THE JBBA

PEER REVIEWED RESEARCH

OPEN ACCESS
ISSN Online: 2516-3957
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-3-1-(7)2020

Distributed Ledger Technologies and the Internet of Things: A Devices Attestation System for Smart Cities

Evandro Pioli Moro, Alistair Keith Duke
Department of Applied Research, British Telecommunications, UK

Correspondence: evandro.moro@bt.com

Received: 15 January 2020 **Accepted:** 16 March 2020 **Published:** 3 April 2020

Abstract
Traditional IT security mechanisms are generally not well suited for IoT devices, where processing and network connectivity should be kept to a minimum. Consequently, IoT devices have been recently identified as an easy target for cyber-attacks, like for example on the Mirai botnet Distributed Denial of Service attacks in 2016, where various devices were hacked into and taken over. Different solutions have been developed aiming at guaranteeing the security at both the device application layer and the network layer. Few succeeded to deliver the flexibility necessary for IoT devices. Even fewer have implemented an effective threats detection system, and just a handful have realised all the previous features in a fully decentralised fashion, including this one. This Distributed Ledger Technology (DLT) attestation system is maintained and supported by most, or all, IoT devices because it is based on a light-weight DLT protocol. It comprises of a system for authorisation and authentication for the individual devices as well as includes an anomalies detection system based on smart contracts. A demonstration was built to support a Smart City use case. The objective is to guarantee, in a decentralised manner, the security of low computational power devices executing the sensing function and their connectivity, and therefore the correct functioning of the system. On the demonstrator, the system was run using DLT supported by the sensors connectivity bridge (built using Raspberry Pi's). The system proved to be rapid to develop, flexible with regard to systems changes and resilient to attacks to both individual IoT devices and to the DLT.

Keywords: *Internet of Things, Distributed Ledger Technologies, Blockchain, Attestation, Smart Cities*
JEL Classifications: *H00, L22, L60, L86, M1, O32, P11, R00, Z13*

1. Introduction
a. Internet of Things

First deployed during the Second World War by the Royal Air Force for assets identification [1], radio frequency identification (RFID) tags are nowadays widely used by retailers to replace bar codes of products or to prevent shoplifting. In October 2003, during the McCormick Place conference in Chicago, USA, retail, technology and academic partners realised a local network including connected products using RFID tags. Because this network involved tracing and gathering information about different things in real time, it was called *internet of things* [3].

Now that more than a decade has passed since the McCormick Place conference, the Internet of Things (IoT) remains a technology model under development and it is expanding rapidly across different sectors. The definition of IoT has gained a more comprehensive shape, now being defined as the collection of various devices, as opposed to only RFID tags, which are able to produce data and are inter-connected over the Internet [4].

According to recent studies, the number of Internet connected devices is expected to reach 34mi by the end of 2020 [5]. A great part of this explosion in numbers is due to the deployment of an ever-growing amount of different IoT devices. Devices that traditionally were not connected to the Internet, like utility meters, cameras and various sensors, are now being provided with Internet connection and are sharing data on the web. The estimated economic impact of the IoT applications across sectors like homes, offices, health, cities and other, is estimated to going to be at least £2.2tn per year by 2025, with confident forecasts predicting an economic impact of up to £9tn per year [6].

An example of an application of IoT is to enable intelligent cities. If data about air quality, traffic, buses and trains real

[1] passive micro-chips capable of responding with information when excited by certain radio frequencies [2]

time schedule, electricity production and consumption, cycling experience and car parking occupancy is produced in real time, applications like smart people routing, intelligent energy management and air quality enhancement policies can be implemented, making commute in big cities easier, improving the air quality and energy efficiency, and enhancing road safety.

The general idea of the IoT is to bring the right information to the right people at the right time. On an IoT system, information about different environments are collected and delivered in a relevant and secure way to the end users. In between the measured environments and the information consumption, four layers of infrastructure exist: the sensors, the connectivity, the information exchange and the application layers. Figure 1 depicts this architecture with examples of some possible components on each of them.

