jitsuin

WHITE PAPER

SHARED DEVICE LIFECYCLE MANAGEMENT

jitsuin.com

info@jitsuin.com

1 Summary

Keeping Internet Things up to date and healthy requires a team effort – it is not the sole responsibility of a single stakeholder in the IoT value chain and accounting for who needs to perform what action at what time is a significant challenge.

Thing Makers, System Integrators, Owners, Operators and Auditors may all have a role to play in maintaining Internet Things and Jitsuin connects these stakeholders with blockchain technology to reach agreement on the state of Things at any given instant. With that shared knowledge they can make faster, better decisions.

Jitsuin Shared Device Lifecycle Assurance can track any type of Internet Thing – from security hardened microcontrollers to general purpose embedded computers. Understanding the provenance and lifecycle of Things enables clean and truthful data for man or machine to act with assured intelligence.

Shared Device Lifecycle Assurance enables higher levels of trust in data from Things. Higher trust means more value in data to fund the maintenance of Things. Sustainably funded maintenance keeps Things producing truthful data. A virtuous circle completes to keep Things in service longer and reduce electronics waste.

Jitsuin is independent of chip architecture, chipset, device maker, and IoT platform and records data about Things, which enables stakeholders to build consensus in their IoT value chains.

IoT data marketplaces will only function with clean data. Now more than ever, a record of how Things were born secure and maintained throughout their lifetime is the meta-information that's needed to trust the IoT.

Jitsuin builds Truth in Things.

2 Scope

The Jitsuin definition of Internet of Things means Internet *connected* Things, from powerful web services to small, microcontroller enabled sensors and actuators that communicate over standard internet protocols.

Blockchains are distributed shared ledgers that record transactions that participants agree upon and are the foundations of cryptocurrencies such as Bitcoin. Public permission-less blockchains allow anyone to participate, establish nodes on the network and maintain a copy of a shared ledger. Private permissioned blockchains control who can perform what actions on a shared ledger, such as reading, writing, updating or deleting and what transactions are allowed.

Jitsuin uses private permissioned blockchain technology to build Truth in Things.

3 Market overview

The Internet of Things is not delivering on its promises. Today there are many Things that connect to platforms using Internet protocols – but the vision of Things openly and autonomously connecting and sharing data with other Things has not yet been realized. A lack of trust is the constraint because there is no easy way for everyone to check the source of data and the reliability of Things that produce it throughout their lifetime; Internet Things are only secure until they are not.

Some issues in the wider market signpost a timely need for a new solution.

Political – Hacking and data breaches are now front-page news and Internet Things have been weaponized. IoT security is on government agendas but perhaps a more pernicious threat is that of "Fake News" and artificially created Truth applied to the IoT.
Internet Things must prove the data they produce is real.

Economic – Digital transformation toward service-based business models and subscriptions is normality for industries and people that accept rental rather than sinking capital into ownership of depreciating assets.

Although hardware costs are lowering, the ongoing cost of maintenance for connected things must be addressed.
A sustainable business model for lifetime secured IoT is subscription-based.

Social – The financial crash of 2008 eroded trust in centralized systems and Bitcoin emerged shortly thereafter. Removing control from central authority is a common theme for many social movements. The self-sovereign identity movement aims to decentralize and empower people to take control of their personally identifying information.
People will trust Internet Things if they understand how they are controlled.

Technological – The trend to connect everything brings greater potential value and faster innovation yet introduces new systemic vulnerabilities. Much of this is facilitated through highly scalable cloud computing, serverless technology, machine learning and centralized platforms.
Blockchains and collaborative platforms promise an open, distributed and scalable infrastructure.

Legal – There will be investigations into liability when Things cause injury or damage to property. A national healthcare service bought to its knees through unpatched vulnerabilities, a smart thermostat update that froze people's mountain retreats – Contractual liability must be codified when updates are not applied, or products misused.
Things and infrastructure need an accountable audit trail.

Environmental – An increasing public awareness of the damage caused by waste electronics and the environmental damage caused by inefficient energy hungry devices will lead to a reduction in consumerism and landfill.
Internet Things must have a longer life expectancy to reduce waste electronics.

