis Enterprise is used to send a message to a virtual device, the recipient virtual device generates a new Bitcoin address to receive the message. As such, when two virtual devices repeatedly communicate with each other, each message transmission in that thread occurs between different pairs of Bitcoin addresses. We refer to this as an ephemeral tunnel since the communication pathway (i.e. the specific pair of Bitcoin addresses) is constructed in real time, lasts for a blink of an eye, and is subsequently torn down never to be used again for a transmission. Loosely based on both Hierarchical Deterministic Wallets (HD wallet) technology[35] and Hub-and-Spoke Micro-Payment Channels,[36 37] Catenis ephemeral tunnels provide multilevel security modeled after IEEE temporary address (also known as "private address") recommendations. Private addresses are notably used to eliminate "four generic attack types: correlation of activities over time, location tracking, address scanning, and device-specific vulnerability exploitation."[38]

- **Catenis Enables Perfect Forward Secrecy:** Not only do Catenis ephemeral tunnels complicate traffic analysis by unauthorized observers, they also enable Perfect Forward Secrecy[39] on every transmission since every message in a thread is encrypted with a different public key. Perfect Forward Secrecy ensures that the owner of a private key for one message cannot read previous or future messages in the same message thread. This means that if a decryption key is compromised, it only exposes a small portion of a user's sensitive data since any previous or future messages in the same thread cannot be decrypted with the same key.

Lightning Fast Speed with Radical Scalability

Bitcoin Transactions Can Be Slow and Expensive: Bitcoin is associated with transactions that require 10-minute confirmation times and expensive miner fees. On the surface, Bitcoin appears to be impractical for frequent, time-sensitive IoT device messaging.

- **Catenis IoT Messages are Lightning Fast:** Although Bitcoin confirmation times average 10 minutes, the actual transaction occurs in the blink of an eye. The main reason people wait for the confirmation is to avoid counterparty risk in the form of a double spend attack. This is a nonissue for IoT related applications since customers are typically transacting messages (not valuable digital currency) with their own endpoints (not someone else's). Since there is no need to worry about counterparty risk of double spend, there is no need to wait for on-chain confirmations before reacting to messages.

• **Catenis Smart-Asset Transfers are Lightning Fast:** If a Catenis user were sending a valuable smart-asset to a different Catenis user, a double spend attack would still not be possible. To understand why, one must first understand what is necessary for a double spend attack to occur. In Bitcoin, a skilled programmer would have to custom build their own digital wallet and use their access to Bitcoin's input/output structure to conduct a double spend attack. Since this is a possibility in Bitcoin, most users wait for on-chain confirmations to avoid getting cheated. However, since Catenis is a layer 2 technology, Catenis users don't have access to the underlying Bitcoin input/output structure, so there is no way to conduct a double spend attack in Catenis. As such, Catenis smart-asset transfers occur in the blink of an eye since the legitimacy of the transfer is pre-determined without needing to wait for the on-chain confirmation.

• **Catenis Transactions Are Inexpensive:** Bitcoin is associated with expensive transaction fees since most Bitcoin wallets are optimized for 10-minute confirmation times (basically as quick as possible). Catenis takes a different approach by targeting a service level guarantee from 10 minutes up to 5 hours. While the exact savings will depend on market conditions, we estimate that 5-hour confirmations are typically 70%-98% cheaper than 10-minute confirmations. The primary downside of delayed confirmation times in Catenis is delayed access to auditability on the immutable ledger. We suspect most customers will be willing to make that trade-off. However, Catenis users who prefer quicker access to auditability (e.g. 10-minute confirmations) or rock-bottom transaction fees (e.g. 5-hour confirmations) will be able to calibrate their target confirmation times accordingly.

