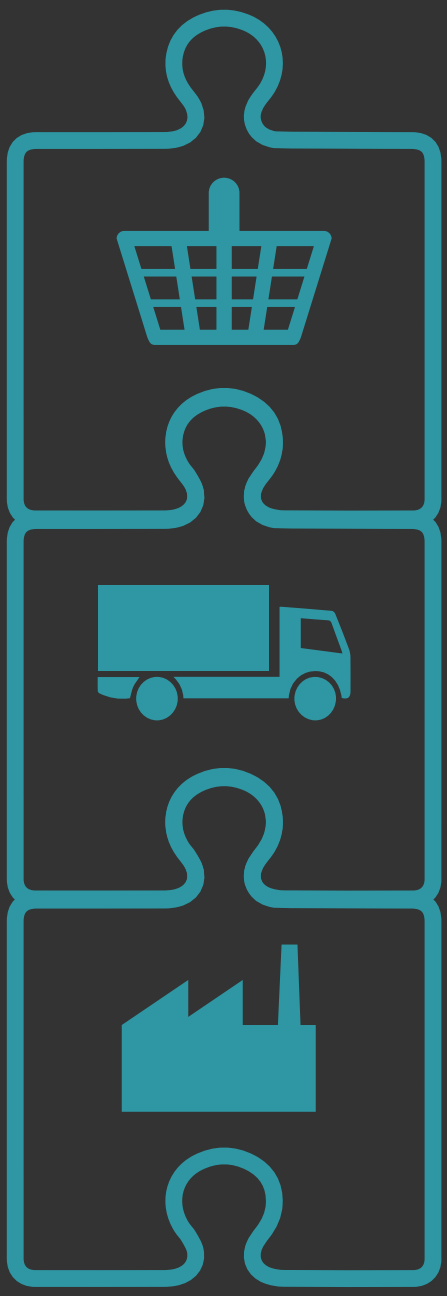
White paper



BLOCKCHAINS FOR THE IOT: BEYOND THE HYPE

Activate the things that move your business

London . New York . San Francisco
evrythng.com • @evrythng • hello@evrythng.com

Executive Summary

The answer is blockchain. What is the question?

Much has been written about blockchain and how it will be a 'game-changer' for the Internet of Things, addressing the challenges around security, scale and resilience as more and more things get connected.

But how much is hype and how much is reality? And how will these two technologies work together?

IoT is much more than driverless cars, industrial M2M or smart home appliances. Everyday products, such as clothing or consumer packaged goods (CPG), are also getting connected to the Web too. These non-powered items have no powerful embedded electronics and gain their intelligence through on-pack tags, labels or sensors which generate data throughout their lifecycle, as they move along the supply chain, from factory to retail and then into consumer homes. Over 3 trillion of these consumer products are manufactured every year and once they are 'switched on', the impact will be seismic.

> "3 trillion consumer products manufactured every year"

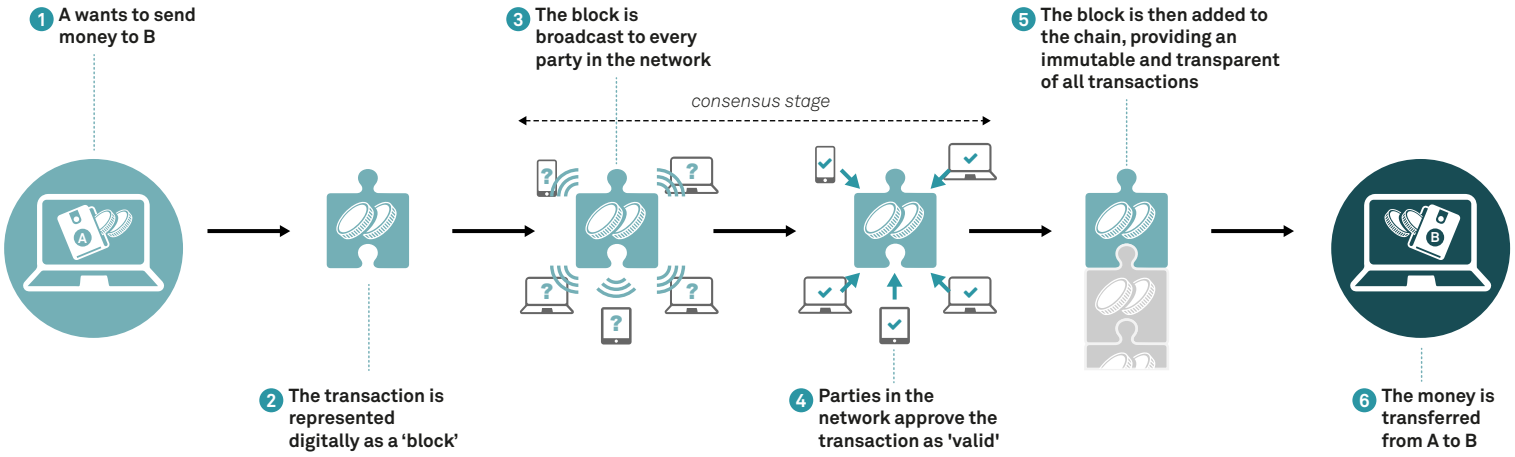
But what role will blockchain play in this transformation? With a focus on the Apparel and CPG markets, the EVRYTHNG Innovation team has been working with blockchain technology in our labs to see how it might enhance or complement different IoT use cases.

