EMMANUEL OKORO

ENERGY CONSIDERATION WHEN INTEGRATING BLOCKCHAIN WITH IOT FOR ANTI-COUNTERFEIT

Master of Science Thesis

Examiner: Prof. Donald Lupo
& Asst. Prof. David Hästbacka
Examiner and topic approved
by Dean of faculty Electronics
and Communication on 08
August 2018

ABSTRACT

EMMANUEL OKORO: Energy consideration when integrating Blockchain with IoT for anti-counterfeit

Tampere University

Masters of Science Thesis, 53 pages

December 2019

Master's Degree Programme in Electrical Engineering

Major: Electronics

Examiners: Professor Donald Lupo and Assistant Professor (tenure track) David Hästbacka

Keywords: IoT, Blockchain, Energy, RFID, NFC, Mining, Consensus

Blockchain technology has been growing in popularity after Bitcoin, the first protocol has demonstrated a strong use case of the technology in Finance. Over the years, as the technology develops more and more, other use cases for the technology which basically relies on a distributed ledger database system have been explored in areas like supply chain and Internet of Things, to help in some of the bottleneck which IoT faces, some of the challenges are security, privacy, scalability, etc.

This thesis work will consider energy consumption when integrating IoT with the Blockchain for anti-counterfeit purposes. Because there is little public academic information about the integration of Blockchain with IoT, it is very difficult to ascertain quantitatively, the energy requirement in application areas like anti-counterfeit. This thesis work has to qualitatively, rely on projects whitepapers and application documentation when comparing the energy requirement in the integration of Blockchain and IoT used for counterfeit solutions by different projects. Both private and public (open-sourced) projects were considered and resulted in two broad classifications 'integration by brands using a unique identifier (RFID and NFC)' and 'integration throughout a product lifecycle'. Energy need for each project(s) in a class is considered based on the IoT hardware used and the Blockchain generation and consensus which also seems to have an impact on the implementation cost and complexity of the project.

PREFACE

I will like to say a big thank you to everyone who in one way or the other helped me during the course of this thesis. Special thanks to my supervisors, Prof. Donald Lupo, and Asst. Prof. David Hästbacka. Big thank you to my family for their support all through my studies and my friends, especially, Augustine Aninwezi and Ugochukwu Aronu.

Tampere 02.09.2019
Emmanuel Okoro

Table of Content

Chapter One: INTRODUCTION ……..…..… 1

1.1 Problem Statement and Scope …….…..…..... 1

Chapter Two: INTERNET OF THINGS (IoT) …….……...….. 3

2.1 History and Introduction of Internet of Things (IoT)…….……...…. 3

2.2 IoT Architecture ……...…….. 4

2.3 Applications of IoT ……..…..… 5

2.3.1 Industrial application ……...… 5

2.3.2 Home automation application …….....… 6

2.3.3 Smart cities application ……..…. 6

2.4 Challenges in IoT (Implementation) …….….. 7

2.5 Blockchain Applications …… 7

Chapter Three: BLOCKCHAIN …….. 9

3.1 Introduction to Blockchain …… 9

3.2 Different types of Blockchain ……..… 11

3.2.1 Blockchain Types Based on Accessibility ……..……..…… 11

3.2.1.1 Private/Permissioned Blockchain ……..…. 11

3.2.1.2 Public/Permissionless Blockchain …….…. 11

3.2.2 Blockchain Consensus …….…….…. 13

3.2.2.1 Proof of Work …….…….…... 13

3.2.2.2 Proof of stakes …….……... 14

3.3 Applications of Blockchain ……..……..…….…….... 15

3.3.1 Application in Finance …… 15

3.3.2 Application in Supply Chain ……... 16

3.4 Current challenges with Blockchain …….. 20

3.4.1 High Energy Demand in Blockchain ……..... 20

3.4.2 Scalability of Blockchain ……..... 21

Chapter Four: POWER CONSIDERATION DURING INTEGRATION …….. 22
4.1 Energy requirement in IoT network …….. 22
4.2 Energy resulting from different actions ……. 25
4.2.1 From data centers …… 25
4.2.2 Machine-to-machine communications …… 26
4.2.3 Embodied energy …… 28
4.2.4 Obsolescence digital technology ……. 28

4.3 Energy consideration when integrating IoT with Blockchain ……...… 28
4.3.1 Considering Application ……. 28
4.3.2 Considering Blockchain protocol/type and consensus ……...… 29

Chapter Five: WAYS OF INTEGRATING IOT WITH BLOCKCHAIN FOR ANTI COUNTERFEIT PURPOSE ……...… 31

5.1 Integration by brands through a unique identifier (Linxens, Smartrac & Vechain) …… 31
5.2 Integration throughout product lifecycle (Waltonchain) ……. 33
5.3 Proposed Ideal Integration Method ……. 36
5.4 Ideal Application Scenario (case) …… 40
5.5 Energy Consideration for the Scenario (case) …….. 41

6 Chapter Six: CHALLENGES AND CONCLUSION ……. 42
REFERENCE ……. 47

LIST OF FIGURES AND TABLES

Figure 1. The layered architecture of the IoT
Figure 2. The contents of a Blockchain block
Figure 3. Architectural sketch of a Blockchain
Figure 4. Formation and content of a block
Figure 5. Illustration of Blockchain use in product provenance or attestation
Figure 6. Illustration of Blockchain integrated with IoT for product real-time monitoring
Figure 7. Illustration of Blockchain use in supply chain dispute resolution
Figure 8. The growth rate in bitcoin mining energy consumption
Figure 9a. Proposed role-based layered architecture
Figure 9b. Proposed system architecture
Figure 10. Proposed energy-efficient architecture for IoT network
Figure 11. The global carbon footprint for mobile communication projected till 2020
Figure 12. dLoc ecosystem
Figure 13. Waltonchain ecosystem diagram
Figure 14. Encrypted data collector
Figure 15: An Ideal application in pharmaceutical industry

Table 1a. Few properties of Public and Private Blockchain
Table 1b. Comparing Public, Private and Consortium Blockchain
Table 2. Comparing different clustering algorithms for WSNs
Table 3. Comparing the two integration methods

LIST OF ABBREVIATION

AL	Application Layer
API	Application Program Interface
ASIC	Application Specific Integrated Circuit
BG	Byzantine General
CH	Cluster Head
CMOS	Complementary Metal Oxide Semiconductor
DPoS	Delegated Proof of Stake
DSL	Digital Subscriber Line
eGNs	Energy Saving Gateway Nodes
eRA	Energy-Efficient Resource Allocator
FTTN	Fiber To The Node
HFC	Hybrid Fiber-Coaxial
IC	Integrated Circuit
ICN	Inventory Control Number
IoT	Internet of Things
IP	Intellectual Property
IPL	Information Processing Layer
KYS	Know Your Suppliers
M2M	Machine-to-Machine
MB	MegaBytes
NFC	Near Field Communication
P2P	Peer-to-Peer
PC	Personal Computer

PoL Proof of Labor

PON Passive Optical Network

PoS Proof of Stake

PoW Proof of Work

PtP Precision Time Protocol

RAN Radio Access Network

RFID Radio Frequency Identification

SAM Secure Access Module

SCL Sensing and Control Layer

Sub-G Sub-GHz

TpS Transaction per Second

TWh TeraWatt Hour

UMTS Universal Mobile Telecommunication S

USD United States Dollar

WiMax Worldwide Interoperability for Microwave Access

WSN Wireless Sensor Network

CHAPTER ONE: INTRODUCTION

Fake products or counterfeited or pirated products have been of great concern to the global trade of physical goods as it impacts all nations and hinders innovation in the global economy [1]. The recent spread of the internet means that the number of people purchasing products online through popular e-commerce platforms like Amazon and Alibaba is increasing rapidly. Tracking of fake products very hard for these platforms with the result that 2.5% of the counterfeit products (461 billion USD) transactions in international trade were estimated as of 2013 [1]. This has increased and as of 2017 to the amounts of 1.2 trillion USD. It is projected to reach 1.82 trillion USD by 2020 [2].

Counterfeited products are a big problem in global trade not just to big brands and nations but also to the consumers especially in the food or drug industries where not just capital but also life is lost [3].

Much research has been performed within organizations, nations, and institutions on applicable solutions to stop fake products in the global trade, some solutions have been designed and implemented but are either expensive to implement or can be exploited by bad actors. In some cases, because of the complicated nature of the existing supply chain, most organizations and brands risk exposing some of their confidential data in the process.

The inherent privacy and security properties that the Blockchain technology possesses as a result of its distributed data ledger network, makes its integration with IoT systems a natural fit to solve the counterfeit problem. There are still challenges to solve to realize this. Top among these is high energy consumption [4].

1.1 Problem statement and Scope: With the rapid development of Blockchain technology, integration with IoT is sought to tackle fake products since existing solutions for counterfeiting are error-prone, easy to exploit or complex to implement as there are always different parties involved. This thesis work looks at how different Blockchain projects (both private and public) integrates with IoT using RFID or NFC to track a product for anti-counterfeit purposes throughout a product's lifecycle. It tries to classify them into two broad classes and compare how they differ in teams of energy need, security, complexity, and cost of implementation. Finally, an ideal solution and integration method is proposed with consideration on the energy need such that data

is uploaded directly to the Blockchain on the chip level with minimal error or chances of corrupting the data, therefore creating authentic data that can be traced back to the source (origin).