• **Flash Network Will Enable Near-Zero Transaction Costs:** Catenis' Flash Network allows for near-zero transaction costs for messages sent between two distinct devices. The Flash Network has similarities to Bitcoin's Lightning Network[40] in that both will use payment channels to facilitate unlimited, free, trustless, off-chain transactions. In both cases, transaction fees are only paid to open and close a payment channel. This will allow users to conduct an unlimited number of transactions for the cost of an on-chain transaction when using the Flash Network.[20]

• **Flash Network is Easier to Implement Than the Lightning Network:** Unlike the Lightning Network, the Flash Network does not depend on Bitcoin enhancements such as the malleability soft-fork because Catenis users don't need to worry about counterparty risk in the same way that Bitcoin users do (see page 16-17). As such, the Flash Network can provide similar scalability while avoiding the design challenges that come with counterparty risk. Despite this lack of counterparty risk, final confirmation of message transmission / smart-asset transfer is still based on Bitcoin's consensus mechanism. This ensures full auditability for Catenis users.

• **Messages Over the Flash Network Will Be Fully Auditable:** Messages sent over Bitcoin's Lightning Network will not be fully auditable since only the transactions that open and close payment channels are logged to the blockchain, not the intermediate transactions. Unlike Bitcoin's Lightning Network, Catenis' Flash Network will log the log of all intermediate transactions into the final on-chain transaction that closes the payment channel. Although the final on-chain transaction will be large, this can be mitigated since the payload would be assembled into a Merkel tree (control document) and the hash of the tree's root would be placed inside the final payload. In layman's terms, this ensures that users will be able to easily retrieve and audit all the messages they received over the Flash Network by using the information embedded in the final on-chain Bitcoin transaction through the use of Catenis.[20]

- **Flash Network Will Retain Key Catenis Security Features:** As a peer-to-peer permissioned network, the Flash Network will retain many of the most important Catenis security features including permissioning, man-in-the-middle attack prevention, and DDoS prevention. In fact, Catenis customers actually gain an improved ability to defend against traffic analysis attacks since most Flash Network transactions will happen off-chain. The primary trade-off for Flash Network users is the loss of Perfect Forward Secrecy since ephemeral tunnels can't be created for every transaction in the Flash Network. This is a modest security trade-off for near-zero transaction fees, and we suspect users taking advantage of the near-zero cost of the Flash Network will be willing to make that trade-off for certain edge device scenarios. End users that are not willing to make that trade-off are likely using Catenis to protect high-value, mission-critical systems, in which case it would make sense to pay a premium (but still low) transaction fee for the added benefit of Perfect Forward Secrecy.[41]

Rapid Adoption Technology

Integrating Bitcoin Technology is Difficult: The Bitcoin blockchain is difficult to use since most IT staff are not familiar with blockchain protocols. It can also have a steep learning curve for firms that are not experienced in managing cryptocurrencies.

- **Catenis Simplifies Blockchain Integration for CTOs:** Most corporate IT engineers are not familiar with Blockchain protocols, but they are familiar with the use of web services as an integration medium. Catenis enables easy blockchain integration for the IT staff by creating a web services layer and an easy-to-use API. Adoption of Catenis is rapid and seamless, ushering in a world of developers who are unfamiliar with crypto-tokens and Bitcoins.

- **Catenis Simplifies Blockchain Integration for CFOs:** Although crypto-tokens are necessary for activating Catenis functionality (see page 24), clients who are new to crypto-tokens may prefer to pay via fiat (e.g. cash, credit cards, and checks) due to greater familiarity. To soften the learning curve for those customers, Blockchain of Things has created a fiat gateway so that new customers don't have to purchase tokens through exchanges. Instead, for a convenience fee, Blockchain of Things will directly sell the necessary tokens and feed it into the system to activate functionality for those clients. As customers gain experience managing cryptocurrencies, it would be logical for them to manage the crypto-tokens on their own to avoid paying additional convenience charges. In this way, we hope to encourage rapid adoption from new customers while providing a path toward eliminating convenience charges as customers progress up the learning curve.