There are real world consequences when an IoT platform blindly trusts data. In 2014 researchers at Ben Gurion university were able to fool a social navigation system into re-routing users around a traffic jam that didn't exist. Fake users and fake devices enrolled to inject fake GPS coordinates into the system. The real-world outcome diverted users to alternate routes of the attacker's choosing. Could attackers divert an autonomous vehicle relying on social navigation information? Could attackers identify high-net-worth individuals in a vehicle? Could attackers choose to stop an autonomous vehicle with brute force in a hostile neighbourhood? It may not need more than a well applied stroke of white paint on a road.

The answer to these challenging problems lies in identifying sources of information before relying too heavily upon them. There is a great difference between a GPS receiver chip that signs its coordinate payload before software has a chance to modify it and an open API that accepts data from anything with access. Signed data is very likely to have come from a real piece of hardware in the claimed location. Knowing a GPS receiver was built into a well maintained and regularly patched automotive module would be even more helpful. We don't need to know whose vehicle it is, or who's in it - just that a vehicle reported it. Knowing the difference makes all the difference for we gain "clean data" – where data sources are identified and provenance verifiable.

An internet connected smart traffic light could use that verifiable GPS data along with trusted traffic data from other sources to improve quality of life in urban areas. It would enable "green-lanes" not only for emergency vehicles but heavy goods vehicles too – improving air quality through a function normally reserved for emergency services. It would enable light phasing to adapt based upon user's intended direction of travel at any given instance. And traffic lights could talk to GPS systems in cars to inform them of how much dwell-time remains – giving opportunity to advertisers to run appropriate length commercials while they have drivers' attention.

Clean IoT data on an open market could see many more uses - if only everyone had sufficient trust in it. If only a mechanism existed for connecting the provenance of Things to the users of data.

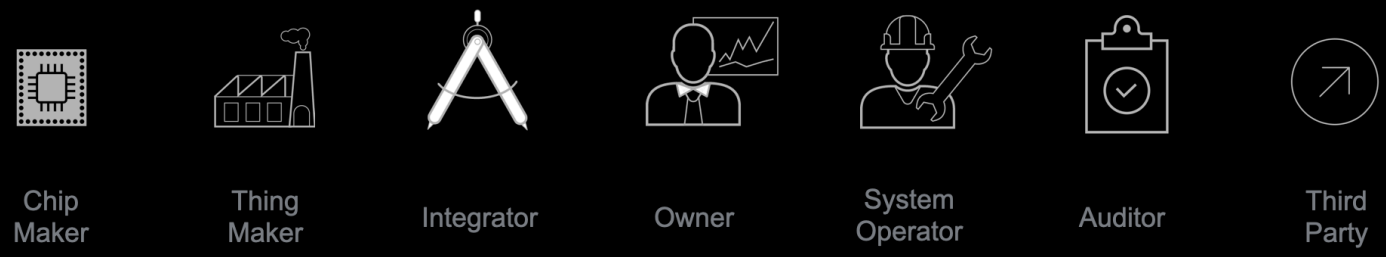
Some social networks use "Blue Ticks" as a trust mark to indicate high-profile users have passed stringent identity verification checks – it's important to know that information coming from an account is from whom you expect it to be – particularly if that individual has the power to move markets or cause disruption. "Know Your Customer" (KYC) is a prerequisite for Anti Money Laundering (AML) in the financial world and now it's time the Internet of Things has KYT – "Know Your Things".

3.1 The Secret Life of Things

To understand why Things haven't made the grade it pays to look to the security industry which has always suffered from the classic economic problem of "externalities". This means that the costs of implementing security measures are not borne by those who actually feel at risk; and by that same token that the pain of a security failure is not felt by the person taking the risk. When business cases are reviewed it has always been very difficult for device and software makers to put extra time and money into integrating features that only protect users several steps down the value chain: users who in turn are generally unwilling to pay for such fine gestures.

A Thing Maker needs to build a lifetime's maintenance cost into the sales price of a unit, while forecasting how long a Thing will live a useful life, how many units will be sold or how it will be used to create value for its users. Price too high and not enough units will be sold to be profitable, but price too low and security issues will bite later.

Examining the value chain and roles in the development path shows how early decisions or lack of awareness can significantly affect the life chances of a Thing.



Chip Maker – designs and builds embedded compute capability for general purpose or specific applications.

Thing Maker – packages hardware, software and services to make a product that is approved for use in its intended application.

Integrator – designs a system composed of many products, platforms and applications to serve a business purpose defined by the owner.

Owner – improves business outcomes from connected Things and is the legal owner of the system and data.

System Operator – manages the day-to-day running and safe operation on behalf of an IoT system owner.

