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.

---

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