The white paper is for enterprise business leaders who are tasked with understanding the impact and potential convergence of IoT and blockchain, and how this should shape their digital transformation strategies. It will cut through the hype to understand the real-world commercial value, and will show how companies can deploy a simple Proof of Concept (PoC) to evaluate blockchain and IoT working together.

Blockchains overview

Definition

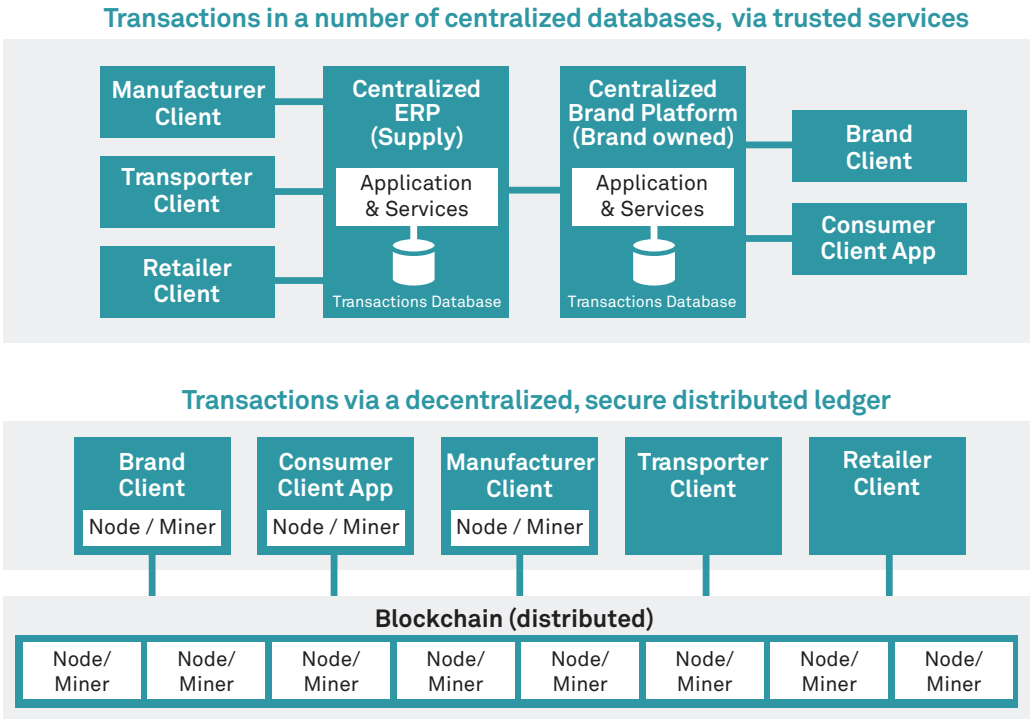
A blockchain is a distributed digital ledger technology - at the heart of systems like Bitcoin and Ethereum - where transactions are recorded and stored on many computers across a peer-to-peer network without the need for a centralized third party. Every transaction is verified and secured by all participants in the blockchain using cryptography and only validated by a consensus. (See figure 1.) This data trail is immutable and will be stored in the blockchain, unchanged, for as long as the blockchain exists.