With little or no academic material about this topic, the thesis work had to qualitatively rely on projects whitepaper and documentation materials of Blockchain projects and application that integrates IoT accessed from a web portal (https://coinmarketcap.com) that list basic information about Blockchain projects. The selected projects were such that each had a unique way it integrated with the Blockchain with few shared similarities such that its energy requirement, security, cost, and complexity can be accessed and compared for different application scenarios. To achieve this, projects that integrated with both private and public Blockchain was considered together with how they are interfaced and the IoT device used (RFID or NFC).

CHAPTER TWO: INTERNET OF THINGS (IoT)

2.1 History and Introduction of Internet of Things (IoT)

Internet of things (IoT) was a term used to describe a system where the internet enables connections with real things through a ubiquitous network of data sensors and was first documented by Kevin Ashton in 1999 [5]. Right from the 1990s, internet connectivity began spreading across enterprise and consumer markets, and this led to an improvement in factory automation and automotive connectivity, wearable body sensors, home appliances, and other automation application to date [5]. Through IoT, an intelligent system is created to form an invisible network fabric that can be sensed, controlled and programmed.

Embedded technology has enabled IoT product devices to communicates directly or indirectly with each other or the internet [6] and all these are possible because the embedded systems have a microcontroller that runs software with little memory footprint placed in almost every IoT devices we use. It is foreseen as the most disruptive technology to touch every part of our lives [7] with such networks of things around us constantly changing and evolving based on our surroundings and inputs from other systems. With about 5 billion IoT devices already connected till date [6] and more to be connected in coming years, IoT complimented with other new technologies like Blockchain and AI have shown great prospects to improve our lives and make it better in areas such as:

- Safe autonomous cars that can safely sense each other and avoid accidents
- Smart lighting systems for street lighting can make us live greener as the light is automatically controlled based on the amount of daylight outside
- Wearables systems which detect illness like cancers and heart attacks before there happens, therefore, making us live healthier [6].

Prediction by Gartner is that about 26 billion units of things will be connected via the internet by the year 2020, while Cisco has an even higher prediction of 50 billion. Connected things as used here also mean a range of devices connected through a secondary network like RFID, Sensors, NFC, Bluetooth nodes, and home networks like 6LoWPan, Zigbee.

2.2 IoT Architecture:

The most popular IoT architecture is based on layer architecture that has evolved from a three-layer architecture to a five-layer architecture [8, 9]. This evolvement became necessary with improvement in technology development and with more researches carried out to solves some of the major challenges like security, privacy, and high energy limiting IoT applications. Figure 1 below shows the three-layer and five-layer architecture.

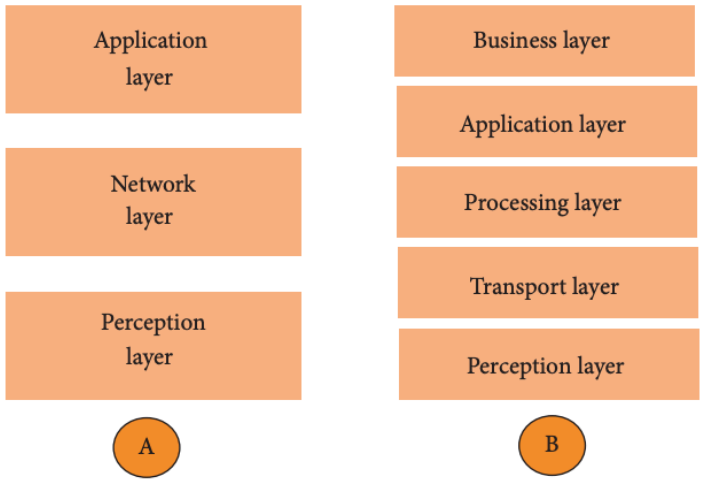


Figure 1: The layered architecture of the IoT [8].

The Perception layer is the physical layer that acts the same as the human sensing organs (nose, eyes, etc. It uses sensors and RFID, bar-codes attached to an object to continuously collect information about the objects and their surrounding environments or over a time interval. There are possible threats in this layer that can be exploited by bad actors to gain access to the network or objects connected in the network [10,11,12,13].

The Network layer acts as a bridge between the application and perception layer by using a wired or wireless system to connects and transfers data between the two layers, other network devices or the server (cloud). The choice of transmission network can have a great impact on the energy requirement of the entire IoT system which will be shown later. Also, different kinds of threats like in [14, 15, 16] are possible at this layer which can be exploited by an attacker.

The Application layer is where different applications like industrial or consumer-based are deployed. Example of such applications are in smart cities, health care, smart home, etc which relies on the IoT network for its services. Just like the other layers, there are major security issues at this layer as well, such as ones covered in [17].

To resolve the threats that are possible in the three-layer architecture, results from researches lead in a proposal for a five-layer architecture that tackled some of these major threats. These layers have all the layers in the three-layer architecture with the inclusion of the processing layer or the middleware layer and the business layer. The middleware layer collects all the data or information from the transport (network) layer and analyzes and processes the data using big data processing modules or cloud computing to remove unwanted data and improves generally the performance of the IoT systems. While the Business layer is introduced to manage the whole IoT system, user access, user profile, and privacy. The general system performance and security are improved by the five-layer architecture.

2.3 Applications of IoT:

The advancement in sensors, RFID's and other hardware technologies have resulted in research successes in the IoT field. This has extended the applications from just the basic machine-to-machine (M2M) communication and exchange of data to other applications in commercial and industrial automation, wearables and other unforeseen fields. Some of these applications will be explored further below.

2.3.1 Industrial application:

In manufacturing, products can be connected to information technologies at manufacturing sites through embedded smart IoT devices or unique identifiers using RFID to interact and exchange information with other products or with other sets of an information system [18]. Production processes can be improved by this and the products whole lifecycle can be easily tracked and recorded to prevent cloning most especially of high-cost products with counterfeits along the supply chain. In other industries like the oil and gas, cases like in [19] can be prevented using identification systems integrated with IoT and wireless systems, designed and implemented to monitor petroleum personnel in critical onshore and offshore operations and also to track other drilling components or equipment to avoid accidents and loss of lives or properties.

2.3.2 Home automation application:

IoT can also be applied in home automation, reasons being that maturity in sensors, actuator, and wireless technologies have reduced device price and also people trust in technology have increased over time in addressing their concerns about the quality of life and security of their home like in the example as stated in [20]. Sensors combined with artificial intelligence technology can serve as an intelligent agent at homes for elderly people and by using algorithms, can adapt to the routines of the inhabitants, trigger some events or response automatically. An example is the MavHome project [21]. Another application also is in energy conservation in homes, for automatic control of the lighting system, such that light can be automatically turned off when movement is not sensed over a while [18]. Also, through context awareness, an environmental parameter such as temperature and humidity are measured and analyzed and used to turn ON appliances like air conditioning units automatically [23].

2.3.3 Smart cities application:

The high population in cities resulting from migration from the rural area and other countries means that cities' resources must be used optimally and efficiently. IoT is used to manage resources by using smart meters, sensors and wireless systems applied in smart transportation like in [23]. There is also smart water management, used to control water resources efficiently in city areas as in [24], smart energy and lighting systems that automatically switch street lighting ON and OFF when necessary and manages energy usage. Smart waste and recycle management is another recent prominent application of IoT used for the collection of recyclable materials and proper disposal of wastes to avoid climate changes [18].

2.3.4 Supply Chain and Logistics:

Supply chain and logistics use IoT to simplify the complex real-world business processes in information digitalization and management [25]. IoT devices can be attached to goods, to easily track, record and analyze information about the goods throughout their production stage to their distribution and consumption stages using RFID or NFC systems. The RFID system, for example, has continued to provide greater visibility in the complex supply chain management by helping

the different companies and parties involved to efficiently track and manage inventories in real-time therefore helping reduce unnecessary transportation and other logistics costs [18].

[26] gave an example of an information transmission system based on IoT technology that can be used in supply chain management. IoT devices like RFID have been integrated with sensors for smart shelves used in retail and supply chain management to track when products in a shelve are sold in real-time, therefore optimizing retail inventory applications and processes [27].

2.4 Current Challenges with IoT Technology:

Notwithstanding the research advancement and breakthrough in IoT technology areas such as wireless communication, sensors, and power management, there still exist challenges yet to be overcome to achieve the full potentials of the technology.

These challenges can be grouped into technological, businesses and societal challenges [28] that cannot be solved through technology alone. The major technological challenges for IoT are security and privacy of data collected and the network through which the data is transmitted [29, 30, 31]. There have been several incidents of security breach and theft of IoT data. Also, as the number of connected devices grows and becomes more complex over time, the issue of energy consumption arises for the devices used for sensing, processing, networking, and storage. This means that a better energy-efficient device, a highly efficient hardware architecture, and a software architecture, will be highly needed to drive future IoT applications.

Non-technological problems that are business or social related can be solved through innovative and sustainable business models that are profitable for the stakeholders involved and through social engineering respectively.

2.5 Blockchain Application:

Blockchain is quite a new technology that is becoming more popular after its application as a cryptocurrency used for transfer-of-value and will be properly explained in the next chapter. The key characteristics are being a decentralized network, data immutability, high data transparency and fault tolerance network [32] inherent from its distributed ledger data structure. This makes integration with IoT technology very intuitive because it compliments well and aligns to be a

perfect solution for most of the IoT challenges listed in 2.4 above. [33, 34, 35, 36] considered how Blockchain could be a solution to the security, privacy and trust issues faced by IoT technology while there are research implementation works with projects in [37, 38, 39, 40, 41, 42, 43].