Auditor – oversees and ensures that all actors involved in operating the system can be held to account.

Third Party – Any organisation other than the Thing Owner that wishes to benefit from data generated by Internet Things.

This is a long chain for all security requirements to be adequately fulfilled – especially when economies of scale pivot around producing one product variant to use in many applications. Adding to this already complex delivery channel, there are many more organisations alongside this value chain. Technology suppliers of Thing Identity certificates, identity and IoT platforms that manage API access to people things and cloud applications play an important role in building and maintaining trust.

3.1.1 Design of Hardware and Software

Things are made from many components of intellectual property, processor architecture, silicon implementation and software configurations – so many variables that make diverse and competitive products adapted for purpose, yet which make it hard to tell the difference between what is secure (against whom) and what is not. Not knowing how and where Things will ultimately be put to use exacerbates the problem – secure in one context may be wholly inappropriate for another.

For example a remote-enabled door lock may have conflicting requirements: for the security of the assets behind the door it is best to design a system that fails closed, such that it remains secure even in the case of unforeseen and unhandled extreme circumstances; but for the safety of people working inside it is preferable to fail open, lest they be trapped inside during an emergency. No matter how good the security primitives in the embedded component that drives the door control, it is impossible to know at component design time which of the safety and security needs will be prioritized by the system owners once installed. One thing is certain – safety cannot be guaranteed without appropriate information security of the Thing.

An Internet Thing Maker would have a hardware team that selects an appropriate silicon chipset to fit a price, performance and energy budget. Security budgets always get squeezed; non-functional requirements are generally viewed as "someone else's problem" and at this stage it is easy to dismiss the problem with an answer of "we'll secure it later if there is a problem", or "we'll fix that in version two". Perhaps the biggest issue is that Thing Users have not understood the need nor asked for truth in Things and writing security requirements is not trivial.

Secure Things don't happen by accident - they need careful design of boot sequence, update capability and identity protection measures. It's also essential to shut down back-door access; debug interfaces should only open to authorised technicians.

Regulation and legislation are emerging. Secure by Design guidelines and standards are being developed and regulators are starting to take a more forceful approach. Things need strong identity protections from the outset since the days of hiding connected devices behind network perimeters are gone – Internet Things by definition use internet protocols and should assume no trust in the network. Internet Things must be designed to stand up for themselves.

3.1.2 Manufacture and Deploy by Thing Maker

Thing Makers have security requirements of their own, for example some need protection from contract manufacturers overproducing to sell into grey markets or stealing intellectual property to enable competitive offerings without sunk R&D costs. Once hardware is assembled in the manufacturing process, a Thing is brought to life with an injection of embedded firmware. At this sensitive stage, a Thing can be issued a Digital Birth Certificate that is the first piece of its identity and can protect its basic operating program.

Production stations can be fitted with Hardware Security Modules that manage device identities and encrypt firmware images that can only be used on specific devices, while controlling the number of devices produced. The ability to inject secure identity is highly useful when it comes to field updates of devices too. Since Things can be individualised securely, this capability should extend to Thing Users when it comes to installing and operating their Things.

3.1.3 Design-in by Systems Integrator

Unlike consumer digital systems, which can be created from scratch and renewed from green shoots every couple of years, the physical world is constructed piece-by-piece over hundreds of years. Technologies of all ages, from all kinds of manufacturers, are mixed together and made to work, carefully stitched together in approved configurations by a system Design Authority. Chosen primarily for their immediate extant utility, and not their embedded 'smartness', it is inconceivable that any industrial connected system of any size will feature embedded components exclusively from one architecture or product family. Things will be chosen with features and functions that meet immediate needs and once designed in must be relied upon to continue meeting those needs. Updates that deprecate functionality or change the way a component behaves can be very bad for systems that have come to rely upon those features.

3.1.4 Install and Commission for System Owner

An Internet Thing may become stale sitting on a shelf before deployment so an on-first-boot firmware update would save enrolling Things that may already contain identified vulnerabilities and exposures. Once updated, a Thing should present itself to its User's platform and attest its provenance. A User needs to know that a Thing is genuine, untampered, up-to-date and can protect identity secrets generated during enrolment. If a Thing passes these first checks, it can be registered, and an authentication secret established so a platform can be sure it talks to the same Thing over time. Start trusted, stay trusted.