Architecture

Blockchains represent an evolution from centralized to decentralized systems where there is no master computer. Rather all participating 'nodes' have an immutable copy of the chain, which is updated and verified through consensus of the parties involved.

Figure 1: How a blockchain works



Types of blockchain

Public Blockchain

A fully decentralized, distributed system that anyone in the world can read, send transactions to and expect to see them included if they are valid. Any party can participate in the consensus process – the process for determining what blocks get added to the chain and what the current state is.

Good illustrations of a public blockchain implementation are Bitcoin, the digital currency, and Ethereum which uses the concept of smart contracts.

Private Blockchain

These are systems often dedicated to a single organization, or group of companies, where access permissions are more tightly controlled and restricted to a few users to ensure greater privacy and governance. These blockchains are built from scratch or based on open source implementation of blockchain principles such as HyperLedger.

Figure 2: A comparison of architectures

The missing piece of the jigsaw?

According to Cisco[1] 99% of things in the world will become connected and part of a network. But this vision of full interconnectivity between things, people, applications and infrastructure across industries is not yet a mainstream reality.

Perceived security vulnerabilities, fragmented ecosystems, inconsistent interoperability standards, lack of scalable computing infrastructure and limitations in network access are all thorny challenges that need to be overcome.

Blockchain has indisputable potential to help, but such IoT obstacles cut across many different areas, including operational, economic and even regulatory, and so cannot be overcome by technology alone. Moreover, there are still many concerns with blockchain itself which are holding back wider adoption, including:

1. **Immaturity:** Blockchains will undergo significant change over the coming months and years, with new distributed ledger alternatives surfacing regularly.
2. **Scalability:** Executing peer-to-peer transactions with shared consensus is not particularly efficient and involves significant latency, cost and energy consumption. Cost effective models needs to be found.
3. **Security and privacy:** Clear policies are needed for how data is stored and accessible on the shared ledger in a secure and permissioned way, that suits both enterprises and consumers.
4. **Transparency and governance:** Clarity around legal compliance and the operationalization of blockchain technology is needed before it can be embraced by major enterprises.
5. **The centralization question:** There is likely to be continued disagreement about the true value and role of emerging public, private and community blockchain models.

[1] http://www.cioinsight.com/it-management/innovation/the-internet-of-things-gets-real.html

How blockchains work with the Internet of Things

When should you use blockchain?

The distributed ledger approach is suited to some specific real-world scenarios: financial transactions, smart insurances, drug or medical compliance and even diamond authenticity are all areas where blockchain-based solutions have already been deployed.

Ledger Litmus Test

But, with the above concerns in mind, EVRYTHNG recommend a simple assessment - our *Ledger Litmus Test* - to see if blockchain is merited for your specific IoT use case. Answering yes to each of these 3 criteria is a strong indication that blockchain is worth exploring.

