

Blockchain and the Internet of Things: the IoT blockchain opportunity and challenge

Blockchain, a form of Distributed Ledger Technology, has been gaining enormous attention in areas beyond its cryptocurrency roots since more or less 2014: blockchain and **IoT** (*the Internet of Things*), blockchain and security, blockchain and finance, blockchain and logistics, you name it. In this article we look at the IoT blockchain opportunities, evolutions and challenges.

By 2019, 20% of all IoT deployments will have basic levels of blockchain services enabled (*IDC*)

As we wrote before it seems as if blockchain technology or, better, Distributed Ledger Technology, is about to change all aspects of digital business and according to some such as Don Tapscott, blockchain is a bigger deal than the Internet. Combine blockchain and IoT and you have two bigger deals than the Internet who need each other for numerous reasons we explain in this IoT blockchain overview.

Blockchain (*there are many blockchains in fact and it's more than the technology powering Bitcoin*), has been mentioned by virtually all research firms as a rapidly accelerating evolution and it's not just about financial services companies, the scope in which we tackled blockchain outside of its cryptocurrency roots the first time (*namely FinTech or financial technology*). In fact, the convergence of blockchain and the Internet of Things is on the agenda for many companies and there are existing implementations, solutions and initiatives in several areas, outside of IoT and financial services too.

The distributed Internet of Things meets Distributed Ledger Technology

As Frank Gens said in IDC's 2017 worldwide IT technology FutureScape webcast ([report here](#)), blockchain is also becoming important in third generation security, to name just one example.

And since quite some time blockchain is increasingly being looked upon in an Internet of Things context. Blockchains have many benefits. They are not the answer to all challenges of the digital economy as sometimes is said but it's certain that they will play an increasing role in the Internet of Things.

Forrester's Dan Bieler mentioned blockchain's potential for IoT solutions. In a nutshell:

As Internet of Things applications are by definition distributed it's only normal that the distributed ledger technology, which blockchain is, will play a role in how devices will communicate directly between each other (*keeping a ledger and thus trail of not just devices but also how they interact and, potentially, in which state they are and how they are 'handled' in the case of tagged goods*).

Blockchain is designed as a basis for applications that involve transaction and interactions. These can include smart contracts (*smart contracts are automatically carried out when a specific condition is met, for instance regarding the conditions of goods or environmental conditions*) or other smart applications that support specific Internet of Things processes. This way blockchain technology can improve not just compliance in the IoT but also IoT features and cost-efficiency.

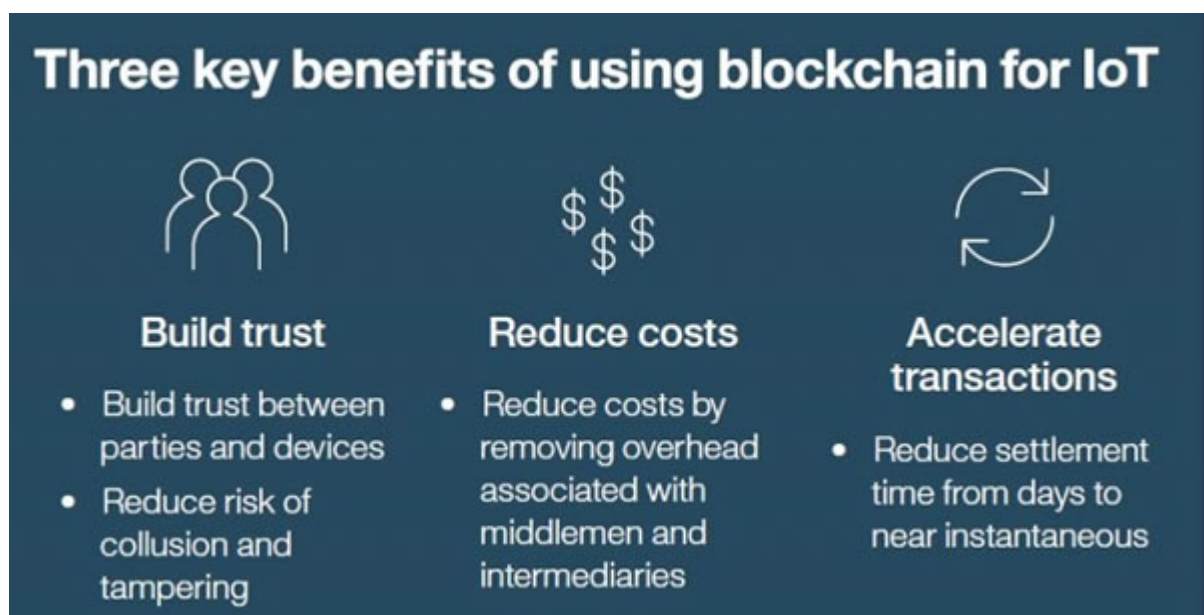
The industry is not waiting and takes initiatives

