White Paper

Open Registry for IoT

Creating an immutable and interoperable digital identity for real world things

Abstract: With a blockchain-hosted Open Registry for Internet of Things, we envision a future where everything—from your car, to a work of art, to the glass of wine you drink at the end of a long day—can have a unique and unforgeable identity, life, and history on the Internet. This identity is created with a microchip embedded in the product and registered to a blockchain. This white paper is provided to share the vision and roadmap for Chronicled Open Source with a goal of establishing an ecosystem of like-minded developers and partners who share a common vision and interests.

To submit your comments or feedback please reach us here:

Forum: http://forum.chronicled.org/
Slack: http://slack.chronicled.org

Prepared By:
Chronicled
Open Source
Team

Prepared For:
Prospective
Ecosystem
Partners

Preface

Hitchhiker's Guide to the Internet of Things

Imagine that you are a 21-year old hitchhiker in the year 2029, and you decide to visit Silicon Valley. You arrive in Palo Alto wearing your augmented reality glasses and lock eyes on a car displayed in front of the Palo Alto Electric Car Museum. The glasses inform you, "This is a 2015 Tesla Model S". Once you are in proximity of the car, additional information about the car – where it was manufactured, the designer's original drawings, the owner's manual, a Model S driving simulator, a list of prior owners, etc. – are all accessible via voice command. You have a digital treasure trove of data about the product model and this individual automobile available to you instantly. Similarly, when you arrive at the family home of Steve Jobs, long ago converted into a cultural heritage site, the glasses inform you, "You are at 2101 Waverly Street, Palo Alto, CA. Would you like to purchase a tour?" You purchase the tour via voice command, and as you approach the door to the home it opens automatically. You just purchased a digital token that provides a two-hour period of access. None of the items in the home are compatible with your augmented reality glasses. You see an old Apple iPhone 5, a pair of Steve Jobs' iconic white New Balance sneakers, a pair of his Levi's blue jeans, and one of his wife's Chanel handbags, all clearly antiques because your augmented reality glasses cannot "discover" them. No information pops up—these objects seem lifeless and terribly out of date. They have no digital life. It even crosses your mind that the items could be counterfeits, and remember your parents talking about how around the time of Steve Job's death the American economy was being flooded with fake products. Feeling thirsty after the tour, you stop by a nearby restaurant and order a bottle of beer. When the bottle comes to your table, the basic product information is displayed on your augmented reality glasses, "Lagunitas IPA, 2028 Vintage—how would you like to pay?". You answer, "from my digital wallet" and twist off the cap. You feel lonely and wish your friends and family were here to share the experience—so you post a video from your glasses to your social media, overlaying date, time, temperature, and geolocation onto the video, which is immediately shared to the social profile for Lagunitas IPA, 2014 Vintage beer as well.

With a blockchain hosted Open Registry for the Internet of Things, everything—from your car, to a work of art, to the glass of wine you drink at the end of a long day—can have a unique and unforgeable digital identity.

Table of Contents

INTRODUCTION

How close are we to realizing The Hitchhiker's 2029 Vision, today? The short answer: we are very close. More than 2B consumers globally have a smartphone in their pocket supporting BLE and NFC protocols, and the BLE and NFC chips are getting very cheap. They will be less than $1 at volume within 18 months. The BLE protocol already works with both Android and iPhone devices. The NFC protocol already works openly with Android devices, and is rumored that Apple is circulating "NFC kits" to major Brands, and discussing a timeline for opening-up the NFC reader capability in the iPhone. Secure element and Elliptical Curve Cryptography (ECC) technology is optimized to work with BLE and NFC protocols and Chronicled is leveraging these cryptographic standards to create a secure system.

Technologists are further behind on the development of augmented reality. Nevertheless, we are moving in the right direction and today consumers can use their smartphone to interact with products that contain a BLE chip and "range for" and "discover" smart products up to 100' away via a list screen on the smartphone.

In summary, the smart phone devices, chips, secure elements, chip communication protocols, and cryptographic protocols are in existence—so, what is still missing?

1) A common and interoperable back-end to support the growth of this new ecosystem of 'smart products'. Currently consumer brands are running experiments with chips registered to private, proprietary back-end databases. This solution can work, but it is going to lead to two major problems:

- Without interoperability for developers, the growth of the entire ecosystem will be stunted,
- Brands will need to keep up with numerous chip type, versions, and communication protocols on an in-house basis over the coming decades,

2) A seamless and easy to use solution. It needs to be dead easy for an artist, wine authenticator, sneaker customizer, firearms appraiser, or major Fortune 1000 Brand to order product identity chips, add to products, and link product identities to the registry.