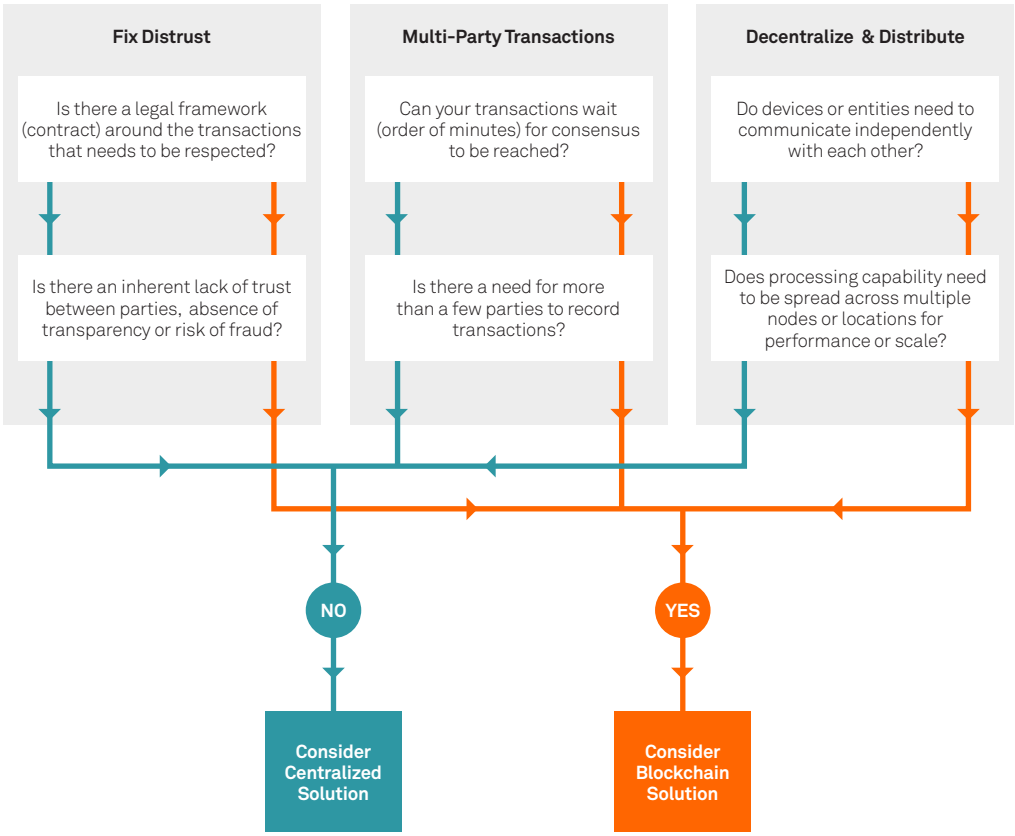


Figure 3: Ledger Litmus Test.

London . New York . San Francisco
evrythng.com • @evrythng • hello@evrythng.com

Evaluating 4 potential use cases

Let us apply the Ledger Litmus Test to assess whether blockchain is warranted for some common use cases where IoT currently plays a role.

1. Supply Chain Traceability

Thanks to the IoT, supply chains are experiencing a revolution. This has been enabled by the digitization and serialization of product packaging, including RFID, steganography and barcode technologies, combined with massive-scale IoT data management platforms which are able to collate the data generated. Item-level traceability has become a reality, making supply chains more transparent and efficient. But is blockchain needed?

Criteria: Fix Distrust — **MET:** *PARTIALLY* ●●●○○○

A detailed time- and location-based chain of custody across the supply chain for any product brings transparency and value. For example, manufacturers can manage 3PL partners more effectively, and retailers can have certainty on the quality of the product being delivered to them. But blockchain is not the sole way to bring this transparency, and there are data management platforms today which aggregate disparate data from ERP systems, and share this securely with various actors in the ecosystem. Moreover, full transparency is not always desired by all parties, as it can weaken commercial leverage when agreeing contracts.

Criteria: Multi-Party Transactions — **MET:** *PARTIALLY* ●●●○○○

Most supply chain are by definition highly distributed, with several actors, including suppliers, 3PL partners and retailers needing to validate and participate in transactions. Delays to reach consensus are usually acceptable in supply chains, but in some cases this might be problematic (e.g. when real-time programmatic decisions are taken on manufacturing conveyer belts).

Criteria: Decentralized & Distributed — **MET:** *PARTIALLY* ●●●○○○

Decentralization often achieves better resilience but well architected, high-availability centralized platforms often provide sufficient resilience for most common use cases today.

2. Product Provenance

There is a growing demand for apparel and CPG firms to provide consumers with details about a unique item's provenance, the raw materials used, and where it was farmed, sourced or manufactured. In effect providing visibility back into the supply chains to consumers at point of sale or post-purchase. As an example, EVRYTHNG is collaborating with the **Sustainable Apparel Coalition** (SAC) and its members in the apparel industry to provide a breakthrough program providing consumers with sustainability information about clothes and footwear products to help inform purchase decisions.

Does the Litmus Test indicate that blockchain technology is also required?

Criteria: Fix Distrust

MET: *FULLY* ●●●●●

Consumer distrust of brands has become an issue over recent years. If shoppers are to fully believe product labels that claim the item is organic, fairtrade or made without GMO ingredients, for example, it can be argued that an independent stamp of approval or immutable history is needed. This is highlighted by a Mintel survey in 2015 found that "more than half of Americans now think brands are using the terms 'organic' and 'artisanal' as an excuse to increase prices."