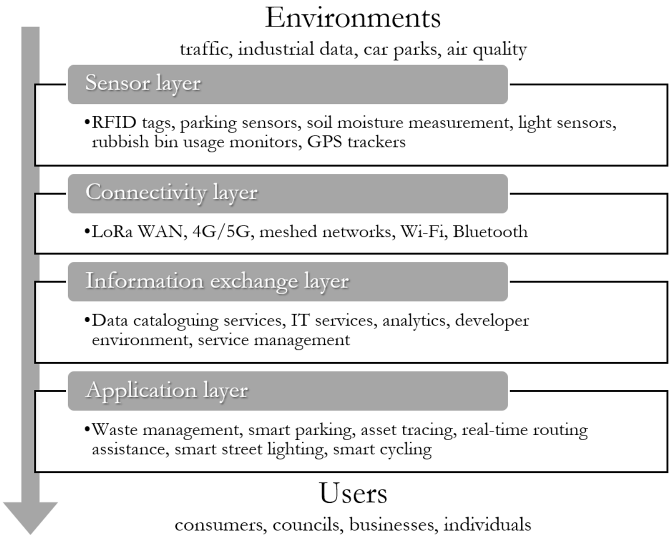
Environments
traffic, industrial data, car parks, air quality
Sensor layer
•RFID tags, parking sensors, soil moisture measurement, light sensors, rubbish bin usage monitors, GPS trackers
Connectivity layer
•LoRa WAN, 4G/5G, meshed networks, Wi-Fi, Bluetooth
Information exchange layer
•Data cataloguing services, IT services, analytics, developer environment, service management
Application layer
•Waste management, smart parking, asset tracing, real-time routing assistance, smart street lighting, smart cycling
Users
consumers, councils, businesses, individuals

Figure 1. High level architecture of a typical Internet of Things system

On the top of Figure 1, different environments are conceived, representing various eco-systems where IoT services are intended to be provided. The first layer of the IoT architecture, called sensors layer, is comprised of the various sensors deployed. These sensors are used to produce data from different sources and are provided with Internet connection, which builds the second layer of the structure: the connectivity layer. At the connectivity layer, the data is transported from the sensors to an information exchange centre by different technologies, which are dependent on the application requirements. It can be over a Wireless Local Area Network (LAN), or Wi-Fi, connection if the sensors and the environment are close to each other, like for example on a smart home or factory; or it can be over a 4G or 5G connection if the application requires wider band or faster actuation time. Yet another example largely used for narrow bandwidth and low power consuming communications provision is the LoRa WAN (Long Range Wide Area Network) technology. LoRa WAN is preferred for applications like smart solar panels within a campus, where only small data packets need to be exchanged in a power-efficient way. The third level, the information exchange layer, is where the data is stored, processed and shared across different parties. Here, the data is made uniform to be exposed and consumed, providing the ability for IoT data consuming applications to be developed rapidly. This is also where the data access policy is implemented and where the applications are provided with specific ways for interacting with the data, for example being provided with a uniform application programming interface for data input and consumption. The application layer, at the bottom of Figure 1, and is the one responsible for delivering the information to the end users in the most appropriate manner. The end users are the IoT information consumers, for example, cyclists, commuters, councils, banks or any relevant IoT information consumer.

b. Distributed Ledger Technologies

Distributed Ledger Technology (DLT) is a peer-to-peer networking system where the exact copy of a transactions ledger is shared, supported and trusted by all peers (nodes), without having to rely on a central authority [7]. If the transactions of the network are organised in the form of blocks of information, containing among the transactions, other identifiers, in such a way that one block is generated at every determined period of time and the blocks are linked (chained) to the previous ones, then the DLT is called *blockchain* [8].

Information stored on the DLT can be trusted by design because it has to undergo a decentralised and fair consensus algorithm. A consensus algorithm is a computational process by which the network collectively agrees on a single source of truth by determining which transactions are to be added to the ledger via a series of verifications. This algorithm is usually also used to decide which computing peer will be the sealing node, the node responsible to update the ledger with the newer transactions and to broadcast the newly created block to the other peers. Usually, the fairer the network is, the less repetition and predictability of sealing nodes there will be. Different consensus algorithms exist, depending on the type of blockchain and on the requirements of the use cases. For example, the Bitcoin network, where heavier requirements for security must be put in place, the proof-of-work was the chosen consensus algorithm. If an enterprise-level blockchain is designed, a more flexible consensus algorithm may be adopted, like, for example, the proof-of-authority or proof-of-stake types.