Intelligent Contracts on a Bitcoin-Based Edge-Network

Catenis Integrates IoT Edge-Computing with Bitcoin: Intelligent contracts and autonomous agents run on computers and systems on the edge-network. This is known as edge-computing and is an emerging trend in the IoT.[42] These intelligent contracts can be written in any robust programming language, while the state and intellectual property control can be maintained by the application owner. Through Catenis, these intelligent contracts can listen to blockchain messages and smart-asset events while simultaneously communicating in real time with external data. As such they can trigger logic within the context of a blockchain and are not limited to bridges and gateways to take advantage of integration with external blockchains such as Ethereum, Zcash, or Hyperledger.

Catenis Enables Auditable Oracles: Oracles transfer off-blockchain information onto the blockchain, but often do it in a centralized way that can create a trust deficit. Through Catenis, edge-based intelligent contracts can act as an Oracle for blockchains such as Ethereum while using the Bitcoin blockchain as an independent, auditable trust layer. This process is facilitated by Catenis' easy-to-use API and message logging capabilities. By using the Bitcoin blockchain as the independent auditable trust layer, centralized Oracles can add trust layers to further improve user confidence.

IoT 2.0: Proof of Authenticity / Proof of Delivery

Overview

Catenis' enhanced feature set enables applications that go beyond the traditional scope of IoT to include a system to prove the authenticity and delivery of digital and physical products. With Catenis, one can mitigate both retail and supply chain product fraud, which is a $1.9 trillion per year global problem.[43]

Proof of Authenticity

Bitcoin Provides Proof of Authenticity in a Weak Form: Since the Bitcoin blockchain is an irreversible ledger, one may think that proof of authenticity should be simple. For example, a manufacturer could log the cryptographic fingerprint of a certificate of authenticity to the blockchain and provide the reseller/customer with a reference ID that allows the reseller/customer to see the certificate of authenticity on the blockchain. The problem is that Bitcoin is an open ledger and anyone can fingerprint content, even counterfeiters. A product counterfeiter could produce a certificate of authenticity, fingerprint the counterfeit, place it in the blockchain, and then provide the reseller/customer a reference ID allowing them to verify the fingerprint of a fake product. How would the reseller/customer ever know what is fake and what is not!?

- **Catenis Provides Proof of Authenticity in a Stronger Form:** To address this issue, Catenis enables permissioned third-parties to independently verify the originator of a blockchain entry, and therefore the identity of the actual product manufacturer. The owner of a Catenis virtual device can elect to prove their identity by demonstrating access to or ownership of the appropriate website domain, government registration, or third-party certification. Cryptographic proof of identity is placed into the Bitcoin blockchain so that any third-party can independently verify if the certificate of authenticity created by a given virtual device is genuine. This powerful mechanism for proof of authenticity can help mitigate supply chain and retail fraud.

- **Counterfeit Goods Is a Major Problem and Catenis Can Help:** Consulting firm

PWC estimates the global counterfeit goods market is $1.9 trillion per year, of which the largest segment is the $200 billion per year in counterfeit pharmaceuticals sold to consumers, pharmacies, and hospitals.[44] A key problem is that the technology currently used to fight counterfeits is insufficient and even hospitals are getting counterfeit medicines.[45 46] Catenis offers a technological leap forward with its proof of authenticity feature. For example, in the healthcare industry, a pharmaceutical manufacturer using Catenis could enclose the reference ID (i.e. the drug package ID) along with the medicine in a tamper-evident pill container. The pharmacy could confirm the medicine's authenticity by opening the tamper-evident container to retrieve the reference ID. The pharmacy would then use the reference ID to query the manufacturer's virtual device and receive cryptographic confirmation if the medicine is authentic.

Proof of Delivery

Catenis Enterprise can also be set to generate a confirmation when a target virtual device receives or reads a transmission. These deliveries and read confirmations are cryptographically provable and logged to the Bitcoin blockchain. As such, delivery confirmations and read receipts can be used to support tracking of information, documents, and physical assets.