3) Every Registrant needs to be able to easily supplement its existing App with a 'smart product authentication screen' and integrate other user engagement plug-ins that leverage this product authentication capability via an open source plug-ins library.

Introducing Chronicled Open Source

In order to bring the world closer to the 2029 Hitchhiker's Vision and immediately combat counterfeit product fraud, we are launching Chronicled Open Source, a free-to-use toolkit that will address the missing links described above. Key building blocks include the Open Registry for IoT and Open Registry Explorer, and also Registration SDK and Verification SDK to interact with chips added to the registry. This open source toolkit is targeted for individuals, small business, and also Brands and the digital agencies who support them. The toolkit will make it easy to introduce smart products that contain strong digital identities. A hosted version of the open source do-it-yourself toolkit and product authentication chips available from Amazon.com will make it easy for individual artists, product authenticators, and product customizers to access and use the system as well.

ABOUT US

Founding Sponsor

Chronicled, Inc. is a technology company with 19 employees. The Company is playing the role of founding sponsor for the Open Registry for IoT, described herein, and hopes that many hobbyists, partners, and collaborators – and even competitors – can join hands around this open source vision. The Company has three primary revenue lines, microchip resales, professional services, and cloud hosting services, and is based in San Francisco.

Team

Business, Product, Marketing

- Ryan Orr
- David Aho
- Samantha Radocchia
- Sean Medcalf
- Kim Pham
- Andy Mai
- Bryon Sheng
- Rob Leo
- Ray Cruz

Software Development

- Maurizio Greco
- Allen Sogis-Hernandez
- Josh Beam
- Dylan Ross
- Duncan Smith
- Maksym Petkus
- Orlando Castillo
- Johann Barbie
- Andrey Zamovski
- Drew Stone

Technical Advisors

- Adam Krellenstein
- Andrew Lockhart
- Adam Marsh
- Alex Mizrahi
- David Schwartz
- D'Wayne Edwards
- Zaki Manian

Web Presence

- **Chronicled Open Source** – all work related to the Open Registry for IoT will be published at www.chronicled.org.

- **Chronicled Open Source Forum** – a public forum to discuss the present proposal and the open source project is available at forum.chronicled.org.

- **Open Source Community -** anyone interested in collaborating on the project, reach out on Slack channel, http://slack.chronicled.org.

- **Chronicled, Inc.** – password-protected platform for clients to order and provision microchips for their products, will be available at www.chronicled.com.

- **Chronicled Wallet** – consumer app to interact with authentic products is available in the iOS App store under the name "**Chronicled for iPhone**."

- **@chronicled** – public Instagram account with photos of collectible sneakers authenticated with product identity tags. The collectible sneaker vertical was used to validate the concept of consumer and luxury product authentication.

OVERVIEW

Vision

We envision a future where any product can have a identity, life, and history on the Internet. This identity is created with an embedded microchip registered to a blockchain, which is a decentralized network not controlled by any central authority.

Problem

The Problem in Consumer Products

Serial numbers, QR codes, UPC codes, barcodes, and other unique identification systems can all be cloned or copied. Currently the global market for fake and counterfeit products is estimated to be as large as $1.8T—which is 10% of the U.S. gross domestic product. This is enormous problem facing Fortune 1000 Brands today, see: http://www.economist.com/news/business/21660111-makers-expensive-bags-clothes-and-watches-are-fighting-fakery-courts-battle.

The Problem in Augmented Reality

The world is ready to interact with the physical environment of products everywhere, but, without a strong digital identity embedded in every product, progress will be much slower than is possible.

The Problem in IoT

The consumer IoT is progressing, and many large Brands are experimenting with adding microchips to consumer and luxury products. However, without a common registry and authentication protocol, major interoperability issues and roadblocks will ensue for Brands, developers, and consumers.

The Problem in Autonomous Machines

Amazon wants to deliver packages using drones, Google is pioneering self-driving vehicles, and Tesla added a snake charger to fuel a car without human intervention. The more autonomous machines are deployed, the more these will need to interact with humans and with each other. Without a secure system of digital identity, these machines won't be able to safely identify one another or perform cooperative tasks.

Solution

Chronicled is creating a decentralized system of product identity registration and verification. A developer can order encrypted microchips, add them to consumer or luxury products, register the chips/products to a blockchain hosted registry, download a code snippet to supplement any existing App with smart product authentication functionality, and leverage/contribute to libraries of user engagement plug-ins to create bespoke consumer experiences for IoT products on top of the decentralized registry.