Another important feature of modern blockchain protocols is the implementation of smart contracts. Smart contracts are pieces of code executed in a decentralised fashion by all nodes of the network. They provide programmability to the system, are able to react to inputs and to the blockchain state and produce the program output at all nodes for the system. Smart contracts are pieces of code triggered either by conditions set, i.e. reacting to a certain blockchain state, or by a call from any node via a transaction [9]. They can perform various functions in a blockchain system, e.g. enabling an agreement between two or more parties, to provide virtual identities for devices, to check authorisation of nodes, to transfer digital assets, among others.

Since smart contracts reside on the blockchain, they must have an associated address, which is used to collect the funds in exchange of their execution. Moreover, smart contract scripts are inheritably deterministic, meaning that it will always provide the same outputs for the same inputs. Furthermore, all interactions with the smart contract will be supported by cryptographically signed messages registered on the ledger, meaning all smart contract interactions are traceable and auditable [13]. These factors are what make smart contracts so important for current distributed ledgers implementations.

In order to evaluate the benefits of immutable DLTs for any information technology (IT) project, five key dimensions should be evaluated in order to avoid falling into the technology hype:

- Does the project require an immutable ledger, where data cannot be deleted or updated?

This is primarily concerned with the IT challenge of access to historical data for system processes. Since blockchains structure the data in such a way that information cannot be changed, thanks to its hashing algorithm implementation, deletion or change of data in the ledger is very complicated and energy consuming. At DLTs, the information is generally stored in a way such that it contains one field storing a reference to a series of previous transactions bundled together. In blockchains, this reference is usually implemented at block level as the hash output of all the previous blocks bundled together to generate the hash output. This means that in order to change or tamper with one or more transactions on any block, a new recalculation of the entire blockchain is necessary, requiring an immense computational cost and a prolonged time. This makes changes to the ledger generally an impractical task.

- Do the interested parties need access to a single and trusted source of truth?

This is primarily concerned with the IT challenge of access to true information for processes. DLT is a repository of transactions and data which is synchronized, shared and supported by peers without the requirement of a central authority mediation. Usually guaranteed by the network consensus algorithm, DLTs assure all peers of the network trust on the data stored on the ledger. All nodes have a local and synchronised copy of the ledger of transactions and can fetch any transaction or provide access means to non-peer users at any time, representing an attractive technology candidate for IT projects where various parties need to access a singular repository of data which all can inheritably trust in order to convey truthful information.

- Is an independent and cryptographic audit trail required for the use case, e.g. to prove identity, state or provenance of an asset?

This is primarily concerned with the IT challenge of access to data for audit purposes. DLTs process transactions using uniquely referenced signatures for peers based on enhanced cryptographic protocols. Furthermore, all the history of actions of the unique signatures is stored on the immutable ledger. Hence, provided DLTs are powerful tools to store immutable and historical data and are a trusted source of information to all peers, it proves to be a strong technology candidate to power audit trails IT systems.

- Does the system have good reasons for not putting a centralised utility in place or to have a single entity in control of the architecture activities?

This is primarily concerned with IT systems which are by nature, or need to be, decentralised. DLTs are systems that enable trust, immutable information and audit trails in a decentralized fashion. In general, the consensus algorithms for a DLT require a plurality of peers to be effective, meaning that it is designed to enable access to decentralised, and trusted information provided multiple parties participate in the system. If this is the case, and there are reasons for not having an authority, or a peer, with elevated control of the network activities, DLTs are a candidate technology to enable trust on the data when there is no central authority in place. This is often referred as the *trustless* feature of DLTs.

- Does the interest of the parties lie on the success of the system, to keep its distinct characteristics?

As explored previously, DLTs can adopt different types of consensus algorithms, depending on the use case requirements. After all, a DLT system will only make sense for any application if the previously explored characteristics will add value to the IT project and if the participants are interested in keeping these distinct characteristics. This is especially true for enterprise DLTs, where the levels of computational power requirements might need to be reduced, provided the parties are interested in participating fairly on the system. If this is not true, then the computational requirements for a proof-of-work type of consensus algorithm may be prohibitive.