Criteria: Multi-Party Transactions

MET: *FULLY* ●●●●●

As with Traceability, product provenance data comes from multiple parties that need to work together to provide a full picture of the product origins. And in most cases, delays incurred by the time needed to reach consensus are acceptable in product provenance use cases.

Criteria: Decentralized & Distributed

MET: *NOT MET* ○○○○○

There is no absolute need for provenance data to be decentralized. Data could be aggregated in a centralized system.

3. Compliance

Compliance is one of the most compelling and convincing use cases for blockchain technology. Brands having to comply with an increasing number of regulations which means transparency of a product's provenance, its transportation journey and its condition is vital. Product location and temperature information from on pack sensors can be automatically recorded as a product moves among multiple parties to its destination. Avery Dennison's **TT Sensor Plus ™** is an example of such smart packaging technology.

Criteria: Fix Distrust

MET: *FULLY* ●●●●●

As an example, the EU law GDP2013/C343/0 states that a deviation of temperature within the supply chain of a drug should be reported to the distributor and recipient. What is considered in the interest of the consumer (product quality) may be to the detriment of the transporter or producer in additional costs or penalties. Having this data added to a blockchain with a public ledger provides 100% transparency and enables parties to demonstrate whether contractual commitments have been met. Several start-up companies have based their compliance solutions on blockchains such as Ethereum for this.

Criteria: Multi-Party Transactions

MET: *FULLY* ●●●●●

Compliance use cases require multiple parties to collaborate within the law or contract. Transactions can usually wait to be confirmed and do not need to be instantaneous.

Criteria: Decentralized & Distributed

MET: *FULLY* ●●●●●

Having a decentralized system for gathering data and making this available to any member of the ecosystem is important and helps with resilience, compliance and auditing.

4. Product Authenticity

The OECD estimates that 2.5% of global trade is lost to counterfeit each year, and in the apparel industry alone, fake goods are worth $1.8 trillion. The manifold impacts of lost revenues, risks to consumer health and brand reputation mean it is a critical business problem for brands to address.

Criteria: Fix Distrust

MET: *PARTIALLY* ●●●○○○

Global distrust does not exist in the same way as other examples, as consumers will trust the CPG or Apparel brand's 'authentic' stamp of approval, knowing it is in the brand's interest to fight counterfeit and prove authenticity. However there are some specific use cases, such as the secondary (resell) markets or the diamond industry, where sellers can gain financially from selling fake goods, and in these instances, an immutable product history would eliminate fraud and distrust.

Criteria: Multi-Party Transactions

MET: *PARTIALLY* ●●●○○○

Providing proof of a unique item's authenticity to consumers or the manufacturer's brand protection officers requires a combination of technologies. First, an on-pack digital identification code, either visible or invisible. Second is an app for scanning the product and third, a product identity management system to validate whether or not the product is genuine, operated by the brand owner. However, information from multiple parties (along the supply chain and in retail) helps reinforce product authenticity data especially in cases when the on-pack digital identification trigger could be forged.

Criteria: Decentralized & Distributed

MET: *NOT MET* ○○○○○○

Brands usually own product authenticity systems and well-architected, high-availability centralized platforms are resilient enough for most cases.

Blockchains are just part of the picture

To trust the data we first need to get the data

It is not so much that consumers do not trust the data they get today from brands about what is in the products they purchase or how they were made, but more that this traceability data is largely not provided. Brands first need to fill this *visibility vacuum* by providing clear real-time information on the product's they're buying or consuming.

To do this brands must instrument their supply chain operations with IoT technology. This enables them to capture information through the product lifecycle and make this easily accessible to consumers. Only when such transparency has become 'the norm', will the immutability, or trust in this data, be the next challenge to tackle. At that point, expect to see blockchains become of some competitive differentiation.

> "Consumer goods companies could take a step toward this goal by using serialization to provide a platform for gathering data at different nodes in the supply chain.[2]"
>
> **Gartner, 2017**

Physical things first need digitizing

Blockchains are not IoT solutions in their own right. For physical products to exist and interact in the digital world, enterprises first need a solution to digitize these physical assets.

Companies who embark on discrete blockchain projects without a wider digital transformation strategy risk being left with orphan solutions. This is akin to erecting street signs before the roads have been built.