CHAPTER THREE: BLOCKCHAIN

3.1 Introduction to Blockchain

Blockchain is a decentralized distributed network technology that uses a distributed ledger system to keep track and store records of data in the form of a sequence of blocks which join with one another. It is decentralized such that no single entity or body has total control over the network. A block normally consists of a block header and body as shown in figure 2 below. Also, an example of a Blockchain architecture is shown in figure 3. The initial first block is known as the genesis block and is formed from the initialization of the network. Subsequent blocks are added in chronological order with previously formed blocks without any dependency on a central body [44]. This results in a chain of data network that is trustless and immutable as anyone can join without the need for central control and the data on the blocks cannot be modified once added.

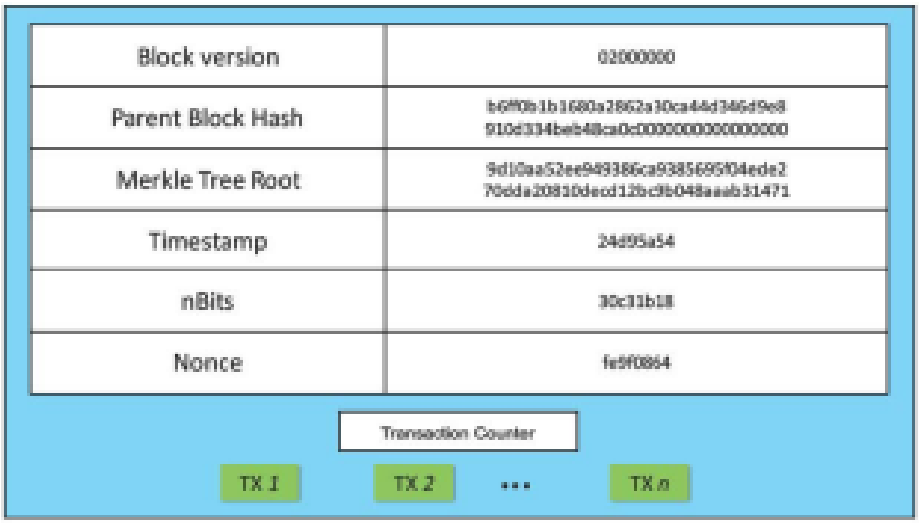


Figure 2: The contents of a Blockchain block [46].

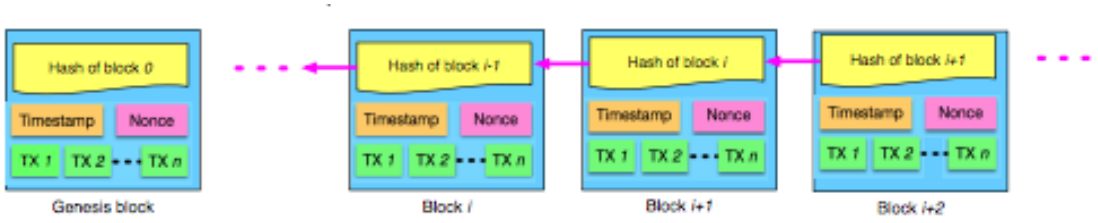


Figure 3: Architectural sketch of a Blockchain [46].

Some key characteristics of the Blockchain technology are:

• Decentralization: In conventional centralized data systems, each data transaction needs to be validated through a central trusted agency (manually), resulting in high cost and performance bottlenecks. Differently, a transaction in the Blockchain network is open to anyone to join by participating in the network consensus. In most cases, this means having the right hardware system to run the consensus node software. It means that transactions can be authenticated through a decentralized process easily, therefore, facilitating a peer-to-peer (P2P) exchange between two parties without the need for a central entity. This can significantly reduce the server costs (including the development cost and the operation cost) for most applications and also mitigate the performance bottlenecks inherent in central servers.

• Persistency: Each node that runs on a Blockchain network always has the recently updated data and since these nodes are distributed across different locations, it is hard to tamper or change the data across all nodes through breaking the consensus. This means that the data are immutable and hard to change once recorded on the chain. Additionally, each broadcasted block needs to be validated by other nodes and transactions would be checked for consistency, meaning that any falsification can be detected easily on the network.

• Anonymity. It is possible to conceal the information of users in a Blockchain network such that two or more users can transact without revealing they identify or other information to the public. This kind of privacy is important is IoT applications where the need for privacy is required for communication and data exchange without revealing the information of the devices. Also, since no private information is stored in central storage, stealing, exposing or hacking of personal information is impossible.

• Transparency. Since each transaction that is validated and recorded on the Blockchain has a timestamp, anyone can easily access the transaction time and other public information about the transaction. In the Bitcoin network, for example, each transaction can be traced to previous transactions iteratively by querying the transaction history. This improves the traceability and the transparency of the data stored in the Blockchain [45].

3.2 Different types of Blockchain

Blockchain networks can be classified based on its accessibility and its consensus or protocol. The accessibility determines if the network can be accessed publicly by anyone with the required

hardware and software resources or privately. The consensus serves as the governance system where rules are set to guides all parties involved and how blocks are formed [44].

3.2.1 Blockchain Types Based on Accessibility

Blockchain networks can be grouped based on the access restrictions which determine if they can be accessed publicly or privately by several individuals or groups. Depending on the restriction, a network can be grouped as permissioned (private) and permissionless (public) [46].

3.2.1.1 Private or Permissioned Blockchain: This is a Blockchain network that requires some form of approval from a controlling entity to grant access to participation in the network. Normally, the write permissions are kept controlled by this central organization while the read permission is fully open to the public or partially restricted. There is an argument if such networks should or should not be considered a Blockchain as the data structure is controlled centrally like in traditional databases.

This type of Blockchain is mostly used by organizations like banks and in supply change management by some groups of organizations involved in the same value chain where some sensitive data are required to private. Because there is limited access and availability is just restricted to a group of individuals, only a few people are needed to be involved in its consensus and that makes them very scalable, fast and more energy-efficient as compared to public Blockchains. Examples of such Blockchain are Corda and R3, few of the properties between the types are compared in table 1 below.

3.2.1.2 Public or Permissionless Blockchain:

A public or permissionless Blockchain network is fully open and available for any interested participant to join. The participant can join in reading or writing data from/to the network and verify transactions through the forming of blocks by running a node. This means that the protocol and codebase are open and available and therefore can be modified or extended by any party interested without any permission from a central body. There are dozens of such Blockchain but Bitcoin and Ethereum remain the most popular.

Also, there is Consortium Blockchain which properties and accessibility are in-between that of a private and a public Blockchain. The properties are compared in the table below.

Property	Public Blockchain	Private Blockchain
Access	Open both Read/Write	Permissioned Read and/or Write
Speed	Slower	Faster
Security	Proof of Work Proof of Stake Other Consensus mechanisms	Pre-approved participants
Identity	Anonymous Pseudonymous	Know identities
Asset (Token)	Native assets	Any asset

a)

Properties	Public Blockchain	Consortium Blockchain	Private Blockchain
Consensus determiners	All nodes/miners	Selected sets nodes	One organization
Read permission	Public	Could be public or restricted	Could be public or restricted
Immutability	Nearly impossible to tamper	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralized	No	Partial	Yes
Consensus process	Permissionless	Permissioned	Permissioned

Table 1: a) Properties of Public and Private Blockchain b) Comparing Public, Private and Consortium Blockchain

3.2.2 Blockchain Consensus

According to [47], the concept used by Blockchain technology to reach consensus without any central trust dependent was adopted from the transformation of the Byzantine General (BG) problem. This problem was from a challenge once faced within a group of distributed Generals on

how to agree and communicate if and when to attack on a battlefield. Considering that there might be a traitor with a different agenda different from that of the other Generals.

The same applies to Blockchain, where a distributed group of nodes most agree with each other without a controlling central node to make decisions. This is achieved through a decentralized autonomous governance system known as consensus that determines the rules in the form of an algorithm. The two most popular of such consensuses are Proof of Work (PoW) and Proof of Stakes (PoS) [46].

3.2.2.1 Proof of Work

In PoW consensus, the network nodes run sets of complicated computational processes for the authentication of transactions and formation of blocks and it was first used in Bitcoin Blockchain [45]. Each network node is constantly scanning for a value which when hashed with a cryptographic function like the SHA-256, the hash begins with a certain number of zero bits known as the nonce that determines the average amount of hashing (work) to be done by the computing node. The nodes that calculate this hash are known as the miners and they mine using hardware systems like graphic cards or Application Specific Integrated Circuit (ASIC). In a decentralized network, valid blocks are formed when multiple nodes find the suitable nonce and the new block is merged chronically with previous blocks. Care has to be taken for the case where more than one block is formed simultaneously which might result in forking of the Blockchain into multiples branches [46].

The PoW consensus involves computational calculation for its processes that is time and resource consuming, an incentive monetary mechanism is used to pay the node miners in form of the network tokens or coins known as cryptocurrency [45]. These cryptocurrencies can be converted to fiat currency through an exchange. PoW is very energy-intensive, the miner hardware has to run continuously and consumes a lot of energy. The fact that more than one node can find a new block at the same time with just one merged with previous blocks create a wastage in energy which has resulted in the design and use of more energy-efficient consensus or the use of the PoW protocol in combination to other side application like high-intensive graphic rendering [46].