CHARTER

Principles

Mission: To create a decentralized and open source toolkit and ecosystem for any product creator, product authenticator, product customizer, or individual to assign a secure digital identity to a physical object by embedding a microchip and linking it to a blockchain record.

Open Source: All software published on the Chronicled Open Source platform will be licensed under the Apache license and will be freely available for open use by the blockchain and IoT developer communities and the world at large.

Community: The project will operate under principles of openness, transparency, and respect of community participation.

Sponsor: Chronicled, Inc. is initially playing the role of project sponsor. However, the intent is to make available a fully decentralized system as a public good or utility that lives on the blockchain. We will seek ongoing participation from many partners and technology teams at other companies. Our goal is to enable usage of the system without any ongoing dependency on Chronicled, Inc.

USER DEFINITION & NEEDS

System Users: Who can register products?

Anyone. The system is decentralized, open, and accessible.

Practically speaking, there are probably three initial classes of market participants who would benefit most from the registry:

- **Product Creators** – artists; small, midsized, and large Brands.
- **Product Authenticators** – art authenticators, wine authenticators, antique furniture authenticators, vintage firearm authenticators, etc.
- **Product Customizers** – automobile customizers; motorcycle customizers; sneaker customizers, eg. see @Mache and @TheShoeSurgeon on Instagram; etc.

For purposes of their interactions with the Open Registry for IoT system described herein, these three classes of market participants are referred to as “Registrants”.

Rationale for an “open” Registry

An “open” Registry, that runs on a fully decentralized basis, is a valuable missing element in the evolving consumer IoT ecosystem.

There are many use cases for individuals and small businesses – i.e. art collectors, artists, sneaker customizers, wine authenticators, firearm’s refurbishers, antique furniture appraisers – to add a chip to create a digital identity for a product. Secondary authentication services exist in numerous verticals including art, collectible sneakers, autographed sports memorabilia, vintage firearms, wine, and other classes of collectibles. There are also many small businesses that upgrade, customize, or refurbish products – i.e. sneaker customizers, fine art refurbishers, automobile

customizers, motorcycle customizers, etc. All of these businesses are small and decentralized, and they need a similarly decentralized system to support their business needs. Moreover, none of these small-businesses that provide product customization or authentication services has the scale to create a system on a blockchain for product registration and verification, but, as with Etsy, a large number of “little guys” sharing a common “open” platform and protocol can create a meaningful volume of business and value in the world.

Moreover, there are also many medium- and large-sized Brand’s that sell consumer and luxury products, who also need an “open” registry. Each Fortune 1000 Brand working in its own self-interest will want to include microchips in its products to make it impossible for counterfeiters to compete, enhance consumer engagement, and track product usage patterns over the lifecycle; but, if each Brand goes about solving this problem of ‘product authentication’ in its own way, then the consumer will need 100s of different Apps to verify authenticity of a product that he or she encounters out in the world, and growth of the ecosystem will be stymied. By agreeing that product authentication should be a free, public, utility-like service, and registering the chips to an open registry on an attributed or anonymous basis, Brands can -- without any added cost or risk -- contribute to creating an open and interoperable standard for product identity verification.

With an open standard, CTOs and software developers at every Brand and digital agency will find it easy to integrate new product authentication and other user engagement tools into their products and Apps, product registrations become interoperable across all Apps, and consumers can gain a seamless experience with IoT connected products.

A valuable attribute of the Open Registry for IoT, as described herein, is an option to openly publish a link to a cloud hosting service where a consumer can access additional information about a product, e.g. photos, videos, operating manuals, promotions, timelines of ownership, social interactions, etc. Thus, the Open Registry for IoT becomes like a central switchboard or reverse look-up table, and, additional product data can be protected and accessed only when a user is in physical proximity.

System Usage

The Open Registry for IoT:

- makes it possible to authenticate the identity of NFC and BLE chips, i.e. counterfeit detection

- makes it easy to associate chips with branded products and digital content in a secure way that cannot be hacked or duplicated, e.g. sneakers, handbags, automobiles, drones, wine, furniture, etc. can all have a strong, verifiable digital identity on the Internet

- makes it simple for third-party developers to add a Verification SDK to an App to verify the identity of a chip and associated branded product against its blockchain registration

- once the unique digital identity of a chip or branded product can be verified in a standard and interoperable way, this makes it easy for third-party App developers to build consumer-engagement plug-ins that work with any NFC or BLE module

SYSTEM ELEMENTS

Encrypted Chips

The registration protocol is technology and vendor agnostic. While it supports BLE and NFC communication methods today, new protocols (and protocol versions) are easily added. Any vendor-specification format can be appended for universal lookups.