It is still early days, Bieler says. That is certainly true. However, at the same time big tech companies are not waiting, probably one of the reasons Bieler advises to start looking at the combination of blockchain(s) and the Internet of Things. And they did and will continue to in 2018 and beyond.

IBM Blockchain, for instance, already allows to extend (private) blockchain into cognitive Internet of Things. In fact, ultimately it will be the combination of [artificial intelligence](#), IoT and blockchain that will prove most interesting across industries and in myriad possible IoT applications. With blockchain we are pretty much adding to the changing digital infrastructure that powers so many evolutions and impacts so many areas, from analytics to security, in an environment that thus far was centralized.

To illustrate the benefits of blockchain and Internet of Things convergence, IBM gives the example of complex trade lanes and logistics whereby smart contracts can follow (*and via blockchain technology register*), everything that has happened to individual items and packages. The benefits: audit trails, accountability, new forms of contracts and speed, to name a few.

In the image below from an IBM infographic, the company sums up three key benefits of using blockchain for IoT. They are also often mentioned as other blockchain benefits but in other parts of the infographic and the IBM video below, there is more in-depth information about the topic. The three benefits of blockchain for IoT, according to IBM: building trust, cost reduction and the acceleration of transactions.



[source](#)

[IBM infographic](#)

IoT and blockchain challenges to solve

Forrester's Martha Bennet confirmed that it's time to start looking at that IoT and blockchain convergence, even if the combination of both might not be for today.

She defines three categories of challenges that Internet of Things and blockchain ecosystems participants must address.

In a nutshell the key challenges for IoT and blockchain ecosystems participants, according to Forrester, are:

Technology, whereby mainly security comes in the picture. In an Internet of Things context where [security is already a challenge](#), it's clear that security needs to be even more looked at. It is important to note though that blockchain is also seen as a way to secure the Internet of Things and, as mentioned, security overall but that is another discussions with several opinions and aspects to cover.

Operational challenges: the business model and the practical aspects as this requires many agreements and of course many actors too in a broad ecosystem. Just think about that IBM [logistics](#) example.

Legal and compliance issues. Bennet among others refers to responsibility issues in case of actions that are taken by devices, based on a rule that is automatically executed by a blockchain-based application, triggered by another blockchain-based application (*you see the complexity*). And then there is the mentioned example of smart contracts. As you know contracts are far from easy, even outside this IoT and blockchain context.

[More in Martha Bennet's post.](#)

Here's why blockchain is a **game changer** for IoT

Leveraging blockchain for your IoT data offers new ways to automate business processes among your partners without setting up a complex and expensive centralized IT infrastructure.

Blockchain's data protection fosters:

- Stronger working relationship with your partners
- Greater efficiency as partners take advantage of the information provided



Enable IoT devices to participate in blockchain transactions



Reimagine the world's most fundamental business interactions; open the door to invent new styles of digital interactions



Reduce the cost and complexity of operating sustaining business

[Why blockchain is a game changer for IoT according to the IBM infographic](#)

Blockchain as the answer to IoT challenges

In the Spring of 2017, Nicolas Windpassinger, author of '[Digitize or Die](#)', an [IoT book for digital transformation leaders](#), wrote about the practical aspects blockchain can address in IoT and how blockchain can accelerate the evolution of IoT.