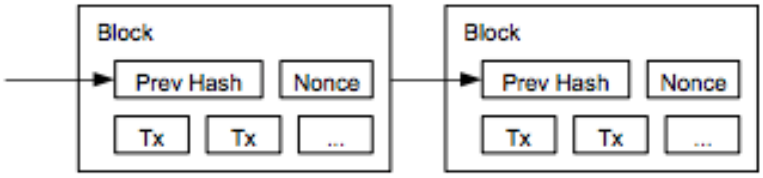


Figure 4: Formation and content of a block [45].

3.2.2.2 Proof of Stakes:

PoS consensus was designed as an alternative to PoW, instead of using high energy computational hardware as nodes for consensus, a certain amount of the network's cryptocurrency (token) is deposited on a node's wallet and locked up. The set of nodes with this amount of token locked up can join and participate in the network consensus process. Two major issues with the PoS consensus are security and decentralization because in most cases, the amount of token needed are high that only a few people can afford it. This has raised questions on the decentralization properties of the PoS consensus but some solutions were suggested in [48,49]. Since only a few users can afford the high cost to buy and lock-up the token needed to run a node, the network tends to become centralized to only these few rich thereby exposing the network so some security risk. The most vulnerable security risk is an attack from the (centralized) node owner, although it can be argued that they have little incentive to attack a network they have heavily invested interest. Because there are still high possibilities for the node owners to coordinate an attack on the network, a combination of PoW and PoS consensus like the DPoS (Delegated Proof of Stake) have been designed to improve the network security against attacks and are mostly used in place of PoS.

3.3 Applications of Blockchain

Blockchain application keeps expanding across different fields, it has been applied to various economic sectors such as Governance, Identification, Finance, Supply Chain management, Information and Technology, and so many others. For this chapter, its application in Finance and Supply Chain will be considered alone since these have direct implications in anti-counterfeit.

3.3.1 Application in Finance:

Bitcoin, which is the first public Blockchain network was built as a trustless peer-to-peer payment gateway [45], after that, Blockchain has gained significant popularity and been applied in other financial areas. In the traditional financial sector, most financial services fundamentally facilitate the trusted exchange of value between multiple parties and brokering of such trust involves enormous responsibilities with a significant amount of risk that makes the industry reliant on very costly intermediaries and error-prone reconciliation system resulting from manual processes [50]. Because the Blockchain offers a real-time unified synchronized distributed data ledger system that is hard or impossible to modify without detection and at the same time is transparent to all parties involved, it can improve the efficiency of most of these financial services. Fives notable functions of the financial services currently been transformed by the Blockchain technology are highlighted by [50] to be:

a) Trade Finance
b) Commercial Insurance
c) Regulatory Compliance
d) Claims Processing
e) B2B [write full meaning] Contract Processing

To evaluate the core processes of a financial system and determine if Blockchain is rightly applicable, [51], suggested four key points and questions below as an evaluation criterion to determine if Blockchain will be rightly applicable.

1. Is the process rule-based: The more standardized a process is, the more it is suited for the application of Blockchain using automated contracts (smart contracts).
2. Does the process require manual intervention: The more the need for reconciliation through human intervention, the greater the opportunity for Blockchain to be applied.
3. Is the data fragmented, with multiple truth versions in existence: Blockchain offers a single source of truth synchronized data accessible to all stakeholders involved.
4. How many stakeholders are involved: When there are so many stakeholders involved, the Blockchain can offer value through its distributed and transparent data record which is available to all in real-time.

However, as the Blockchain technology evolves and more businesses adopt it for their financial services, these future trends below will become more prominent over time as noted in [51].

a) Adoption of a hybrid of private and public Blockchain by businesses

b) Connecting existing financial systems like Enterprise Resource Planning (ERP) system with the Blockchain

c) The regulatory environment towards the technology will be flux.

3.3.2 Application in Supply Chain:

Almost the same rules as in section 3.3.1 apply in the supply chain when evaluating areas where the application of Blockchain is suitable. Consider the complete lifecycle of a product from production to consumption for example and the different stakeholders involved, Blockchain seems to be a good match to improve the complex processes involved among these stakeholders. According to [50], a report from Microsoft found that out of 408 organizations from 64 different countries were facing consistent supply chain challenges, 69% of this do not have full visibility into its supply chain system, whereas 65% experienced at least one disruption in its supply chain system, 41% still relies on an excel spreadsheet to keep track of its supply chain. These issues do not just result in a waste of time alone but also lose money and resources. It is why big companies like Maersk and IBM have established a venture together to develop a global Blockchain-based system for digitizing trade workflow and a shipment end-to-end tracking in the logistics sector [52]. The supply chain management is of great interest because most counterfeited products are introduced and circulated through the supply chain [1].

[50] also explored how Blockchain is transforming the complex supply chain in the following areas:

1) Provenance attestations: Consumers are always concerned with how and where the products are produced. Using Blockchain's immutable distributed ledger, the tracing of product inputs and attestation of the techniques used in production can easily be assessed and tracked by all parties involved in the supply chain.

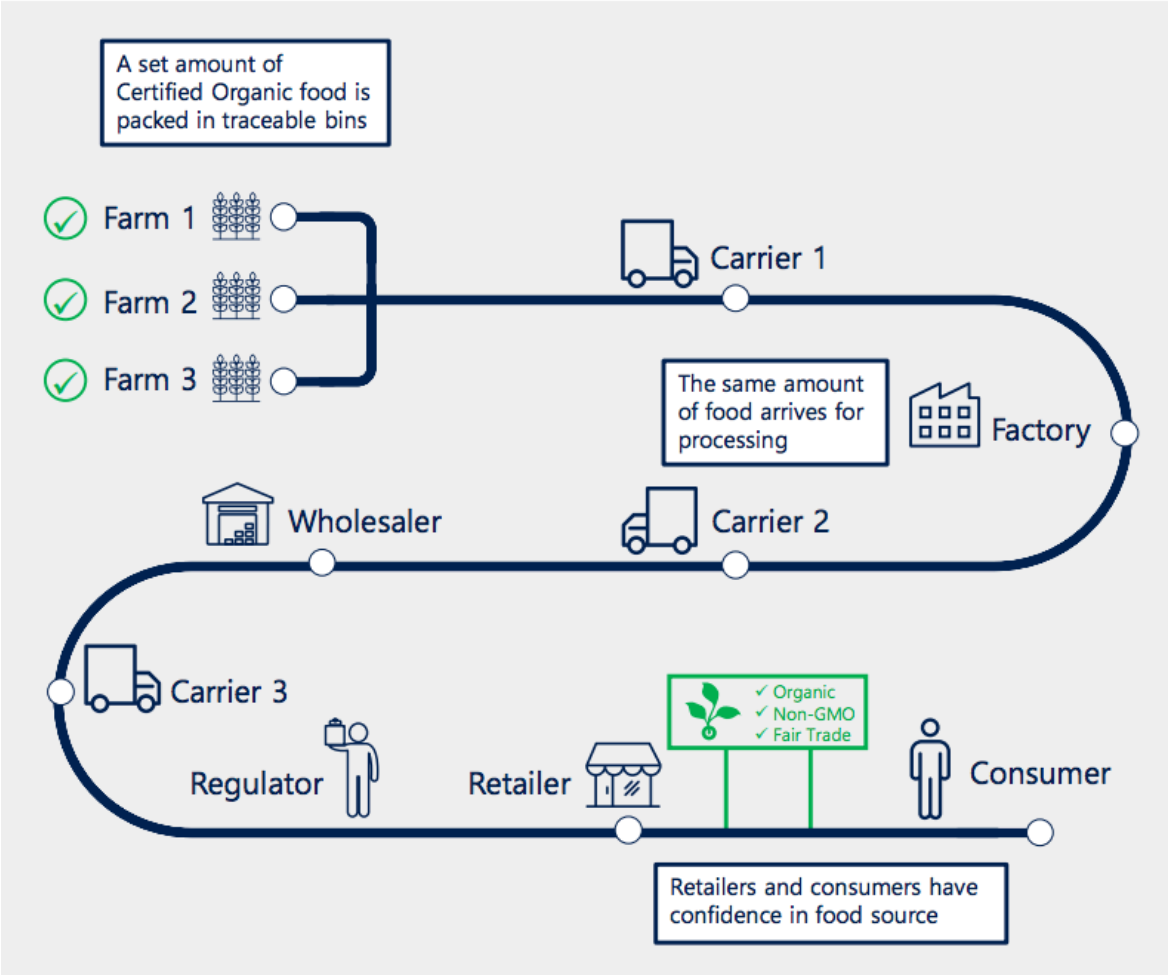


Figure 5: Illustration of Blockchain use in product provenance or attestation [50].

2) Environmental monitoring: For safety and regulation purposes, certain environmental conditions like temperature and humidity must be met for certain products, maintaining these qualities and conditions requires ensuring that all parties in a supply chain and transportation to manage the product under the right condition based on standards.

Recent Blockchain integration with IoT using devices like RFIC, NFC sensors, and other monitoring devices have been applied in this area so that all parties can monitor a product requirement and condition easily. It also means that mistakes can be easily identified, tracked and remedied in real-time.