Chips will be available as follows:

- demo quantity of 5 chips from Chronicled,
- lots of 10 chips or 100 chips for artists and small businesses for purchase on Amazon.com, and
- larger quantities of 10,000 chips or more from silicon chip manufacturers or re-sellers (see Ecosystem Partners section towards end).

Smart Contracts

Registration

The Registry will establish a framework whereby a Registrant can add product registrations to the Open Registry. Registrants can optionally complete a voluntary process of identity confirmation, so that their chip and product registrations appear with a “confirmed identity” badge, or, Registrants can choose to add registrations to the Open Registry on an anonymous basis. For example:

- A winery may decide to verify its identity and register products publically, to certify that there are only 5,000 bottles in a specific limited edition release
- An accessories company may prefer to register their luxury handbags anonymously, so that competing accessories companies cannot lookup the size of a specific handbag release,

Product Registry

- Stores a list of all registered product identities
- Hosts a list of Registrants with confirmed identity status
- Provides methods for registering new products for Registrants

- One by one
- Batch
- Retroactive (i.e. hash of serial number registry)

Registration SDK

Registration of chips can be accomplished from the Registration SDK hosted on your own server, from an instance of the registration SDK hosted on Chronicled.org.

JavaScript library with the following features:

- Register a new product(s) in Open Registry
- Create Ethereum account from entropy
- Encrypt and persist Ethereum account
- Load and decrypt Ethereum account
- Setup recovery for loss or compromise of Ethereum account
- Recover lost or compromised Ethereum account
- Ability to switch between local (custom) and hosted key store

Verification SDK

A standard device-chip authentication protocol published as open-source code that enables any Registrant to easily upgrade their App with a product authentication screen, or to install other user engagement plug-ins that require product identity verification.

Many Brands have struggled to entice consumers to install and use their Apps, and this new functionality may be an important new tool to drive consumer engagement.

iOS, Android, JavaScript libraries that allows:

- Check product existence in registry using product identifier (supports NFC and BLE communication protocols).
- Get product's meta-data.

Open Registry Explorer

Similar to a classic Blockchain Explorer, allows a user to browse all data that available

in the Registry.

Features:

- List of recent transactions
- List of all certified Registrants
- Statistics
    - Total products registered
    - New products registered today
- Search:
    - By transaction id
    - By Authenticator
    - By product id
- Charts:
    - Daily transactions volume
    - Number of authenticators

SYSTEM ARCHITECTURE, PROOF OF AUTHENTICITY & PROOF OF PROXIMITY

The Registry will establish a framework whereby Registrants can add product registrations as a basis of product identity verification. Once a product is included in the registry by a Registrant, a device can authenticate the chip in the product using the **"proof of authenticity"** process outlined in Figure 1.