IoT 2.0: Smart-Assets Powering the World

Overview

Catenis further expands its capabilities beyond the traditional scope of Internet of Things by empowering clients to digitize more things. This goal is accomplished by enabling customers to create customizable smart-assets and transfer them from one user to another.

Smart Contract Capabilities in Catenis Smart-Assets

Smart Contract Functionality in Catenis Smart-Assets: There are four key smart contract capabilities that will be supported by Catenis Smart-Assets:

- **Fee Payment Feature:** A Catenis Smart-Asset will be able to pay a fee to a specific address each time the smart-asset is transferred. This could be used to pay the original issuer of a sports ticket a commission on ticket resales.[47]

- **Expiration Feature:** A Catenis Smart-Asset will be able to expire after a set period of time. This could be used for loans, time-limited coupons, time-limited digital keys, etc.[48]

- **Smart-Asset Generation Rights:** A Catenis Smart-Asset will be able to give administrative privileges to a virtual device so that it can issue more of the same smart-asset. This could be used by organizations to create their own smart-asset or to grant that right to a subsidiary.

- **Smart-Asset Permissioning:** A Catenis Smart-Asset will be able to allow only certain addresses to receive that smart-asset. This could be used to restrict distribution of a smart-asset to pre-approved accounts (e.g. to limit asset sales to accredited investors).

Catenis Smart-Assets Can React to Permissioned Messages: In addition to the functionality described above, Catenis smart-assets can react to messages from Catenis virtual devices on a permissioned or open basis. For example, a message delivered to a virtual device can trigger the generation and distribution of numerous smart-assets. This contrasts with many other crypto projects in which the digital asset is nonresponsive. Further enhancing the power of our system, an intelligent contract on an edge-network device could be written in any robust programming language to trigger a reaction from a smart-asset. The triggering event could be any on-chain or off-chain data input. The combination of intelligent edge contracts and our secure message permissioning layer allows for the creation of powerful smart-assets and real-world disruptive solutions.

More Than Just a Representation of the Asset

Catenis Smart-Assets Can Deliver the Actual Payload: A Catenis smart-asset coupled with its messaging capabilities can transmit the actual digital payload. This contrasts with many other crypto projects in which the digital asset is simply a representation of the payload backed by the promise of a third party such that it must be requested via an unrelated external system. A Catenis smart-asset can be configured to transmit the actual stock certificate, house deed, or MP3 file so that the actual payload can be transferred from one user to another and not merely a representation of the item.

The Actual Payload Can Be Encrypted: The digital payload that travels with the Catenis smart-asset can be encrypted with the public key of the destination endpoint so that only the destination endpoint can access the payload by decrypting it with his/her private key. This contrasts with many other projects in which the payload is unencrypted and visible to the world.

Decentralized Platform for Third-Party Apps

Overview

Catenis is fundamentally a decentralized platform on which third-party developers will be able to build applications using Catenis' core functionality as a building block (e.g. secure messaging, smart-assets, etc.).

Applications built on Catenis can be sold/licensed to others so that the full profit accrues to the third-party developers who built the app. Beyond this inherent profit incentive, we aim to further encourage third-party development by allocating 10% of the BCOT token supply as a bounty for those who build useful apps. BCOT tokens are the utility tokens that are needed to activate functionality in Catenis (see page 24 for additional details). Given the multiple layers of incentive, we expect an ecosystem of third-party apps to grow on Catenis.

Potential Third-Party Apps

In this section, we highlight six of the many categories in which a third-party programmer could focus future development efforts.

• **Industry-Specific Apps for Securing the IoT:** A core functionality in Catenis is the secure messaging feature and its ability to secure the IoT. However, different industries and different parts of an operation will prefer to leverage this feature for different use cases. As such, a third-party developer could build an industry-specific or function-specific IoT application that leverages Catenis' security to bring tailored solutions to different segments of the IoT market.