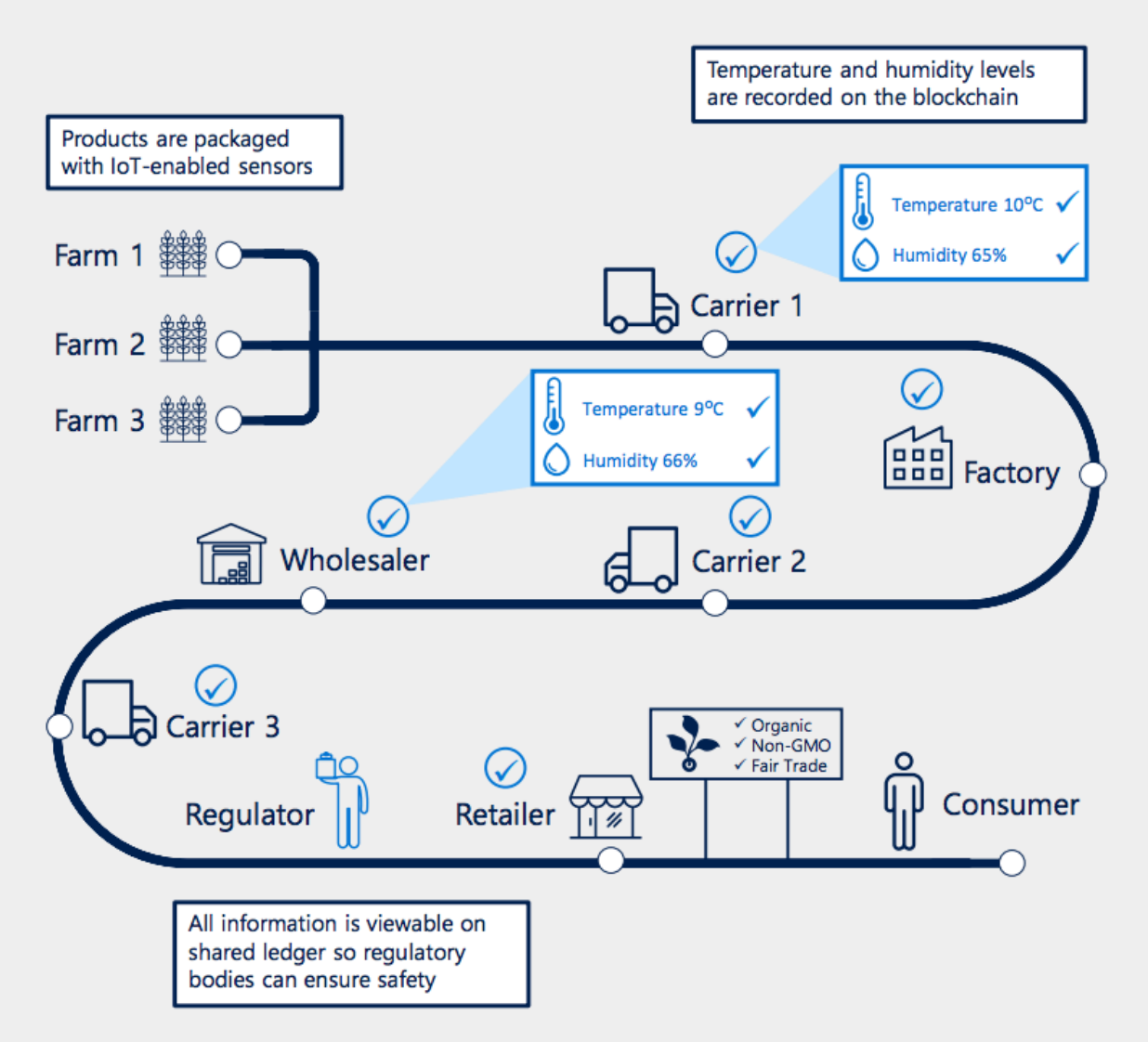


Figure 6: Illustration of Blockchain integrated with IoT for product real-time monitoring [50].

3) Dispute resolution: Things do not always go as planned in a traditional complex supply chain, disputes usually occur and it is imminent that there are always treated and settles as quickly and transparent as possible. When such disputes occur which normally result in fine payment by the defaulting stakeholder, it is always error-prone and costly to identify. Blockchain can enhance the process of resolution a lot and make dispute settlement faster and more transparent.

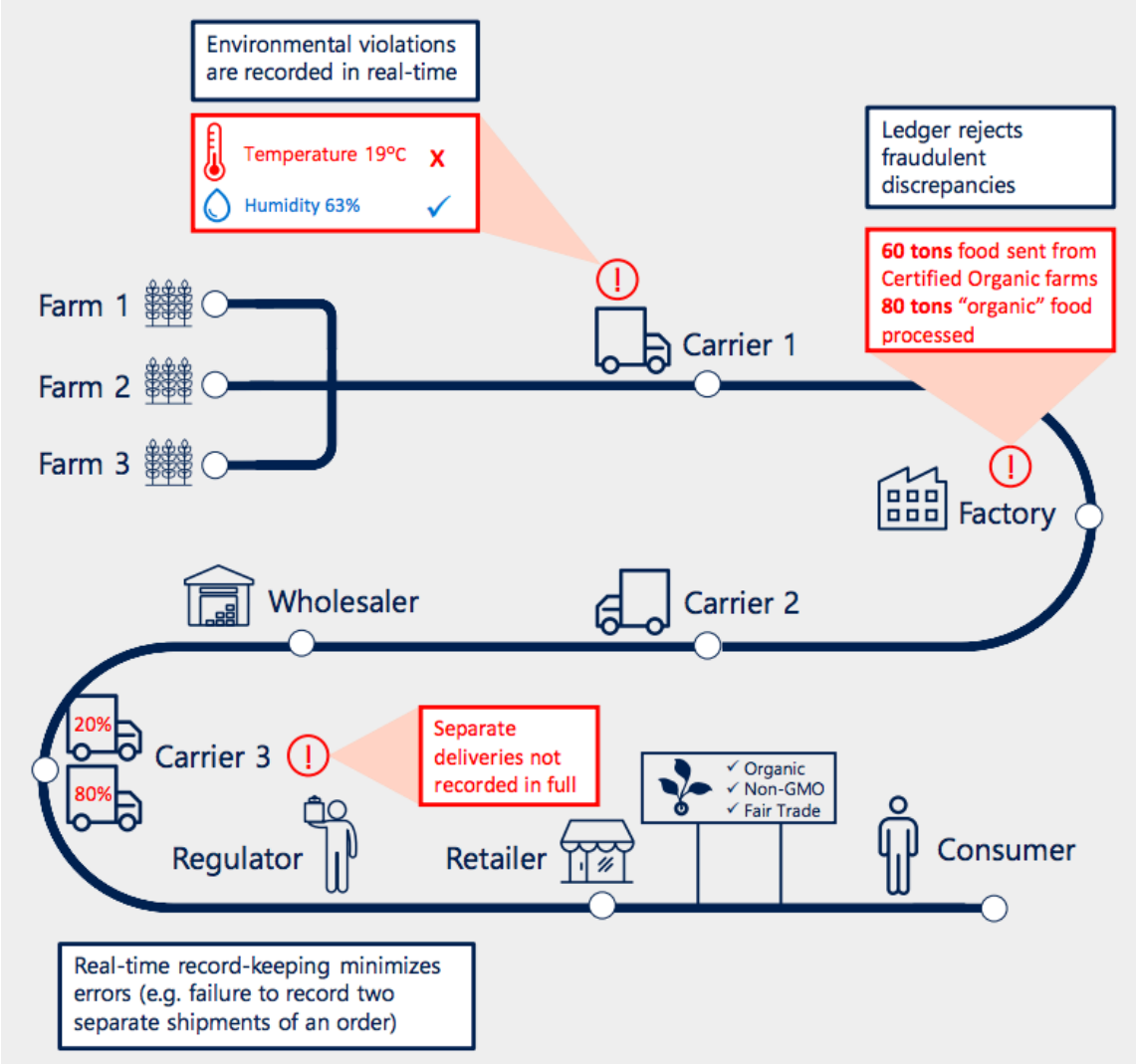


Figure 7: Illustration of Blockchain use in supply chain dispute resolution [50].

All these applications area benefits all stakeholders involved, both the supplier, retailer and consumer that participate in product production, distribution and consumption.

[53] considered three different uses case such as product tracking and traceability for example in drugs and medicine, purchasing platform like in the automotive value chain, for sourcing the different raw materials and know your suppliers (KYS) for identification, verification, and endorsement of all stakeholders involved in a business.

3.4 Current Challenges with Blockchain:

Blockchain still has a lot of challenges preventing its application in different businesses or sectors. Just like the internet or any other new technology, these challenges will be solved as the technology matures over time.

The major setbacks preventing the application of Blockchain in major businesses is lack of awareness or understanding of the technology and where its application is suitable [54]. This is because the technology involves the understanding of multiple disciplines across finance, distributed systems, communication engineering, economics, etc. Also, there is the question of balance between initial set-up cost and efficiency of integrating Blockchain within certain business sectors. This cost is quite high when compared to existing systems but exploring different business models has helped to offset this initial cost.

However, the two major technical challenges with regards to integrating with IoT that will be considered in this section are the high energy used for Blockchain consensus and scalability of the application built on the Blockchain.