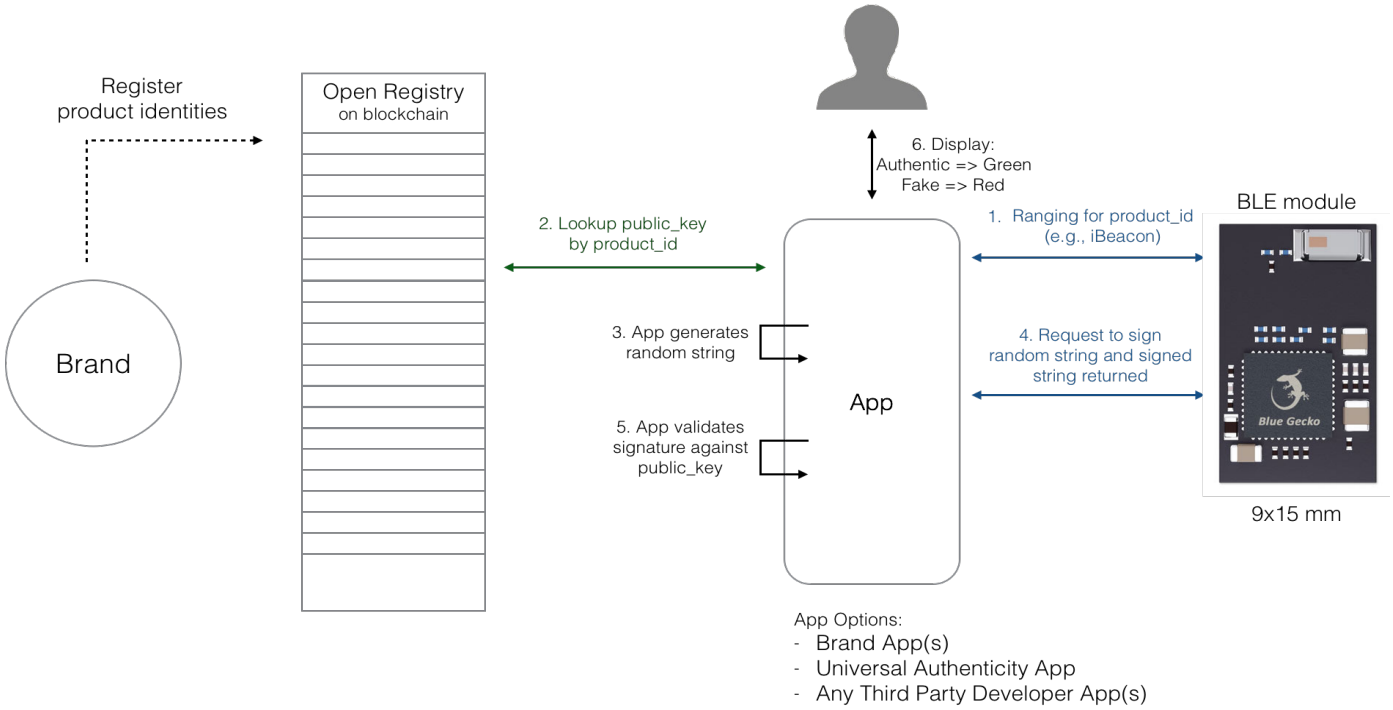

Figure 1. Proof of Authenticity

If a Registrant chooses to register products anonymously without associating its identity to it's Ethereum address, then an App can use **"proof of proximity"** as a basis of gaining access to additional digital content from the Brand's designated cloud service. Specifically:

- The device meets the chip (for instance, via iBeacon ranging) and performs a lookup on the registry to verify if the chip is registered.
- The device requests authorization to access digital content to the cloud service specified in the Service URL.
- The cloud service delivers a random string to the device and requires a "proof of proximity" before serving the device exclusive content.

- The device submits the random string to the chip, which the chip then returns signed using its secret private key.
- The signed random string is the “proof of proximity” that the device submits to the cloud service to gain access to the digital content.