• **Industry-Specific Apps for Detecting Counterfeit Goods:** Catenis' proof of authenticity capability is a key feature that can be used to help eliminate the $1.9 trillion per year in global counterfeit goods sales. However, different industries will need to apply this capability in different ways. As such, a third-party developer could build an industry-specific app that addresses the nuances of a given industry, while building off the fundamental proof of authenticity feature in Catenis.

• **Equity Marketplace:** Delaware state law allows US corporations to issue and trade shares on a blockchain to streamline the costly and lengthy share settlement process. Catenis will have the functionality to encode smart-assets that can transfer the actual stock certificate. In addition, Catenis has the functionality to abstract cryptocurrencies so that traditional equity investors could buy shares in companies from their regular brokerage firm without ever having to directly deal with cryptocurrency. A third-party developer could leverage this functionality to build an equity marketplace that would streamline the share settlement process for the finance community

• **Wallet for Token Sales:** Using Catenis, one can program an autonomous agent to automatically create and distribute smart-assets conditional on the receipt of a message. This allows Catenis to be a platform for the efficient, transparent distribution of any digital asset, including but not limited to token sales. However, to make a token sale platform fully functional, one would need to build an appropriately configured wallet. The necessary wallet would be a Bitcoin wallet that supports Catenis smart-assets. As such, a third-party developer could build this wallet to enable token sales on Catenis.

• **Hardware as a Service:** Catenis smart-assets can be set to expire after a set period so that they can be used for a time-limited digital key. As such, it is possible to enable secure, blockchain-based hardware as a service since digital keys in the form of a smart-asset can unlock functionality in remote hardware connected to a Catenis virtual device. A third-party developer could leverage this functionality to build industry-specific apps that address the needs of a given market.

• **Ticket Marketplace:** A Catenis smart-asset will be able to empower the original issuer of the asset to earn a commission on resales of that asset. By leveraging this feature, concert ticket issuers will be able to earn a commission if their tickets are resold on a secondary marketplace. A third-party developer will be able to commercialize this functionality by building a ticket marketplace that supports Catenis smart-assets and integrates with major ticket issuers.[48]

• **And More:** The above six categories were simply designed to offer a flavor for the types of third-party apps that can be built on Catenis. The list was not comprehensive as there are additional possibilities. Please reach out to us at Blockchain of Things, Inc. if you have an idea for a decentralized app and you wish to discuss the viability of your project.

Decentralized App Store and Certification Program

After our token sale, we will launch a Catenis Decentralized App Store directory where third-party developers will be able to list and sell their apps. While not required, developers can request that their apps are certified by Blockchain of Things, Inc. to ensure that their apps have been built using best practices.[49]

Economics of Blockchain of Things, Inc.

Overview

Blockchain of Things, Inc. offers several products/services that customers can purchase: **1)** a Pilot Development Kit for API integration; **2)** tiered subscription levels for the creation of Catenis virtual devices (e.g. to connect IoT devices to Catenis endpoints); **3)** enterprise licensing with maintenance support packages; **4)** professional services to assist businesses with integration; and **5)** BCOT tokens for all key functionality in the system.

Please review the company website for additional details on the first four products/services. Further details on BCOT tokens follow in the next section.

BCOT Tokens

The BCOT token is the utility token that powers all key functionality in both Catenis Enterprise and any future Blockchain of Things, Inc. products. When used in Catenis, this token converts into internal Catenis credits which activate key system functionality including secure message transmission, blockchain data logging, smart-asset creation, and smart-asset transfers.

BCOT tokens will be distributed pursuant to a token sale that will establish a maximum total token supply (see BCOT Token Sale Structure document for details). At no point will the total supply of BCOT tokens rise higher than the maximum total token supply. This will be cryptographically provable.