3.4.1 High Energy Demand in Blockchain:

Depending on the consensus used by a Blockchain for its transaction authentication, the energy requirement might be high and becomes a challenge as the network grows over time. Section 3.2.2 covered the two major consensuses and since the PoW requires hardware for the computation of hash by the miner, it means that more hardware with higher computational capability is required as the network grows over time and the hash computation becomes more difficult. This makes PoW consensus very energy-intensive and very challenging to sustain over time. The energy consumed by just mining bitcoin which runs on PoW consensus has grown exponentially and is speculated by some that it will consume all the electricity produced in the world by 2020 if the power production remains unchanged [55]. Although this speculation seems to be very overestimated, it is still very clear that the energy consumed by Bitcoin has increased over time as shown in figure 8 below which have also made the carbon footprint far higher and will continue this trend if nothing is done to improve the consensus process.

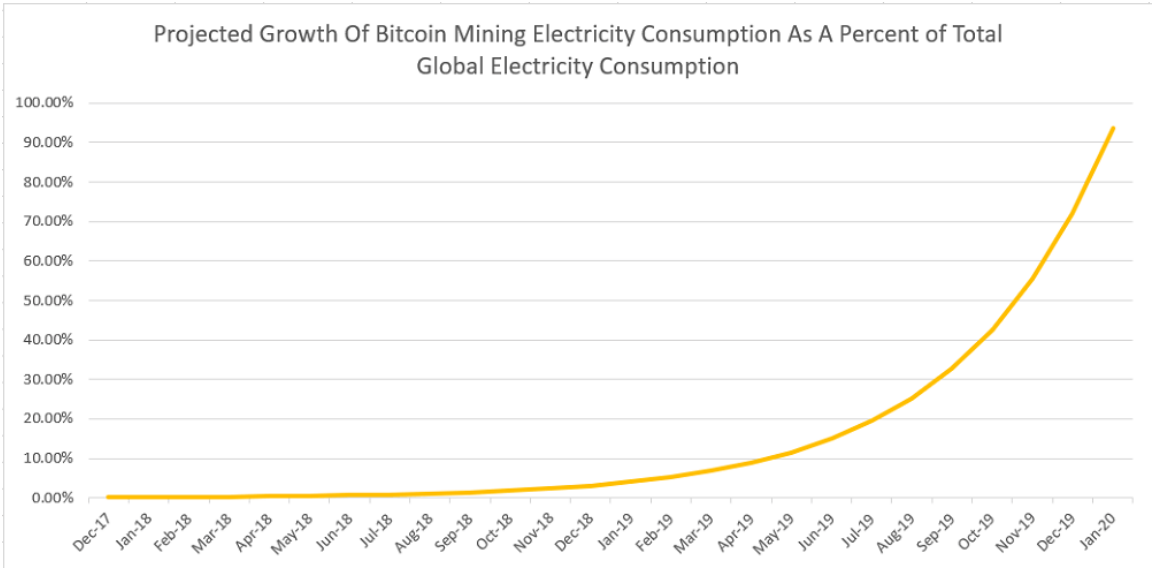


Figure 8: The growth rate in bitcoin mining energy consumption [55].

3.4.2 Scalability of Blockchain:

It mostly takes within 1 – 10 mins to form and confirm a block in public Blockchains [56], Bitcoin, for example, confirms just 7 transactions alone every second, this is so small when compared for instance with Visa payment gateway system which handles about 24,000 transactions per second [57]. Also, the restricted block size of about 1MB for some Blockchain means that only limited transaction can be confirmed per block and since miners are more incentivize to accept transactions which have bigger transaction fees, it means that most other smaller transaction with small transaction fees are dropped and rejected and therefore takes more time to be confirmed. The result of these actions from miners makes Blockchain applications in certain fields like IoT where a small amount of data needs to be confirmed fast with the littlest fees very challenging. Another key issue is in scaling applications running on a Blockchain, because all the data are stored and maintained by all nodes which maintain the network, means that any new node that wishes to join the network must download all the previous block data to be consistence with the other nodes. Bitcoin, for example, has a total data size of about 100GB which makes it very hard for new nodes to join the network and therefore makes the network hard to scale over time [56].

Notwithstanding these challenges, there are feasible solutions and improvements in researches on how to solve these issues which makes the future convincing for the technology.

CHAPTER FOUR: POWER CONSIDERATION DURING INTEGRATION

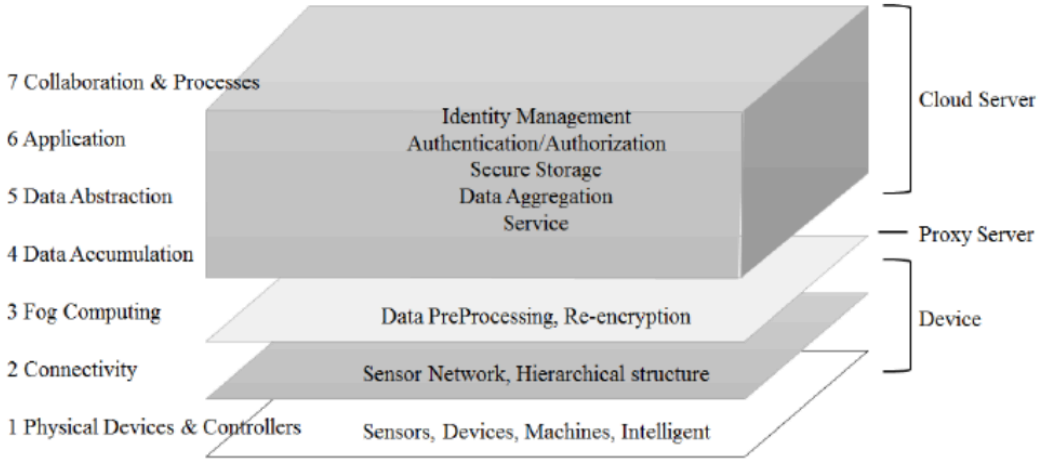
IoT systems on its own alone, have high power requirements resulting not just from the IoT devices itself, but the gateway devices and the networking devices interconnecting them. The gateway device connects the IoT device with other IoT devices or the storage or processing device using networking devices which are either wired or wireless network devices [9]. Also, apart from the energy requirement for operating IoT devices, there is high energy need for the manufacturing and production of these devices known by the term, Emergy [58], these are very high for smart devices which incorporate integrated circuits (IC) and microcontrollers in a very small surface area. Though the recent technological research breakthroughs have drastically reduced the energy required for manufacturing these devices, it is still worth considering when designing and implementing IoT solutions or applications.

4.1 Energy requirement in IoT network:

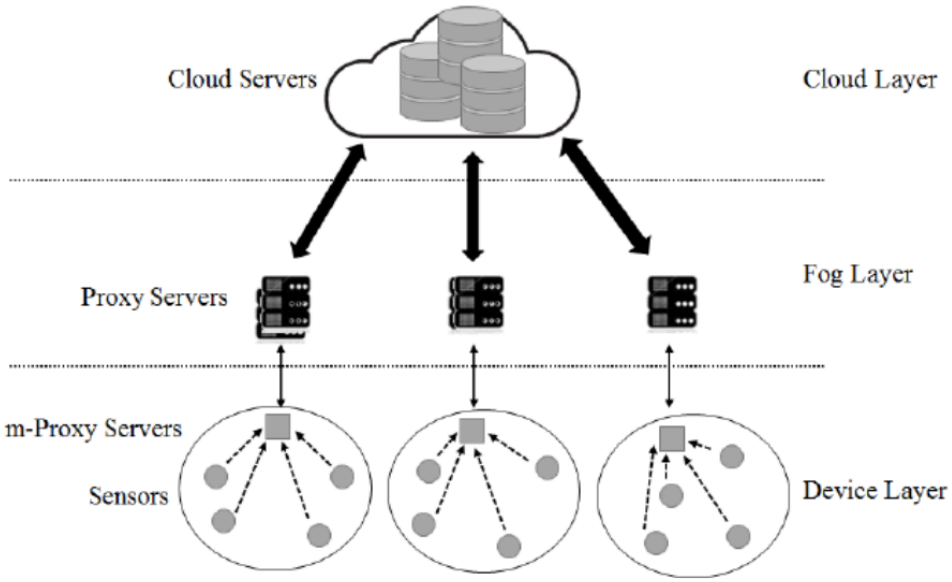
Because IoT network has a high energy requirement, for them to be sustainable, the right architecture, communication protocols, node devices, network devices, and software implementation must be used. This is very important, especially when integrating IoT with Blockchain which from chapter 3 is very energy-intensive on its own. For example, from [59], in an IoT network providing the same access rate and traffic volume, using a wireless network will consume 10 times more energy compared to a wired network. But because most IoT applications do not suit a wired network system leaves the wireless network as the only viable option. This means that for such an application, the high energy need for a wireless network system must be considered right from the design.

Research improvements in network device components like in Complementary Metal Oxide Semiconductor (CMOS) and optical technologies have led to great improvement in power efficiency and management, resulting in less power consumption in these devices [59] and such improvement is expected to continue in future generations of these network equipment. The same applies to the power consumption based on access rate for access network technology like DSL, HFC, PON, FTTN, PtP, WiMAX and UMTS. This same access network technology is used in an IoT network integrated with Blockchain. Also, different researches have explored other different energy-efficient architectures both in the IoT hardware level and the way the hardware is operated. In the hardware level, because of the limited computing and storage capability inherent in the

sensing or data collection nodes of most IoT devices like NFC and RFID tags, Fog and Mist computing architectures have been used in different application cases to supplement the computing ability in an energy-efficient way. In [60], the architectural design of fog computing network using sensors networks was properly covered and figure 9 below shows the role-based hierarchy and system architectural representation of the proposed fog architecture.



a)



b)

Figure 9: a) Proposed role-based layer architecture b) Proposed system architecture [60].