2. Blockchain transactions verification process

General blockchain algorithms implement a recursive and powerful transaction verification process to guarantee that no malicious transactions are sent. Currently, the systems verify for double spending problems (if a user is trying to send the same funds twice in subsequent transactions), verifies the existence of the receiving account, checks for enough funds on the sending account and verifies the key of the sending node (to check if the sending node is the same as the one that signed the transaction). However, there are other fields on a blockchain transaction which are not verified before they are fully processed by the network, including the transaction data field. This data field can be used, for example, as an identifier of the transaction (like reference numbers of bank transfers) or parameters for a smart contract function call (the arguments of the code functions).

One of the ways of invoking a smart contract is through DLT transactions. This is accomplished by sending a transaction of funds in exchange for the code execution efforts. It is therefore important that when a peer is invoking a smart contract with arguments sent in the transaction data field that this is accurate and verified for the system safety. Of more important here is that this is verified in a use case-dependent manner, for instance, if a smart city application is concerned, the sensors data sent across the transaction data field on a blockchain transaction should be accurate.

Therefore, verifying the transaction data field before the transaction is processed by the network can save execution time, and it also helps to reduce the risks of deceptive invoking of smart contracts from happening, hence improving the value of an IoT solution. Moreover, if this verification is flexible enough to perform checks that are relevant to the DLT use case, for example, if it is able to verify that the arguments of the smart contract invoked are pertinent, the aggregated value of this solution for the network is even greater.

3. Internet of Things devices security

Because of the unprecedented increase in the number of IoT devices over the past decade and the growing importance of IoT in IT infrastructures, ensuring the security of IoT devices is at the centre of numerous research projects of the Information and Communications Technology (ICT) industry and academia, and a valuable market niche. It is estimated that the aggregated spending in IoT security measurements has been £780mi in 2018 and it is estimated that it will be four times bigger in 2022 [10].

The design constraints and low computational power of these devices can make them an easy target for cyber-attacks, as it happened in August 2016 with the Mirai botnet attack. The Mirai botnet was a malicious piece of software released to take control of devices like web cameras and digital video recorders running a specific version of a light-weight operational system. From these devices, the botnet took control of other IoT devices connected nearby, causing a big Distributed Denial of Service (DDoS) [11]. Since August 2016, other types of IoT devices were infected in various attacks of the world, exposing the need to increase the security of IoT devices.

Traditional IT security mechanisms designed for computers, servers and systems are based on a three-layer defence structure: static perimeter network layer (i.e. firewalls, intruder detection systems), end-host defence tools (e.g. antivirus software) and software patches (i.e. re-deployment of security packages on a regular basis) [12]. This traditional security structure is not well suited to IoT devices, where software processing and network communications should be kept at a minimum. More specifically, different use cases require different types of IoT structures and security levels; thus, generic IT security systems are difficult to implement for these cases and are often not flexible enough. For instance, a mobile phone application which controls IoT devices via different channels and an IoT ecosystem where one device can affect both its concerned application and another IoT device, require different types of perimeter, end-host and patch security measurements. Moreover, the constrained hardware and software on-boarded to an IoT device reduce their ability to run mechanisms to detect anomalies on the network traffic and to perform complex signature protocols. Furthermore, because IoT devices will often tie the sensing and connectivity layer activities together, and in some cases will also respond with actuation, effectively providing application interface and traditional perimeter defence mechanisms are not efficient. Finally, yet importantly, considering these devices do not run full operating systems, the traditional end-host tools and patching will not work as effectively as they would on traditional IT systems.

In sum, there are two key points to highlight as main network security issues around IoT: end-host defence tools (like antivirus or software-based anomaly detection systems) are not feasible, once the devices are restricted in resources, and traditional static perimeter mechanisms are not as straight-forward as they are for traditional IT systems because these devices are deployed deeper into the network, with their physical and computational behaviour constantly changing.

4. IoT Devices Attestation System for Smart Cities

The solution comprises of a DLT, herein described as a blockchain system with a proof-of-authority type of consensus algorithm, which is used as a registry of IoT data transactions as well as a repository of device profiles, containing, but not limited to, their expected behavior, their system authorisations and an actions registry. These transactions can be the purchase or selling of data feeds, e.g. councils selling air quality information to an IoT service provider, or simply a commit of data regarding a smart utility meter, as a blockchain transaction to a smart contract, for instance.