Cost Structure

BCOT token sales represent revenues for Blockchain of Things, Inc. The underlying bitcoin transaction fees represent a large portion of our cost of goods sold, a real cost that Catenis must pay to bitcoin miners for every secure message that is sent, data that is logged, smart-asset that is created/transferred, etc.

Since the underlying cost of Catenis services varies based on the bitcoin transaction fee market (and other factors), BCOT tokens do not activate a pre-determined quantity of services. For the purposes of acquiring services on Catenis, a BCOT token's value is determined based on the market value of the token at that time. The price of Catenis' services will vary based on changes to the underlying costs (see next paragraph for the cost structure forecast).

We currently estimate 50% of revenues will be allocated toward cost of goods sold (COGS), 25% toward sales/general/administrative (SG&A), 15% toward additional development work, and 10% for corporate profits. This cost structure forecast is an estimate with a high degree of uncertainty and is subject to significant revision based on changes in competitive dynamics and business needs.
Flexible and Scalable N-Tier Software Architecture

An n-Tier Architecture (aka a layer approach) has several benefits including flexibility, scalability, management ease, and security. See diagram of Catenis' software architecture.

Development History and Future Work

The Catenis Enterprise Development History and Timeline depicts past & future Milestones and is available as a separate document and listed on the blockchain of Things BCOT token website (bcot.blockchainofthings.com).

The Catenis Enterprise and Catenis Services may undergo significant changes over time. The functionality described under the caption "Q1 2018 and Beyond" in the Development History and Timeline document and referred to in the text corresponding to footnotes 20,22,42,48 and 50 of this whitepaper may never be developed by the Company. For the functionality described in the Whitepaper that is currently available at the time of purchase of BCOT Tokens under the applicable purchase agreement, we may have to make changes to the specifications of the BCOT Tokens, Catenis Enterprise or Catenis Services for any number of legitimate reasons. This could create the risk that the BCOT Tokens, Catenis Enterprise or Catenis Services, as further developed and maintained, may not meet your expectations at the time of purchase of BCOT Tokens under the applicable purchase agreement.

---

1. http://www.bain.com/Images/BAIN_BRIEF_How_Providers_Can_Succeed_In_the_IoT.pdf
2. Scott Helme May 2014: "Perfect Forward Secrecy - An Introduction" https://scotthelme.co.uk/perfect-forward-secrecy/
3. Joseph Poon, Thaddeus Dryja: "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments" https://lightning.network/lightning-network-paper.pdf
4. https://www.strategyand.pwc.com/reports/counterfeit-pharmaceuticals
5. Colored Coin Protocol: https://github.com/Colored-Coins/Colored-Coins-Protocol-Specification/wiki
6. McKinsey Global Institute, June 2015: "The Internet of Things: Mapping the Value Beyond the Hype"
7. http://www.bain.com/Images/BAIN_BRIEF_How_Providers_Can_Succeed_In_the_IoT.pdf
8. http://www.gartner.com/newsroom/id/2905717
9. http://www.gartner.com/newsroom/id/3165317
10.http://www.gartner.com/newsroom/id/3598917
11. http://www.gartner.com/newsroom/id/3598917
12. http://www.gartner.com/newsroom/id/3598917
13. McKinsey Global Institute, June 2015: "The Internet of Things: Mapping the Value Beyond the Hype"
14. http://cdn.iotwf.com/resources/6/iot_in_manufacturing_january.pdf
15. http://marketing.mitsmr.com.s3.amazonaws.com/PDF/57380-MITSMR-EY-GE-Case.pdf
16. McKinsey Global Institute, June 2015: "The Internet of Things: Mapping the Value Beyond the Hype"
17. McKinsey Global Institute, June 2015: "The Internet of Things: Mapping the Value Beyond the Hype"
18. https://www.nytimes.com/2014/12/01/business/working-the-land-and-the-data.html