3.1.5 Operation and Predictive Maintenance

A System Owner may appoint a System Operator to act on its behalf to manage and maintain its estate of Things. At some point in time a Thing may transmit an “anomalous” payload. According to Claude Shannon’s theory of information (which posits that the most unexpected packet of data carries the most information) this may be the most useful piece of data ever transmitted, or an attack. Which is it? At this point a re-authentication and retransmission of the “anomalous” payload alongside a background check on maintenance schedules could identity an attack before systems start acting on bad data.

It is entirely predictable that maintenance will be needed during a Thing’s operational lifespan to fix a vulnerability. System Owners need notification when an update is available. The trade-off between planned downtime from applying an update or taking a risk of unplanned downtime from an attack can only be made by owner or their maintenance company. That decision may be delegated during an initial setup to allow automatic updates, a predetermined time to install, or a preference for manual updates, but not accommodating that choice to delay updates could affect operational safety in some installations.

3.1.6 Create Value

People and businesses seek benefits from Internet Things such as reduced costs, capital expenditure and downtime while creating new services, payment models and valuable data to resell. An IoT platform can sift through vast amounts of data to find information hidden within – a job that nobody would want to perform manually themselves.

At some point in time a Third party may create ways to make money from the data things generate. The Owner may authorise use of their data for such a purpose – to economically benefit themselves through better service, reduced costs or some combination of services that leads to better outcomes. Third Parties need to know they are dealing with real data from real things and that they have their owner’s consent to use data – particularly if it is Personally Identifiable information covered by General Data Protection Regulations (GDPR).

3.1.7 Retire and Revoke access

The life of an Internet Thing will come to an end when it no longer receives updates. It’s anyone’s guess whether a Thing will be successful, a Thing Maker in business, or the software development team that understands the original code is ready to build patches when necessary. Planned obsolescence may make hardware replacement the only viable option but who and what needs to know when a Thing is orphaned and how will they know?
With a growing movement of rights to repair, there may come a time where an asset owner wishes to take updates from authorised third parties or take matters into their own hands.

3.1.8 Audit and Account

All the decisions and actions taken by the various actors involved throughout the lifetime of a device should be captured in the event that a forensic examination be needed should something go wrong. By holding everyone to account for their actions in a transparent and ambient way, it will be evident for all to see when patches are not made fast enough or devices go unpatched for extended periods.

3.2 Shared Device Lifecycle Assurance

Assuring the lifecycle of a device is a team sport and responsibility must be shared.

Such sharing is important because technical (rather than legal) responsibility for fixing issues and bringing degraded devices back to health will lie with different stakeholders at different times: if a firmware issue, then the device maker needs to issue a patch; if configuration then the owner of the system needs to remedy – having first validated with integrators and operators that a system change is safe and ready to apply; and for industry-wide changes it may fall on a government entity to instigate and enforce change rather than any one actor. Working together as peer stakeholders is the only way.

Developers within a Thing Makers’ software team will create patches, commit updates and then begin a release process to cryptographically sign the resultant update. Firmware signing keys are highly valuable and must be protected from unauthorized use – how signing keys are controlled is an important factor in deciding the trustworthiness of an update. System integrators may have to inspect the software manifest for any functional deprecation in order to approve for use within a given system. How can that approval be noted? Owners must understand the business risk of applying an update or not and finally System Operators must identify an

appropriate moment to apply an update during schedule downtime. How would everyone know when a Thing has regained health? An update should wait until all peers have granted consent, so the question is whose finger is on the reset button?