To enable message exchanges, IoT devices will leverage smart contracts which then model the agreement between the two parties

Windpassinger: blockchain technology promises to be the missing link enabling peer-to-peer contractual behavior without any third party to "certify" the IoT transaction. It answers the challenge of scalability, single point of failure, time stamping, record, privacy, trust and reliability in a very consistent way.

Blockchain technology could provide a simple infrastructure for two devices to directly transfer a piece of property such as money or data between one another with a secured and reliable time-stamped contractual handshake. To enable message exchanges, IoT devices will leverage smart contracts which then model the agreement between the two parties. This feature enables the autonomous functioning of smart devices without the need for centralized authority. If you then extend this peer-to-peer transaction to human to human or human to objects/platforms, you end up with a fully distributed trustworthy digital infrastructure.

Blockchain + IoT across industries: the insurance example

Blockchain is being tested in several industries. And sometimes we see that in those industries there is a link between blockchain and IoT within the specific industry. Point in case: blockchain and IoT in insurance.

The main use case of blockchain in insurance are smart contracts and the enhancement of several processes such as claims management. Other applications include fraud management, legally required applications (*blockchain is thoroughly looked at in the legal sector as well*) and even the usage of technologies in an insurance context.

IoT data and blockchain can lead to intelligent automated insurance policy applications

In the scope of blockchain and IoT it's interesting to look at the combination of blockchain and the Internet of Things as it's used in insurance and will increasingly be, moving beyond the pure telematics model to the connection of real-time IoT data in various perspectives for various intelligent automated insurance policy applications.

Although this might seem like a very future application of blockchain in the insurance industry it is worth noting that from an IoT investment perspective, early 2017 IDC forecasted that insurance would be among the fastest growing industries in the period until 2021, albeit with a major focus on telematics (*where smart contracts of course make sense too*), especially as we'll see ever more smart cars and so forth.

IoT and blockchain: the broader picture and future

And it doesn't stop with somewhat more advanced scenarios in the context of insurance (whereby we only just mentioned the tip of the iceberg). With IoT and blockchain we enter a space of pretty unlimited possibilities.

The reason: as mentioned, IoT obviously doesn't stand on its own and needs to be seen in the broader context of what it enables across various use cases and industries and the additional technologies that are simply needed to make IoT work for whatever reason. Add to that ongoing convergence on technological, data and business levels and the picture becomes broader.

IoT and blockchain – from manufacturing and security to ERP and autonomous decisions

Previously we quoted Frank Gens on the role of blockchain in third generation security and mentioned how the combination of AI, IoT and blockchain will matter. These are of course not the only technologies that fit in the scope of IoT or that will matter in this mix, depending on scope and systems.

In the context of technologies in the broadest sense do, for instance, think about the convergence of [IT and OT](#) whereby operational technologies and [manufacturing technologies](#) (*and standards and protocols*) are essentially revolving around *data* (*capturing, making interoperable, analyzing, leveraging for immediate purposes, leveraging in broader ecosystems whereby data exchanges and blockchain certainly also are looked at in an IoT data perspective and beyond*), increasingly

autonomous decisions based upon data analysis (*whereby an automated interaction can be seen as some form of contract in the non-legal sense but in the sense of condition-based*).

In this context we obviously also need to mention [Industry 4.0](#) and its end-to-end data approach. And of course also the evolutions in logistics (*more with a case below*). In both Industry 4.0 and smart logistics there isn't just a focus on the end-to-end data model but also on autonomous decisions. Yet, as the case below indicates there are ample opportunities in a far less complex context.

We also need to mention security again: IoT, blockchain and next generation security cannot just cover cybersecurity as we know it but also security challenges on, for example, a plant floor or industrial environment level whereby critical infrastructure is increasingly attractive for 'the bad guys' but also different than security as we know it.

Add robotics. Add systems, such as ERP. Then there are systems. Take ERP. According to IDC IoT, blockchain and cognitive computing are three pillars for the next generation of ERP, known as [Intelligent ERP](#). The list does go on.

IoT and blockchain – from smart buildings to the energy industry

You also can look deeper into specific applications and industries: [smart buildings](#), for instance.

Among the main [building management](#) and [building energy management](#) evolutions is convergence, as is the case in so many areas where IoT comes in. One of the areas where this happens is leveraging energy coming from local solar or wind systems and microgrids in the scope of energy efficiency and [facility optimization](#).