The selection of the blockchain nodes is flexible. The nodes can be deployed into the IoT edge computing devices, with a mixture of light and full nodes (if the blockchain infrastructure is light enough to support such a development); it can also be on the servers of the IoT service provider (in a cloud type infrastructure), since they usually have more storage and processing capabilities; it can be a set of trusted and bespoke computing nodes for the application; alternatively, it might also be a public and shared infrastructure (as long as it is compliant with the use case privacy requirements).

The generic architecture of the solution comprises of an IoT ecosystem together with a blockchain backend to provide an anomaly detection system based on smart contracts. The solution accomplishes this by introducing a mechanism capable of inspecting the data field of the blockchain transactions in real time. This can be implemented as an interface, for example an application programming interface (API), to compare the data sent within a transaction with the device expected behavioural data stored in the relevant smart contract. This provides unexpected behaviour detection if one or more IoT devices are compromised, once the registry on the blockchain cannot be changed, are trusted by nature and provide any party on the IoT ecosystem with the ability to check if the current behaviour of the devices is correct according to the device role, profile or expected behaviour. This is designed to provide near real-time information about intrusions, attacks, data tampering or device failures.

In a simple example, represented in Figure 2, suppose a town council is building a smart city ecosystem which comprises of, amongst other sub-systems, an air quality monitoring system. During the system set-up, the town council sets out the expected gas levels to be a given maximum which are then registered as one of the expected behaviour parameters inside the concerned smart contract within the blockchain of cloud-type. Other parameters can be, for example, frequency of data updates, usual data packet size exchanged, and others. Because these parameters reside on the blockchain, they are immutable and shared across all the peers of the blockchain network. When the system starts operations, the air quality information flows from the air quality sensor, to the left of the diagram, to the town council, to the right of the diagram, via the transaction data inspection interface and the blockchain system. This inspection interface serves the purpose of allowing the system to verify the data sent by sensors against the expected devices behaviour parameters residing at the smart contract. As the second step on this information flow, the sensor data is registered on the blockchain for the purposes of anomaly detection. With the aid of the data inspection interface introduced, the relevant smart contracts can process the transaction data sent to another party against the expected parameters and flag a malfunctioning device. This system will then flag the device for further investigation, and depending on the system design choices, can halt the sensors' activities remotely by changing its authorisation parameters on another smart contract.

On the system described, IoT transactions are completed via the blockchain system with the aid of smart contracts. In order to provide full integration of the IoT ecosystem with the blockchain, lightweight APIs were developed. By using these APIs, the devices are locally provided with the ability to commit sensor readings and, more importantly, to verify other devices' integrity. The system is also capable of providing signature verification and implementing identity provisioning mechanisms if required to build a comprehensive authentication, authorization, and accounting (AAA) system. In case devices are flagged as malfunctioning, the system manager can halt their actions on the system by changing their authorisation parameter on the AAA agreement until they are fully recovered. Alternatively, the system can impede the compromised device to ever participate again, by revoking its identity on the blockchain, which represents a ban on the unique device signature.

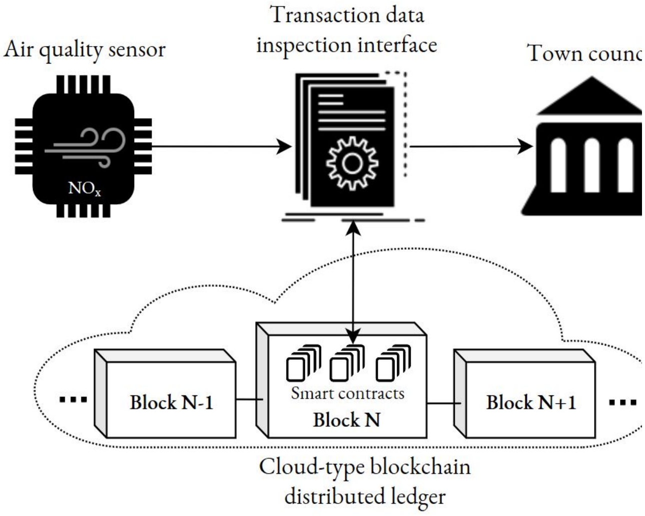

Figure 2. Example application of the IoT devices attestation system based on a cloud type blockchain and a set of relevant smart contracts.