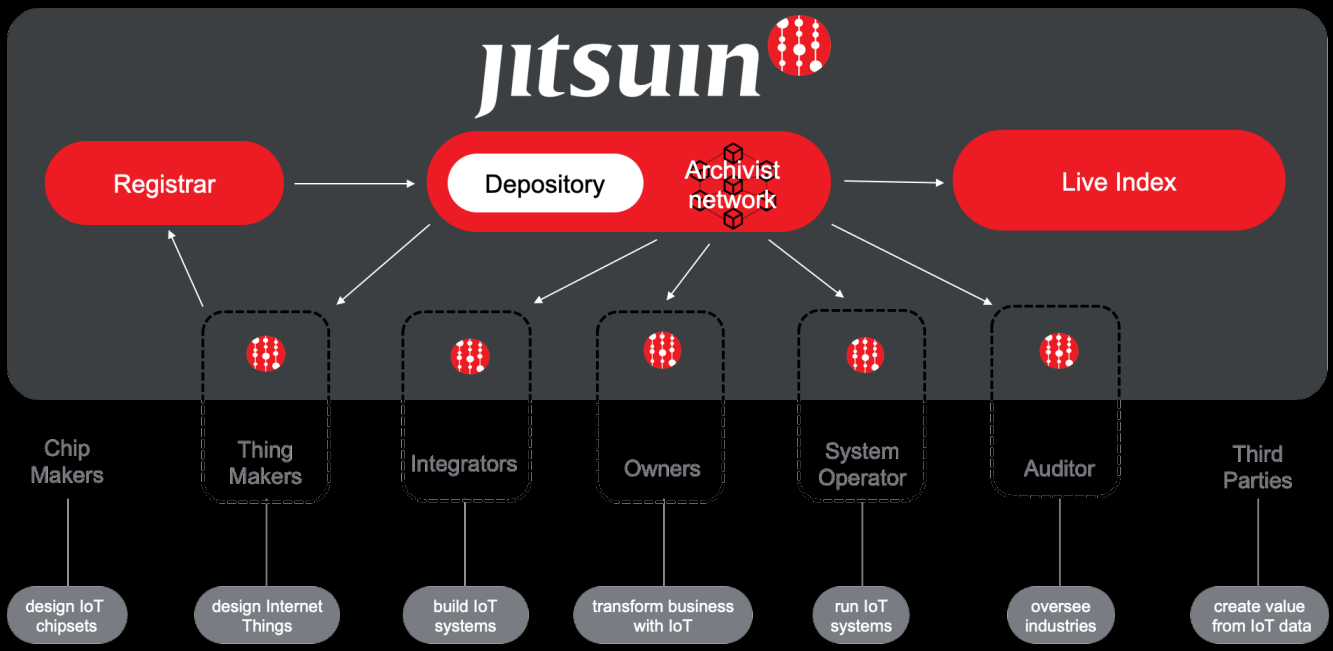
3.3 The ongoing value in truthful data

Things will need maintenance throughout their serviceable lifetime and the only sustainable way to pay for their upkeep is through subscription business models. If a Thing is delivering value, then an owner is motivated to keep it secure. Additional value can be realized through enabling third party access to data – only if those third parties can believe that they are consuming data from real Internet Things, not bots. Security assertions from Things proving their health would be useful meta-information for third parties wishing to know the provenance of data they consume.

The possibilities for trade of clean data with known provenance will realize the true value of the Internet of Things. When man or machine can act on data without fear we can finally build the cleaner, greener, more efficient and more productive connected world that the IoT has always promised.

4 Proposition Overview

Jitsuin talks *about* Things rather than *to* them so Jitsuin Shared Device Lifecycle Assurance supports modern Things with hardware-backed software and digital identity protection technology alongside legacy devices. With all stakeholders sharing and agreeing to the same view of the state of maintenance of all their Things, a digital "Hawthorne Effect" improves performance, facilitates greater automation, and enables ambient accountability.



Registrar
Jitsuin Registrar witnesses device provisioning and securely records device details, including Digital Birth Certificates and identity data, in the Depository.

Depository
The Depository is the secure registry of device provenance information. With the confidence of knowing exactly how trustworthy a device was at creation, Archivist networks can then extend that trust to in-service lifecycle events.

Archivist

Archivist is a hybrid microservices and private blockchain network for permanently recording device lifecycle events and enabling stakeholders to confidently assess and act on device maintenance data. In short: Shared Device Lifecycle Assurance.

Live Index

Using the increased confidence in data that Shared Device Lifecycle Assurance brings, Live index is a public blockchain animated by smart contracts that enables participants to trade in trustworthy IoT data without third party intervention.

5 Use cases

Shared Device Lifecycle Assurance enables higher levels of trust in data from Things. Higher trust means more value in data to fund the maintenance of Things. Sustainably funded maintenance keeps Things producing truthful data. A virtuous circle completes to keep Things in service longer and reduce electronics waste. Other benefits of Shared Device Lifecycle Assurance include:

- Significant opportunities for automation and cost savings
- Improved visibility and communication of firmware vulnerabilities and updates
- Enhanced operational intelligence
- Traceability during maintenance and recovery operations
- Near-real-time audit view of device patch and update status
- Checking data provenance within a system before acting upon it
- Proving that systems are operating to accepted maintenance agreements
- Encoding maintenance responsibility, performance, and SLAs among stakeholders
- Proving to third parties that data was created by real Things running real firmware
- Ensuring downtime during upgrades is managed safely by system operators
- Coordinated end-of-life management
- Recording transfer of liability when exercising rights to repair and modify

Beyond shared device lifecycle management that traverses many industries, from Thing Makers to users there are many more applications that can be realized by third parties when data can be trusted using the Jitsuin Live Index.