19. http://www.bain.com/Images/BAIN_BRIEF_How_Providers_Can_Succeed_In_the_IoT.pdf
20. The gateway functionality referred to in this section relates to functionality that has not yet been developed and is expected to be developed in 2018 or thereafter. Please refer to the Development History and Timeline available on the Blockchain of Things BCOT token website.
21. https://blockchain.info/charts/estimated-transaction-volume-usd?timespan=2years
22. The completion of the complete system state encoding referred to in this section relates to functionality that has not yet been developed and is expected to be developed in 2018 or thereafter. Please refer to the section captioned "Q1 2018 and beyond" in the Development History and Timeline document available on the Blockchain of Things BCOT token website.
23. https://blockstream.com/satellite/blockstream-satellite/
24. https://www.blockstream.com/satellite/faq/
25. McKinsey Global Institute, June 2015: "The Internet of Things: Mapping the Value Beyond the Hype"
26. McKinsey Global Institute, June 2015: "The Internet of Things: Mapping the Value Beyond the Hype"
27. McKinsey Global Institute, June 2015: "The Internet of Things: Mapping the Value Beyond the Hype"
28. http://www.bain.com/Images/BAIN_BRIEF_How_Providers_Can_Succeed_In_the_IoT.pdf
29. https://www.csoonline.com/article/3077537/internet-of-things/security-concerns-rising-for-internet-of-things-devices.html
30. http://451alliance.com/Portals/5/2016reports/101916_3q16_iot_report/3q16_iot_report.pdf
31. https://securityintelligence.com/a-primer-on-iot-security-risks/
32. https://blockchain.info/charts/estimated-transaction-volume-usd?timespan=2years
33. https://themerkle.com/what-is-the-dandelion-anonymization-proposal/
34. https://github.com/ipfs/ipfs
35. Pieter Wuille, Feb 2012: "BIP 0032: Hierarchical Deterministic Wallets" https://github.com/Bitcoin/bips/blob/master/bip-0032.mediawiki, Feb 2012.
36. Alex Akselrod. Apr 2014: "ESCHATON" https://gist.github.com/aakselrod/9964667
37. Peter Todd Dec 2014: "Near-zero fee transactions with hub-and-spoke micro- payments" https://www.mail-archive.com/bitcoin-development@lists.sourceforge.net/msg06576.html
38. Cooper, F Gont et al.: "Privacy Considerations for IPv6 Address Generation Mechanisms" https://tools.ietf.org/html/draft-ietf-6man-ipv6-address-generation-privacy-07
39. Scott Helme, May 2014: "Perfect Forward Secrecy - An Introduction" https://scotthelme.co.uk/perfect-forward-secrecy/
40.https://bitcoin.stackexchange.com/questions/43700/how-does-the-lightning-network-work-in-simple-terms/43701#43701
41. The flash network system services referred to in this section relates to functionality listed under "2018 and beyond" in the Development History and Timeline document . Please refer to the development history and timeline document available on the Blockchain of Things BCOT token website.
42. https://techcrunch.com/2017/08/03/edge-computing-could-push-the-cloud-to-the-fringe/
43. https://www.strategyand.pwc.com/reports/counterfeit-pharmaceuticals
44. https://www.strategyand.pwc.com/reports/counterfeit-pharmaceuticals
45. https://www.strategyand.pwc.com/reports/counterfeit-pharmaceuticals
46. http://www.who.int/bulletin/volumes/88/4/10-020410/en/
47. The enhanced smart asset capabilities this section relates to functionality that has not yet been developed and is expected to be developed in 2018 or thereafter. Please refer to the section captioned "Q1 2018 and beyond" in the Development History and Timeline document available on the Blockchain of Things BCOT token website.
48. https://www.strategyand.pwc.com/reports/counterfeit-pharmaceuticals
49. The Catenis Enterprise app store relates to functionality that has not yet been developed and is expected to be developed in 2018 or thereafter. Please refer to the section captioned "Q1 2018 and beyond" in the Development History and Timeline document available on the Blockchain of Things BCOT token website.