There are other research works too which have tried to propose an energy-efficient architecture for IoT like in [61] and the same can be implemented when IoT is integrated with Blockchain. A layered architecture consisting of a sensing and control layer (SCL), information processing layer (IPL), and application layer (AL) used in [61] is shown in figure 10. The proposed architecture uses layers of nodes like, 'energy-saving gateway nodes (eGNs)' and an energy-efficient base station (eNode)' to achieve great reduction in the amount of energy required at the SCL while at the IPL layer, energy saving is achieved using a proposed 'energy-efficient resource allocator (eRA)'. This is very important for a distributed IoT network integrated with Blockchain networks where the IoT nodes can also serve as the Blockchain data processing and storage node.

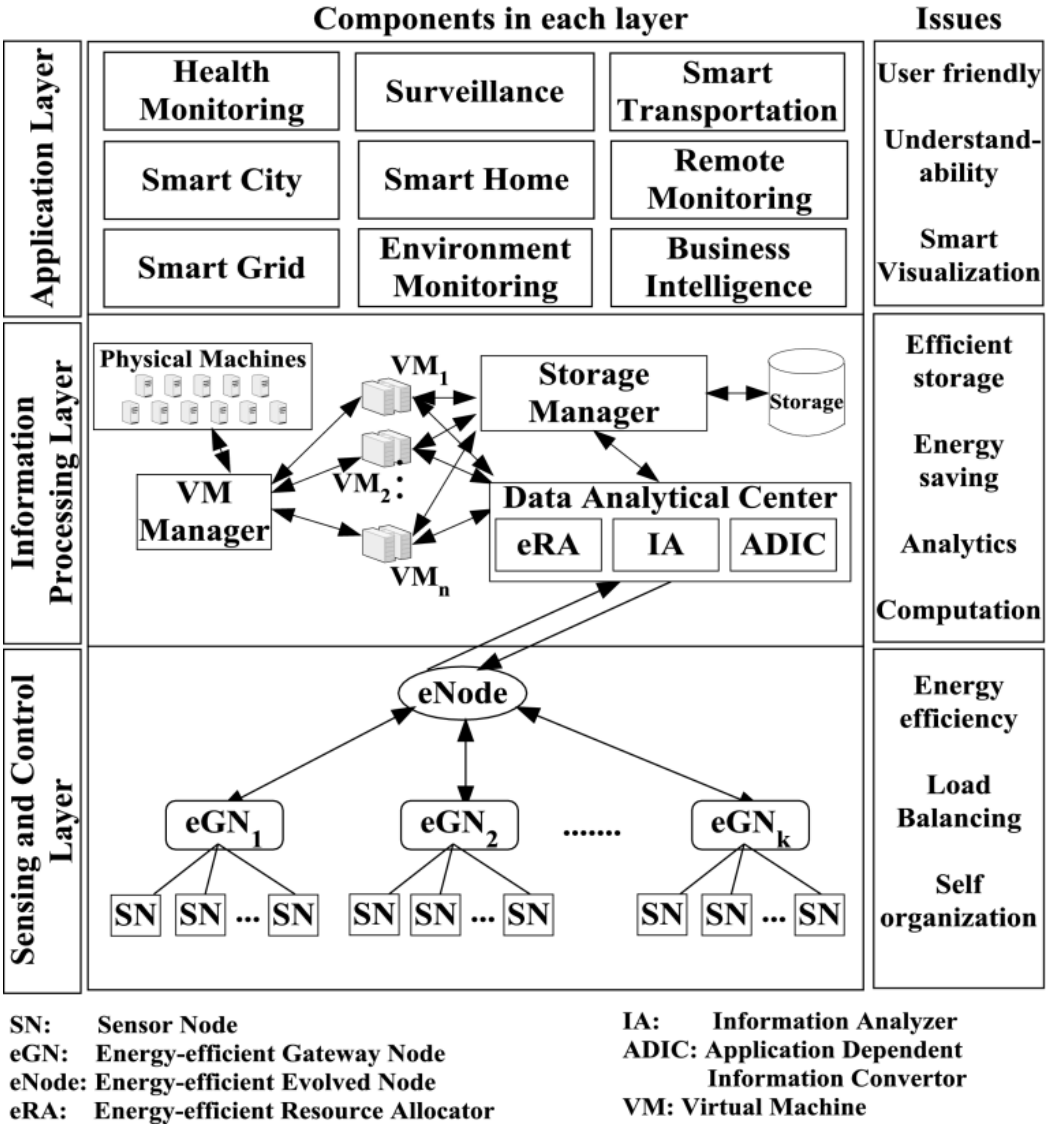


Figure 10: Proposed energy-efficient architecture for IoT network [61]

4.2 Energy resulting from different actions:

Both the IoT network and Blockchain network do have some similarities in their data processing and storage abilities as both are distributed. As the number of connected devices over time increases, the energy need for these devices and the network of devices will increase as well. Many of the energy-consuming actions in existing IoT systems results from data centers and Radio Access Network (RAN), Machine – to – Machine (M2M) communications, embodied energy in manufacturing the devices and energy involved in proper disposal and replacement of obsolescence digital technologies devices. They will be explained briefly below:

4.2.1 From data centers and Radio Access Network (RAN):

Data centers have always been thought to be the major IoT consumer of electricity for so long. It is where all the high energy devices for data processing, storage, networking and cooling systems of the data devices reside. From [62], this energy has been reduced with the advancement in the design and manufacturing of these devices and with recent operators choosing cold areas for their data center sites to reduce the energy needed for cooling.

Also, from [62] report, wireless access technologies such as wifi and cellular (4G LTE) technologies that dominate the method of accessing cloud-based applications consumes more energy than data centers with a recorded 460% increase of 9.2TWh energy consumed in 2012 to 43TWh in 2015. This corresponds also to an increase in carbon footprint from 6 megatonnes to 30 megatonnes of co_2 from 2012 to 2015, an equivalent of adding 4.9 million cars to the road. 90% of this energy was consumed by wireless access network systems whereas the remaining 9% was by data centers. [63] captured a graph of the carbon footprint resulting from factors that consume energy and the projection of this footprint till 2020 for mobile communication systems which logically should be a major framework for IoT and Blockchain integration as well.

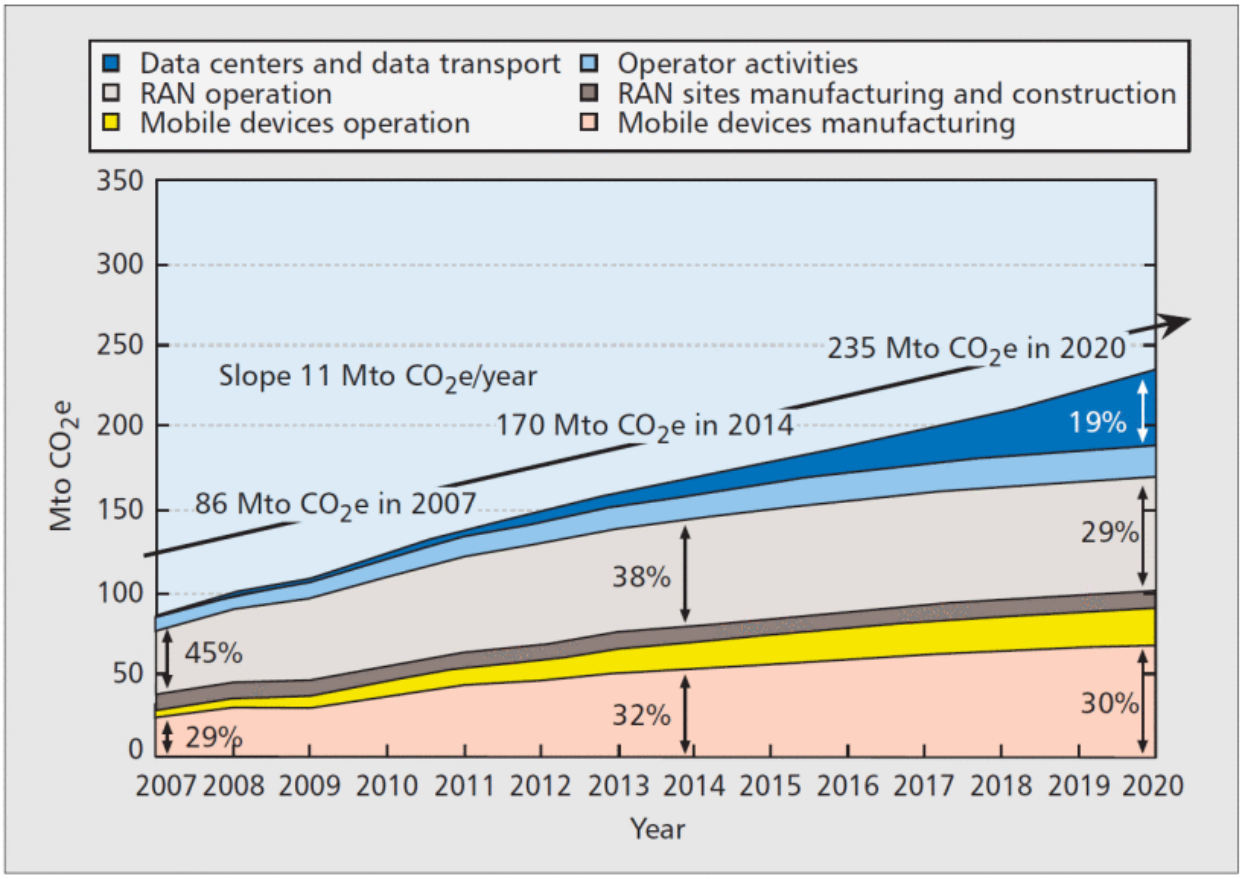


Figure 11: The global carbon footprint for mobile communication projected until 2020 [61]

This will keep increasing as people spend more time online, accessing data, applications, pictures and mostly streaming videos. More energy will be consumed by the access network and data center devices. Also, the increase can be attributed to end-user devices like smartphones, tablets prices becoming cheaper over time and as more IoT devices are connected, the data and applications accessed with these devices increase over time.