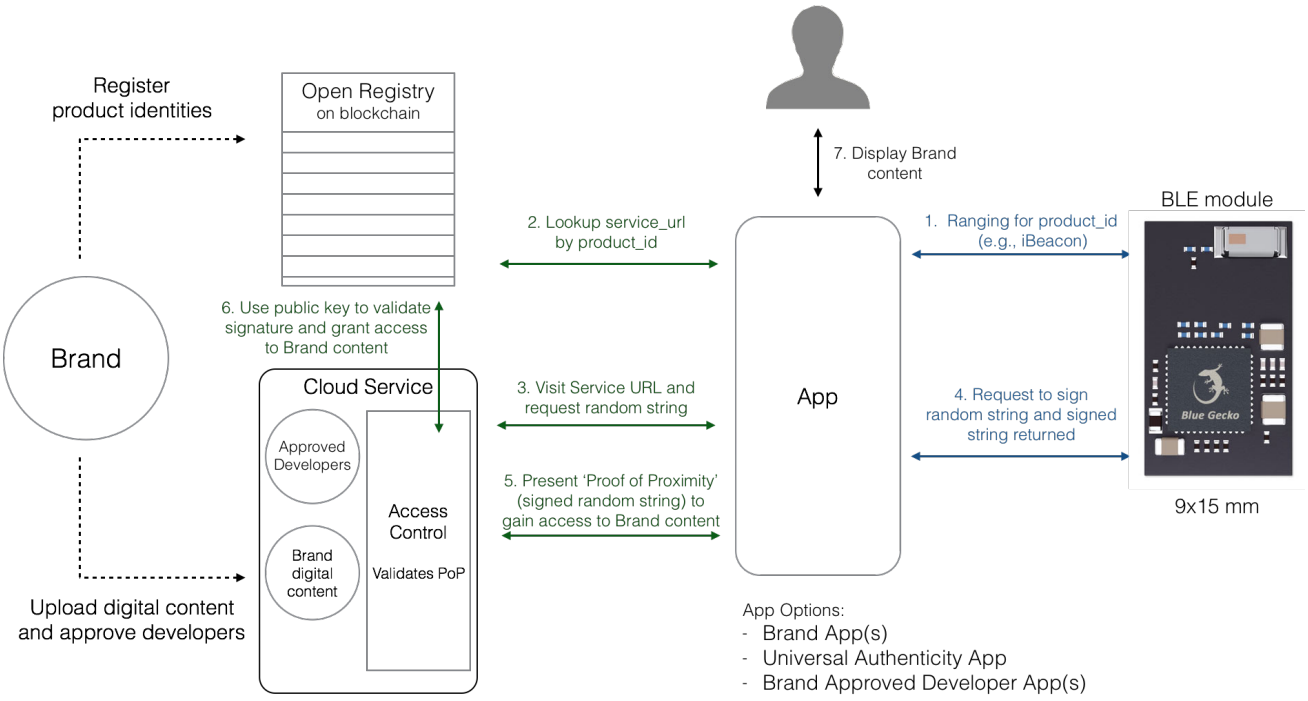

Figure 2. Proof of Proximity

This sequence of actions can happen nearly instantaneously. This hybrid architecture achieves the following benefits:

- All silicon chip companies and Brands can use the same Open Registry to create interoperability for consumer IoT ecosystem
- Brands can choose to register products on a fully anonymous basis restrict consumer access to product content via the proof of proximity test, and obfuscate identity at the registry level by including a proxy address to the cloud service
- Brands can dynamically enable third party developers to serve-up their digital content (e.g. product catalog and images) using “proof of proximity” without disclosing their overall database of product identities and content, and they can monitor how these partners are utilizing the digital content
- Brands can gain independence from their cloud services providers and retain the ability to move digital content to replacement cloud services providers by updating the Service URL for each product registration in the registry

The blockchain-hosted system described herein is neutral, standardized, interoperable for different microchip types, and can be used anonymously—a part of the Internet itself that can be used by all creators, authenticators, customizers, and consumers as a public resource. We envision the Open Registry as a permanent public good that operates according to its published protocol.

Brands face zero risk of loss of business intelligence if they prefer to remain anonymous when they register products to the Open Registry. Consumers face no risk of being tracked if they wish to interact with products without disclosing personal identity information. Brands gain flexibility if they should ever wish to replace a cloud services vendor that is hosting private data.

Most importantly for the growth of the ecosystem, App developers can easily update consumer Apps with product authentication and user engagement functionality using standard open source code. Enhanced interoperability greatly enhances the consumer experience and the growth of the consumer IoT.

As more consumers interact with smart products, Brands will learn more about consumer interaction patterns, and tracking of product possession can be converted into a more explicit relationship between a Brand and its patrons through various user engagement plug-ins that a Brand can add to its Apps.

In summary, Brand registrants can accomplish the following functions:

- **Proof of Authenticity** – by virtue of registering products to the registry with encrypted chips, Brands can establish a basis of strong identity and authentication for their products that cannot be cloned or copied by a counterfeiter.
- **Proof of Proximity** – by publishing private data about a product that can be accessed only when a consumer is in proximity of a product, a Brand can serve up extensible and interactive content or offers with respect to a specific product. Proof of proximity becomes a basis for digital content distribution and a new channel to share content with consumers via IoT.
- **Proof of Possession/Patronage** – when a consumer has been in proximity of a product for a threshold period of time, or based on a string of multiple repeated product authentications, Brands can offer specific content or offers based on their consumers product-interaction patterns and can strengthen the link of direct connectivity with its consumers by offering additional engagement opportunities.

For example, user engagement plug-ins can enhance user engagement around NFC and BLE chips for retail, social, augmented reality, brand-to-consumer interaction, loyalty, gaming, finance, and insurance applications. By creating interoperability and a suite of open source plug-ins for consumer IoT, the Open Registry for IoT may lead to enhanced demand for IoT chipsets and consumer interaction with physical products.

DISTRIBUTION

Initial Validation in Sneakers

So far, using a non-open/non-public version of the technology system described herein, Chronicled has authenticated thousands of items in the footwear, apparel, and luxury goods/accessories industries, and has built a business, product, and software development team consisting 19 team members.

Our system and workflows are now hardened and ready to scale to other market verticals. Moving the registry and registration protocol over to an open blockchain implementation will occur in Q3 2106, and is our next step prior to opening up fully.

To see photos of the Chronicled sneaker authentication activities, visit @chronicled on Instagram. (Or see: *https://www.instagram.com/chronicled/*)

Next Markets & Evolution

Once the system is operating on a fully decentralized basis, the following industry use cases and evolution of the business are imagined:

- Chronicled intends to distribute writable product identity tags via Amazon.com to support individuals and small business who wish to add a digital identity to their physical products, e.g. sneaker authenticators, motorcycle customizers, artists, and other hobbyists.