Automotive and Transportation

A smart connected traffic light could have many authorized users that would benefit from some element of data or control.

- Cars could inductively charge and pay for electricity while waiting
- Heavy goods vehicles could use “green-lanes” to reduce pollution caused by acceleration
- Autonomous vehicles adapt velocity based on light phasing to arrive just in time for green signals
- Emergency response vehicles can communicate destinations “around corners” to clear traffic in advance
- Urban and event planners can adaptively plan better routes
- Navigation systems can plan routes based on known wait-times
- Maintenance teams can predict failures and plan for zero down-time

Industrial Automation

- Maintenance contractors can analyse data to predict failures and offer better service
- Regulated industries can report with instantaneous accountability
- Supply chains can digitally transform with APIs and automation

Healthcare

- Patients can connect their devices to medical services to find the best opinions and care plans for their conditions.

- Patients can supply anonymized sensor data to medical researchers to improve treatments.

Energy and Utilities

- Neighbours could trade excess renewable energy amongst themselves.
- Green appliances could run when the wind blows or the sun shines.
- Homes could “locally load balance” by pausing high energy use appliances for five minutes while boiling a kettle.
- Autonomous vehicles could find and pay for unoccupied domestic charging points.

Insurance

- Homeowners can grant control of lighting to insurers while their homes are unoccupied in exchange for a discount
- Insurers can gain better insight into commercial risks knowing that data is provable and machines reporting it are kept healthy

6 Value propositions

The motivations to solve security issues within the value chain are subtly different for its stakeholders as well as the individual’s functions within each organisation. A minimum viable ecosystem consists of Thing Makers and Industrial IoT users. Chip makers, System integrators, Operators, Auditors and Third parties may also realize benefits of their own.

6.1 Thing Maker

The idea of an internet connected product will be conceived, the market researched, features defined, engineering costs estimated before pricing, distribution and go-to market strategies are finalised. Business models for products are written with forecasts to justify executive sign-off before being shelved and forgotten. The product will launch, sell in volume, the engineering team disband and then move to the next product. Months or years later the products need patching – was this in the support and maintenance plan? Does the warranty cover security updates? Were people aware of the product lifecycle when it was purchased? Who will pay for the security update?

- Jitsuin enables Thing Makers to take part in the data economy and establish recurring revenue to support maintenance throughout a connected product lifecycle.

- Jitsuin provides a broader view of device usage and deployment that will reduce time to fixing vulnerable devices and improve future product development.

- Jitsuin improves tracking of vulnerabilities, disclosure mechanisms, end user notification and life-cycle management including end-of-life consideration.

- Jitsuin is IoT platform agnostic and enables identities created in manufacture to be published once and enrolled anywhere.

6.2 Industrial Thing Owner or Operator

A CISO will be concerned with many aspects of information security and Internet Connected Things broaden the attack surface. The CISO manages risk, balances the need for enabling business and protecting people, assets and reputation. The role assures integrity of operation through monitoring threats and making appropriate response. The needs of business always demand more with less – and adding more attack vectors with IoT cannot be dealt with through yesterday’s technologies.

- New business priorities of digital transformation with open APIs create new opportunities for added value to the top line – data is the new oil.

- Jitsuin enables users to prove to third parties that data generated by Internet Things and accessed through APIs is real, thus making that data more valuable.
- Jitsuin eases tracking of the state of Things from any vendor, while keeping an instantly auditable account which enables more responsive risk management.
- Jitsuin enables devices to live a longer serviceable life whilst still complying with trust and maintenance standards.

7 Jitsuin Differentiation

Jitsuin is independent of chip architecture, chipset, device maker, and IoT platform and records data about Things, which enables stakeholders to build consensus in their IoT value chains.

IoT data marketplaces will only function with clean data. Now more than ever, a record of how Things were born secure and maintained throughout their lifetime is the meta-information that's needed to trust the IoT.

Jitsuin builds Truth in Things.

jitsuin

1 Almaden Blvd Suite #200 • San Jose, CA 95113 • United States
Wellington House • East Road • Cambridge CB1 1BH • United Kingdom

jitsuin.com • info@jitsuin.com