In an alternative setting, the system can detect anomalies independently, meaning the IoT devices when transacting via the distributed ledger will be able to independently verify the transactions. On a generic setting, the IoT sensors participating on a typical IoT system are comprised also of a blockchain to actively trade data. This system is distributed and does not require a central authority to process the transfers, nor to verify and detect anomalies on the data transacted. Figure 3 depicts this setting, where a smart utility meter replicating the blockchain represents the data purchaser

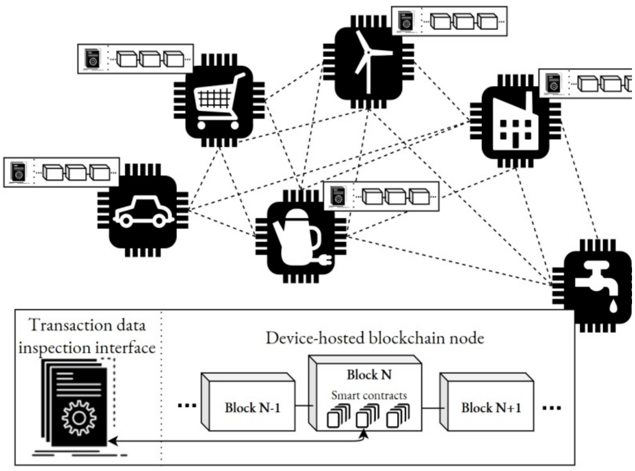
Transaction data inspection interface
Device-hosted blockchain node
...
Block N-1
Block N
Smart contracts
Block N+1
...

Figure 3. Generic architecture diagram of the solution proposed for deployment at the IoT devices with edge computing capabilities.

and can make calls to a transaction verification interface, which can run locally, to perform the checks on the data field of the blockchain transactions. The transaction verification interface will enable the data consumer to compare the transaction data against the device expected behaviour registered on the DLT shared across all IoT devices, including the smart utility meter. This is essential in keeping the system safe from failures and is accomplished in a distributed fashion, happening automatically.

5. Analysis

This solution leverages from the decentralisation feature of blockchain to implement a detection system that is independent of a central authority and which can still be trusted by any peer on the network even when they do not have an established trust relationship with each other. v

This system does not implement end host software in order to allow for maximum performance of the constrained IoT devices. On the other hand, the system implements a strong perimeter network layer protection, by using blockchain smart contracts to interface the IoT transactions while verifying for anomalies. This network layer protection provides means to detect attacks to IoT devices and measurements to reverse them, as well as to provide preventive actions against malfunctioning devices. Additionally, the solution is flexible and agile. Although immutable by nature, new smart contracts can be deployed to all peers quickly and therefore updates about the network operation to cover for new devices expected behaviours can be quickly put in place.

This solution helps adding value to the IoT by realising a decentralised, auditable and trusted devices attestation system. With a light-weight and flexible implementation of DLTs, the solution enhances the trust on the data shared on the IoT, enabling a use case of DLTs as a platform of trust.

6. Conclusion

The rapid development of the IoT over the past decade brought many different applications to life and truly revolutionised the way society lives and consumes data. It made cities smarter, helping to improve the way people commute, made energy more flexible, helping to take down barriers of energy trading, helped councils to save tax payer money by pre-empting road quality issues, among other many applications. At the same time, this quick deployment of millions of low processing power devices revealed the need of to increase device and networking security for the IoT.

The blockchain technology, conceptualised in the early 1980s but only first implemented in 2009 [14], truly revolutionised the way information can be trusted without relying on a central authority. This technology has already been adopted by different sectors to enhance security over transactions. Banks, insurance providers, aircraft manufacturers, and others, leveraged this technology to provide assurance over their data, avoiding the risks of having divergent information and to enable trusted systems and agreements without the central authorities' instrumentation.

The need to improve the technological architecture of blockchain protocols for specific use cases together with the need of increasing the security of IoT devices, has broached an interesting research topic. The solution proposed comprised of a blockchain system serving the purpose of providing an IoT system with predictive failure and attack detection capabilities, by monitoring the information exchanged by the devices against their designed role on the system.