[2] "Blockchain Will Drive Digital Branding in Consumer Goods Manufacturing"

Solutions need more than just a distributed ledger

Enterprises deploying solutions need more than just a distributed ledger. A registry of transactions such as a blockchain is only one component of a successful IoT deployment.

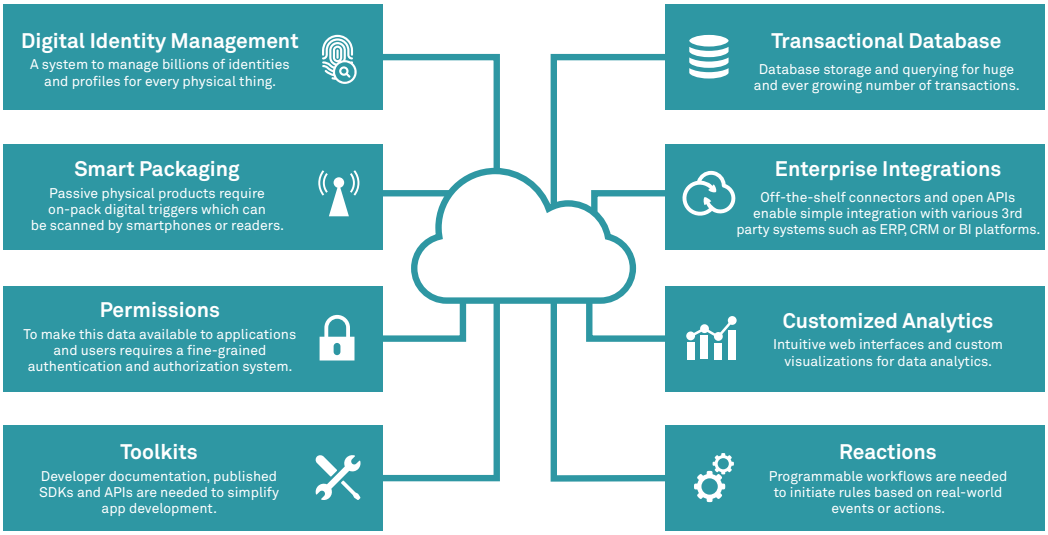


Figure 4: Solution building blocks when using IoT to connect products to the web.

Conclusion

Don't believe the hype

It is easy to carried away with hype. But the Ledger Litmus Test showed many common use cases do not necessarily require blockchain solutions. Moreover, deploying private blockchains threatens to create information silos that represent yet another form of centralization.

The technology, despite clear and unique potential, is not ready for large scale deployment due to the current **complexity and immaturity**. EVRYTHNG recommends at this time that experiments with blockchain are best regarded as proof of concept rather than forming the foundation for a widespread rollout. It should be considered as a complementary layer which can add value in certain cases, such as compliance or when a brand decides to offer 100% transparency.

EVRYTHNG: an IoT platform that works with blockchains

Numerous global companies use EVRYTHNG's IoT platform for exactly the kind of traceability, provenance and authenticity use cases described in this paper. Although blockchains are not required, we have built an optional integration with our platform to ensure our customers have a fully future-proofed IoT solution.

EVRYTHNG is a centralized client-server solution, albeit deployed on a completely distributed cloud platform architecture. The platform securely manages today over half a billion unique digital identities for diverse physical items from soda cans and jackets to plugs and light bulbs. EVRYTHNG is predicated on a model where the brand ultimately owns the product identities and the data about them, and can securely invite other companies (e.g. in a supply chain) to collaborate on this data.

Every product identity is encrypted at rest and in motion, referenced using a cryptographically secure identifier via an authenticated and authorized API, and can be audited via a list of data access and changes. In other words, this gives auditability and high-availability wrapped up by robust, mature security policies.

Our data model, based on the **W3C Web Thing** specification, holds a unique identity - known as an Active Digital Identity™ - for each physical object and captures all changes to those objects.

There is a clear parallel here with how blockchain transactions work. Such a similarity has enabled EVRYTHNG to develop a composite solution which utilizes both technologies and provides:

1. A proven, auditable and latency-free IoT solution with enterprise-ready tools, built upon future-proof web standards, to provide traceability, provenance and digital trust information.
2. 100% data immutability where transactions are simultaneously written to a public blockchain.