- Over a dozen large Brands have expressed interest in proof of concept implementations and development of bespoke user engagement experiences across the following industries: augmented reality; fine art, wine, and furniture; automobiles; hoverboards; men's/women's fashion, handbags, fragrances.

- Over the next 18 months, we foresee several silicon chip companies starting to offer blockchain registration as a standard default feature of their NFC and BLE microchips, so that they have a standard "birth certificate lookup" for all of their

chips across product lines, and so that Brands can invoke libraries of user engagement plug-ins as a value-added service downstream.

- In the medium-term, we hope that other startups can create new business models on-top of this secure and open layer of identity for IoT. For example, on-demand mini-storage services, clothing rental services at airports, insurance for high-value collections/items, second-factor authentication through possession of “things”, etc.

- Eventually, after several years of evolution, governments managing registries for drones, automobiles, boats, aircraft, and other vehicles may require that all registered vehicles have an encrypted digital identity for safety and security, especially as we move into an era of autonomous unmanned vehicles.

BLOCKCHAIN INTEGRATION PHASES

Phase One

The first phase of the project, now complete, was to experiment with various blockchain platforms as a foundation for an Open Registry for IoT. After 18 months investigating the applicability of Bitcoin, Blockstream, Colored Coin, Counterparty, Factom, Ethereum, Hyperledger, Rootstock, Thing Chain, and other blockchain 2.0 frameworks, we determined that the Ethereum framework was the most suitable as a point-of-departure for our product authentication functionality (see Annex 3). We initially launched our sneaker authentication protocol on a private implementation of Ethereum, enabling experimentation and trial-and-error learning with thousands of sneaker and luxury product registrations.

Phase Two

The next phase of the project, scheduled for Q3 2016, is to open up our private blockchain implementation, and to convert this to a fully decentralized system. Through our experience with collectible sneakers over the past 18 months, we have learned that it makes sense to separate development of the blockchain-hosted authentication functionality from claim, transfer of ownership, and provenance functionality, and so version one of the open blockchain system will be exclusively focused on creating the "product birth certificate" and registration and verification functionality that is open source and open to use. We will continue to experiment with claim, transfer of ownership, and provenance functionality on our own private back-end. Phase Two of the project is fully funded from our recent Series Seed financing.

Phase Three

After continued and thorough experimentation and testing on our own private back-end, we hope at some point to also transition claim, transfer of ownership, and provenance functionality over to blockchain layer. We foresee additional hardening of the Solidity programming language and smart contract functions as a prerequisite to making this transition, as demonstrated by the recent smart contract security breech associated with The DAO. Phase Three will be funded from Company revenue and VC investment.

ECOSYSTEM PARTNERS

Silicon Chip Manufacturers

The registration protocol is technology and vendor agnostic. While it supports BLE and NFC communication methods today, new protocols (and protocol versions) are easily added. Any vendor-specification format can be appended for universal lookups. Current partners and vendors include: Silicon Labs, NXP, and Identiv.

Form Factor Providers

For many applications it is important to include a chip in a physically tamperproof form factor. Partners include: Cellotape, Origin Labs, and SmarTrac.

Chip Designers/Firmware Companies

An industry standard exists to include secure elements inside NFC chips. There is less progress to date including secure elements inside BLE chips, and Chronicled is working on projects with BLE chip vendors to upgrade several different BLE chip architectures to also include a secure element. Current vendors include: Viper Design.

Cloud Service Providers

The Open Registry is intended only for “basic birth certificate data” – the chip public key and/or identifier -- for a consumer or luxury product. If a Brand or product creator wishes to associate additional digital content to a chip, they can add a third-party cloud services provider via the Service URL. Current partners and vendors include: SmarTrac, Chronicled, and Blue Bite.

COMMON QUESTIONS

Appendix 1: Problem of Counterfeit Product Fraud

Why has this problem become so big? - It is very lucrative for manufacturers to make unauthorized product runs and to re-use manufacturing tools after the official Brand product run has been supplied. Counterfeiters operate with a very high gross margin. They sell branded products without marketing and advertising costs of having to build-up global Brand recognition.

Don't serial numbers help to solve the problem? Unique identifiers that Brands include in their products are not truly unique. A serial number, UPC code, QR code, or barcode can be copied or cloned. Dishonest manufacturers can easily copy the legitimate identifiers, and consumers have no way to verify if a serial number is real, copy-of-real, or totally bogus.