The synergy between IoT and DLTs is believed to still be in its infancy. DLT has already been proven to be efficient in addressing issues around trust and security of ICT data. It is important to realise that, although blockchain technologies help to solve various issues faced by ICT systems, it still has its own challenges such as relatively high computing processing and large data storage demands, if not carefully designed. Considering these limitations and analysing the benefits is of ultimate necessity when designing a DLT system for the IoT, which demands rapid and trustworthy information exchange. The solution presented in this report is flexible with regard to the type of DLT and is designed to be quickly adapted to newer types of DLTs, regardless of their design.

Nonetheless, it is believed that DLTs are still in the early days of its development, with immense potential to continue revolutionising the way information is stored, shared, audited and trusted. The IoT is one of the biggest potential beneficiaries of this new technology, since it requires trustworthiness on the information it processes, usually in a decentralized way. Developing a powerful interconnection between these two technologies represents a demanded enhancement on IoT systems security and it is therefore expected to bring new business models and to drive changes across many of the existing systems and processes, helping to deliver greater value to the Internet of Things.

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
I am the author, Alistair proof read the article..

Funding:
None declared.

Acknowledgements:
I would like to thank Prof John Davies for the research leadership within the team as well as Dr Alistair Duke for the daily support on my projects.

References:

[1] Dodson, S. (2003). The internet of things. [online] The Guardian. Available at: https://www.theguardian.com/technology/2003/oct/09/shopping.newmedia [Accessed 24 May 2019].

[2] Bonsor, K. and Fenlon, W. (2019). How RFID Works. [online] HowStuffWorks. Available at: https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/rfid.htm [Accessed 24 May 2019].

[3] Sundmaeker, H., Guillemin, P., Friess, P. and Woelfflé, S. (2010). Vision and Challenges for Realising the Internet of Things. Brussels: European Commission - Information Society and Media DG, p.12.

[4] Luigi Atzori, Antonio Iera, Giacomo Morabito, The Internet of Things: A survey, Computer Networks, Volume 54, Issue 15, 2010, Pages 2787-2805, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2010.05.010.

[5] Business Insider. (2019). BI Intelligence projects 34 billion devices will be connected by 2020. [online] Available at: https://www.businessinsider.com/bi-intelligence-34-billion-connected-devices-2020-2015-11?r=US&IR=T [Accessed 8 Feb. 2019].

[6] Colin Tankard, The security issues of the Internet of Things, Computer Fraud & Security, Volume 2015, Issue 9, 2015, Pages 11-14, ISSN 1361-3723, https://doi.org/10.1016/S1361-3723(15)30084-1.

[7] Iansiti, M. and Lakhani, K. (2017). The Truth About Blockchain. Harvard Business Review, R1701J, pp.4-5.

[8] K. Biswas and V. Muthukkumarasamy, "Securing Smart Cities Using Blockchain Technology," 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Sydney, NSW, 2016, pp. 1392-1393. doi: 10.1109/HPCC-SmartCity-DSS.2016.0198

[9] Sun, J., Yan, J. and Zhang, K. (2016). Blockchain-based sharing services: What blockchain technology can contribute to smart cities. Financial Innovation, 2(1).

[10] IOT Analytics. (2017). IoT Security Market Report 2017-2022. IoT Analytics. Retrieved from https://iot-analytics.com/product/iot-security-market-report-2017-22/

[11] J. A. Jerkins, "Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code," 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, 2017, pp. 1-5. doi: 10.1109/CCWC.2017.7868464

[12] Yu, T., Sekar, V., Seshan, S., Agarwal, Y. and Xu, C. (2015). Handling a trillion (unfixable) flaws on a billion devices. Proceedings of the 14th ACM Workshop on Hot Topics in Networks - HotNets-XIV.

[13] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," in IEEE Access, vol. 4, pp. 2292-2303, 2016. doi: 10.1109/ACCESS.2016.2566339

[14] Luther, W. (2016). Bitcoin and the Future of Digital Payments. The Independent Review, 20(3), 397-404. Retrieved from www.jstor.org/stable/24562161