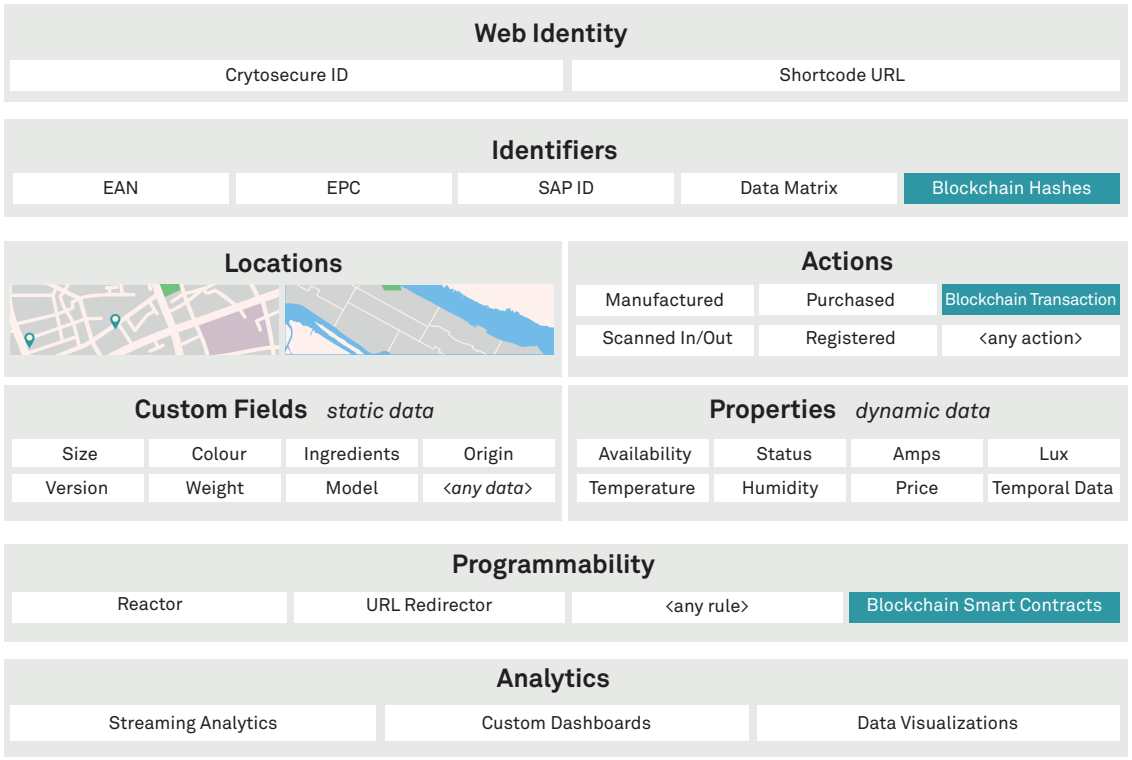
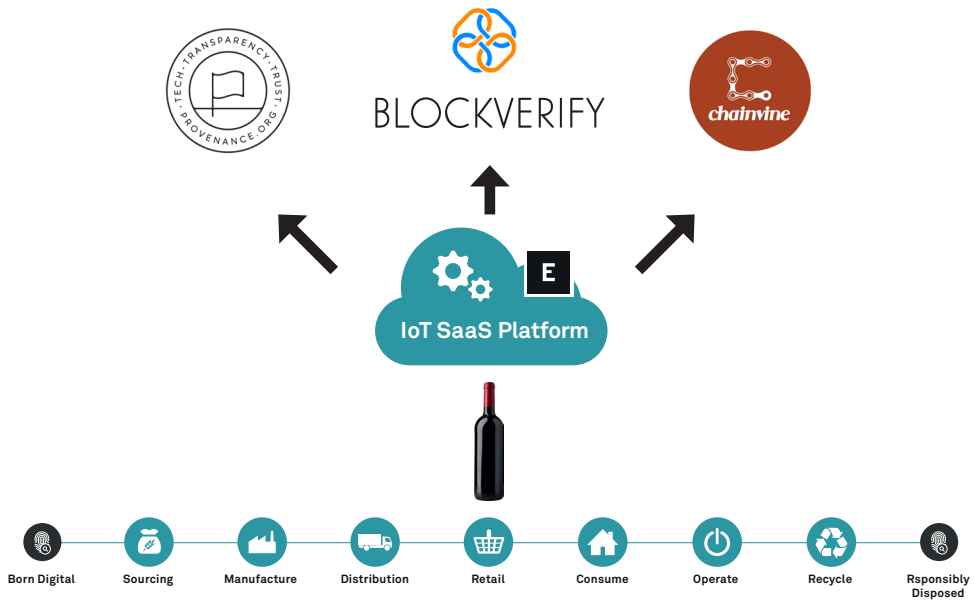