The recording of autonomous, machine-to-machine transactions regarding electricity use is another blockchain application which would take advantage of digital platform opportunities and changing business models for tracing transactions on the smart grid ([NIST](#))

As energy becomes an increasingly digital, decentralized (!) and IoT-enabled given on various levels, including sensors as you can read in this interview on [IoT and critical power buildings](#), one can easily imagine a scenario whereby excess renewable energy could be sold and bought via blockchain. In fact, it's one of many examples that is given in the [NIST report on blockchain technology](#), presented early 2018.

The report also mentions blockchain applications for the recording of autonomous, machine-to-machine transactions regarding electricity usage.

IoT and blockchain: ever more scenarios and use cases in a world of convergence

You can easily come up with several lists of applications where IoT and blockchain play here, whether it's in the scope of the electricity industry and selling/buying and/or smart contracts or any other context where it matters to record autonomous, machine-to-machine transactions.

This could be for security and control reasons with ongoing optimization, predictive maintenance improvements and AI-enabled ways to further enhance the decision-making while enabling again new applications when, for instance combined with digital twins.

Essentially, you can look at all areas where it makes sense to do so, typically where there are many transactions or important transactions whereby one application needs another and/or is built upon others and novel technologies with data and transactions (*including contracts*) at the center.

And it doesn't even need to be that complex. Talking about "important transactions", here is that previously mentioned example of a real logistics and smart contract application (*in pilot but moving fast*) that is somewhat at the intersection of several spheres with IoT and blockchain playing an essential role.

It is a very targeted one for the pharmaceutical industry and pharma logistics but certainly can go beyond.

Modum sensors record environmental conditions that goods are subject to while in transit. When the goods change ownership, the sensor data is verified against predetermined conditions in a smart contract in the blockchain. The contract validates that the conditions meet all of the requirements set out by the sender, their clients, or a regulator and triggers various actions: notifications to sender and receiver, payment, or release of goods ([Modum.io](https://modum.io))

In the scope of regulation, whereby proof is needed that shipped medicines have not been exposed to specific conditions that might compromise their quality (*mainly on the level of temperature*), modum.io essentially combines IoT (sensors) and smart contract technology in the blockchain to offer this proof (*in combination with an app and a dashboard*). The project is born out of the Zurich university and seems to gain track with a solution that makes sense and leverages IoT and blockchain in a relevant way. There is of course a bit more to it than we describe [as you can read on the site of the system](https://modum.io).

End January 2018 the company [wrote](https://modum.io) about how it is now in integration discussions with top-level committees at major players in ERP, big pharma manufacturers, pre-wholesalers and logistics companies. A meeting of spheres indeed, whereby it's easy to see how similar systems could be applied for other logistics situations than pharma.

Blockchain and IoT use cases – a categorization

In its report, [The Internet of Trusted Things: Blockchain as the Foundation for Autonomous Products & Ecosystem Services](#), released early 2018, Kaleido Insights looked at how blockchain enables to bring trust on a product and application level and on the level of the broader ecosystem of 'untrusting constituents'.

The report emphasizes how IoT and blockchain convergence obviously don't stand on their own. Certainly when you think about the big players such as IBM and the way they are building their [IoT platform](#) roadmap to incorporate blockchain and AI, it's clear that the bigger picture is one of several technologies coming together with [IoT and AI](#), IoT and blockchain but also new deep learning algorithms, next-generation security, support for digital twins, edge computing and fog computing, high performance embedded chips, computer and machine vision, the list is pretty endless.

And so is the list of IoT and blockchain use case as the report confirms. Of course not all use cases and additions of technologies are entering at the same speed (*you won't see quantum computing entering the scene tomorrow, for instance*) and aren't valid for all industries, applications, organizations and their use cases and corresponding goals.

However, many of the use cases in the ongoing convergence of IoT and publication definitely are already there be served, both on a product/application use case level as a broader ecosystem use case category level.

The five main use case categories (*with ample examples and use cases per category*) are supply chain, IoT network management, end-user authentication, asset sharing networks and smart contracts and compliance – with security, identity, interactions and transactions as the core elements.