Appendix 2: Choice of Ethereum Blockchain

A common question that we get from our investors and executives at large Brands is, “Why did you chose to host the IoT Open Registry on the Ethereum blockchain?”

Here is our typical response:

Our team at Chronicled has been evaluating all of the major open, permissionless blockchain projects and protocols closely over the period of the past 24 months.

For a long time, the Chronicled team held off on committing to a specific blockchain layer, as we were waiting for enough “convergence” to occur in the ecosystem, so we could make the right choice on behalf of our shareholders and partners.

Most importantly, we have designed a system that is blockchain agnostic, so that if needed the system can be ported over to a different blockchain.

We have selected the Ethereum blockchain after interactions with founding members of the Ethereum team, prototyping our collectible sneaker and luxury goods registrations on the Ethereum blockchain, and watching the Ethereum ecosystem reach a point of traction and global momentum that we believe will support a global standard for consumer product authentication.

The IoT Open Registry that we are developing as part of Chronicled Open Source leverages several important attributes of the Ethereum blockchain protocol:

- First, Ethereum can be viewed as an open database supported by 1,000’s of decentralized computers across 100+ countries, making it a long-lived and neutral record-keeping ledger that all Registrants can use as a shared resource without needing to trust or depend on any single database provider that could be a point of failure,
- Second, Ethereum provides smart contracts functionality. Therefore rules of engagement can be pre-programmed upfront, including rules around how the white-list of bonafide registrants is extended and maintained and how product registrations are completed,
- Thirdly, it is an immutable record with time-stamped blocks. Product registrations can be continuously added to newly created blocks every singled day, but, also,

according to the protocol, previously committed registrations can never be deleted or lost.
- Finally, Ethereum supports numbered accounts such that a Registrant can register products to the leger anonymously and not necessarily disclose identity or details about its products via the open ledger, which prevents loss of sensitive business intelligence and potential tracking of activity by competitors.

The blockchain space is evolving quickly, and although Ethereum is a relatively new project, it is quickly gaining momentum and developer support globally and has a Turing-complete programming language and smart contract framework that we believe can support a new global standard for consumer and luxury product identity verification. Ethereum has been tested with millions of transactions already and IoT could become one of the largest use cases.

While the Solidity smart contract programming language is still largely untested, it is being used for many projects with large financial stakes involved, and many of the smartest developers in the world are now testing and improving upon this framework.

Although the gas price on Ethereum is not free, new product registrations can be completed for 2-5 cents.

We are not aware of any other system that would provide developers with programming flexibility and registrants with neutrality, anonymity, security, and immutability for their product registrations, without a reliance on a third-party actor for the maintenance of the system and / or records.

Appendix 3: FAQs

How will the problem of SPAM registrations be solved?

It costs a small amount of Ethereum gas to register a product, and so while there might be some SPAM chip and product registrations, it would be a waste of money for a spammer to commit considerable registrations without a meaningful reason to do so.

For Registrants who want to be taken seriously, they will be able to confirm their identity by publishing their Ethereum public key on their corporate home page. At the Explorer level, product registrations are parsed into a "green list" that includes all product registrations from a Registrant with confirmed identity, and an "other list" that consists of registrations from Registrants whose identity remains unconfirmed.

Can the contents of an RFID, NFC, or BLE chip be copied and transferred to another identical chip?

The content of most of the RFID, NFC, and BLE chips deployed in the world can be copied easily. However, microchips that contain a "Secure Element" are protected from this form of attack. See: https://www.globalplatform.org/mediaguideSE.asp

What if a rogue employee at the NFC or BLE chip factory creates a duplicate chips with the same private key?

Private key is generated internally in the chip on the first run and stored in a Secure Element so it cannot be copied.

The manufacture of chips at the silicon chip factory and the attachment of chips to branded products is a two-stage operation, and a rogue employee who works for the silicon chip company has no idea what specific branded product a given chip is going to be affixed to and associated with on blockchain.

Whose chips will work?

Major NFC and BLE chip vendors include Broadcom, Intel, LS, NXP, Samsung, Silicon Labs, ST Micro, Texas Instruments, and Qualcomm.

Any NFC or BLE chip containing a Secure Element will work to protect the private key contained in the microchip.

What if Ethereum fails?

While the failure of Ethereum is viewed as unlikely, given the simplicity of our implementation, Chronicled can mirror or port all product registrations over to another blockchain, which makes it possible to fully recover the system should recovery or a switch to another blockchain platform be needed.