Figure 5: A product profile in the EVRYTHNG platform holds a 360 degree dynamic view of a physical object and now includes blockchain data.

One identity to bind them

As the number of public and private blockchain environments multiply, data fragmentation will increase. There will be a growing need for an 'identity and data bridge' or a platform to federate between blockchain ecosystems. EVRYTHNG's composite solution enables world-wide, unique Active Digital Identities ™ generated via our IoT platform to be used to record transactions across several blockchains, throughout the product lifecycle. We believe this federation between blockchains will be vital in the future as it opens up the benefits of different blockchain-based solutions rather than having to bet on a single (potentially immature) blockchain platform. As an example, a brand wanting to take part in a provenance trust mark program can leverage the innovative **Provenance** blockchain solution directly from EVRYTHNG by pushing the relevant data to Provenance (built on top of the Ethereum blockchain).



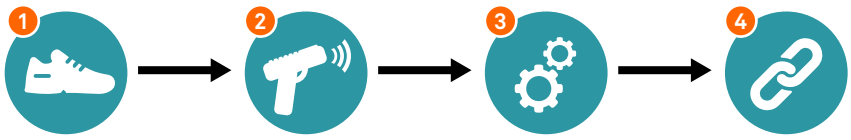
Binding EVRYTHNG to blockchains - how it works

EVRYTHNG effectively puts an API over a blockchain transaction, creating a blockchain copy or backup, executed by thousands of computers around the world in a truly decentralized and immutable way. All actions, events and interactions performed within the EVRYTHNG platform are written to the blockchain.

Figure 6: EVRYTHNG manages data throughout the product lifecycle and can federate between companies providing specific services based on private and public blockchains.

Appendix: POC Integration steps

EVRYTHNG is running proof of concepts (POC's) to enable our customers to test and evaluate both technologies working in tandem. A PoC involves 4 key steps:



1. Create Thngs in the EVRYTHNG platform. A Thng is a unique physical item.

2. Define the Actions (e.g. types of transactions) that will be executed with those physical products in the real-world. As an example, moving a pair (or pallet) of shoes from distribution to a store is an Action on the uniquely identified pair of shoes (Thng), performed by the distributor (source) designated to an actual pair of shoes (destination). In this case, Actions relate to moments in the supply chain: 'Arrive at Distribution Center', 'Scanned at retailer,' etc.

3. Thanks to EVRYTHNG's Reactor™ rules engine, we can 'certify' this transaction via a blockchain. Using a reactor script, which creates a secure hash of an EVRYTHNG Action and pushes this as a transaction in the Bitcoin or Ethereum blockchains or in a private blockchain. This ensures the Action can be validated without its content being publicly revealed. After a number of minutes, the transaction is accepted by the blockchain system and validated by a number of blockchain participants before being permanently added to the blockchain. A blockchain bridge service running on the EVRYTHNG side captures this event and creates a new Action containing the reference to the blockchain transaction. The Action is now certified by the blockchain, it can be audited by anyone and any malicious modification could easily be spotted (the Action hash would become different from what was recorded on the blockchain).

4. Products are scanned or interacted with in real-world and events are simultaneously written to EVRYTHNG against the Thng, and the blockchain.

With this service, trust is instantly established if the hashes are identical on both, and you get a searchable, analytics-ready series of blockchain transactions for your physical products as they move through their product lifecycle. Brands can collect and immutably store data on every action or interaction with their physical products as they make their journey through the supply chain and into the consumers' hands. This could be used for instance to push data to a novel blockchain-based solution with the aim of re-establishing trust in product provenance, global supply chain applications or for compliance issues.

If you would like to participate in a PoC, please email us at **hello@evrythng.com** or tweet @EVRYTHNG using #proj-iot-blockchain.