4.2.2 Machine-to-machine communication:

Machine-to-machine (M2M) communication relates to the transmission of data across all internet-connected things, remote updates of the software for personal devices and back-up of data and other digital content to the cloud [58]. M2M communications have to be seen as a rapid type of developing technology for huge networks of wireless devices independent of a human intervention [64]. This means that as the number of devices connected to the internet keeps increasing, there

will be high energy demand considering that about 50 billion devices are projected to be connected by 2020 and M2M communication will account for 45% of internet traffic by 2022 [58].

For most M2M communication (connected mostly through wireless communication), the majority of the devices are operated using a battery that is not rechargeable [65]. This means that low energy consumption and the need for an energy-efficient design becomes more imperative for applications like anti-counterfeit solutions where IoT is integrated with Blockchain. One such design methods as reported in [65] is 'clustering'. It is a technique that involves a network of devices randomly selecting a cluster head (CH) and then all pooling they data together and transmitting to the core or transporting network through a base station as opposed to doing so individually. This method reduces energy consumption in communication and the different algorithms applicable for using clustering in a wireless sensor network (WSN) are shown in table 2 below. It is also worth noting that the distributed nature of Blockchain will make communication between different M2M (IoT) communication protocols easily possible.

Clustering algorithm	Intra cluster	Inter cluster	CH selection	CH reselection	Propagation model
EEHC	M-hop	M-hop	Random	No	No
HEED	1-hop	M-hop	Random	Yes	No
LEACH	1-hop	Direct	Random	Yes	SP
Our Design	1-hop	Direct	Cost	Yes	LP & SP

Table 2: Comparing different clustering algorithms for WSNs

4.2.3 Embodied energy:

Although not so popular in the research community, the embodied energy was reported in [58] as one of the factors to consider when implementing IoT application. Manufacturing of microchips, integrated circuits (ICs) and microcontrollers which are very small in size, requires far more energy when compared with other electronics like television, desktop personal computer (PC) or refrigerators. Since IoT devices consist mainly of these components, necessary care must be taken when manufacturing them to reduce energy consumption and carbon footprint. This can be achieved by using renewal energy sources in manufacturing, making the devices durable so that the lifecycle is very long and therefore reducing the lifecycle energy requirement of the devices to upset the energy need in its operation.

4.2.4 Obsolescence digital technology:

Perhaps the most factor that contributes to high energy consumption according to [58] is the replacement of old IoT devices over time with new ones as a result of rapid evolvement in information and communication technologies (ICT). This means that the enormous energy used to manufacture the old devices are useless after these devices are disposed within a short time. Also, most times, these devices are very hard to recycle or properly disposed which can have great environmental and energy impact.

4.3 Energy consideration when integrating IoT with Blockchain:

Some energy factors to consider when integrating IoT with Blockchain are:

1. The integration application
2. The Blockchain generation and consensus
3. The IoT hardware and architecture

No 3 was covered in section 4.1 already whereas 1 and 2 will be considered in this section.

4.3.1 Considering Application:

Different applications have been and can be designed and implemented through IoT and Blockchain integration. These applications have been applied in the art industry to verify and authentic (expensive) art artifacts and other art materials and record their ownership and transfer between owners during auctions. In the food industries, there are applications to verify and authenticate food sources and origin, crop growth and growth conditions like humidity,

temperature, fertilization and pesticide conditions have also been tracked with IoT and recorded on the Blockchain. The food production, storage, and distribution can be tracked, and the whole food lifecycle can be tracked and authenticated to know when is unhealthy to consume [66].

The same also applies to health, pharmaceutical, and apparel industries, for the apparel industry, to verify leather authenticity for example and so many other industries. With the increasing number of fake and counterfeit products infiltrating theses industries, IoT plus Blockchain applications can be a viable solution when implemented properly with minimal energy consumption.

Therefore, a good design application should consume a minimal amount of energy possible and still align well with the other needed application specification.

Also, application need determines the least tolerable latency which as well determines the suitable applicable architecture, if edge, cloud, fog or mist architecture best fits the application requirements.

4.3.2 Considering Blockchain generation and consensus:

Another major energy factor to consider is the choice of Blockchain generation and consensus to use when integrating with IoT. This has already been introduced in chapter 3 but the energy requirement of the different popular Blockchain which can be integrated with IoT will be expanded here. The two major properties that determine the energy need of a Blockchain considered here are 'the generation of the Blockchain' and 'its consensus or algorithm'.

a) Blockchain generations: Since Bitcoin emergence, Blockchain technology has progressed through three different generations. The first generation was that of Bitcoin which uses distributed data ledger networks for data storage of transactions. In this generation, the time for block generation is high, therefore they are not fast and scalable nor suitable for application where speed and scalability are needed. The consensus mostly used in this generation is PoW and it consumes a large amount of energy in computing cryptographic hash which has to be solved before new blocks are formed. It was also hard to use this generation in other applications because it is not turing complete (meaning that it cannot run nor execute a set of computer instructions in the form of code). A second generation Blockchain was developed.

The second generation is turing complete, meaning that sets of computer instructions can be executed on the Blockchain network layer through a pooled distributed decentralized virtual machine platform running as network nodes. They execute these sets of codes in a form called the

‘smart contract’ [67]. The consensus used mostly in the second generation is ‘Proof of Stake', ‘Proof of Work' or a combination of the two. An example is Ethereum, the most popular second-generation Blockchain. It was the first to introduce smart contracts using a programming language similar to Javascript known as Solidity. However, the second generation is still not scalable in most application use cases and therefore have to depend on a layer two scaling solution and is the reason for the most recent generation, known as the third generation.

The third generation tries to solve the scalability and other bottlenecks in the first and second generation that restricts its application in IoT integration for example. An example is ‘Waltonchain’ Blockchain. In this generation, since blocks are produced faster at every 30 seconds on average, it can process more transactions needed in applications such as integration with IoT for anti-counterfeits as applied in Waltonchain [68].

Most third-generation Blockchain uses the same consensus as the second generation but the hardware used for its PoW are advanced ASIC hardware that uses very low energy.

b) Blockchain consensus and algorithm: The consensus determines how transactions are authenticated and new blocks are formed. The two popular used ones are PoW and PoS or a combination of the two with each having its pros and cons. The PoW is more secure as it uses distributed and decentralized hardware systems that solve mathematical hash. But this means that high energy-intensive hardware is required once the network, hash rate, and difficulty grow over time. There are different algorithms used for PoW hash, an example is SHA-256, Scrypt, and X11 and each different degree of energy need. So, all these need to be considered depending on the application.

The PoS authenticates transactions by selecting random groups of stakeholders that have a high share in the form of the network currency (token). Although this consumes less energy, it is prone to attacks because it is less decentralized and these major stakeholders can decide to exploit the network against others. Since it is less decentralized, it can also be exploited more easily by an external attacker.

CHAPTER FIVE: WAYS OF INTEGRATING IOT WITH BLOCKCHAIN FOR ANTI COUNTERFEIT PURPOSE

There are lots of interesting projects and teams working on integrating IoT with Blockchain for anti-counterfeit purposes, in fields such as food, medicine, art, apparel, retail, and other industries. In this thesis, the four selected projects are Linxens, Smartrac, Vechain, and Waltonchain which are either private and public projects and they are grouped into two classes depending on how the IoT is integrated with Blockchain as 'integration by a brand using a unique identifier' and 'integration throughout the product lifecycle'. How both are integrated are described next and compared to seek the energy need.

5.1 Integration by brands using a unique identifier (Linxens, Smartrac & Vechain):

Projects like Linxens, Smartrac, and Vechain, provide counterfeiting solutions using third-party IoT hardware like RFID, NFC and sensors integrated on top of its Blockchain or that of a third-party public Blockchain for brands or organizations to uses for their product identification and authentication. While Linxens and Smartrac use Ethereum Blockchain which is a public second-generation Blockchain as described in chapter 4, Vechain extended Ethereum Go GETH codebase to add its customized consensus. Vechain through its Blockchain integrates with its IoT devices to identify, collects and tracks data using APIs and can also run a set of computer instructions in the form of smart contracts when for example a certain event or alarm is triggered. An example of such an event could be registering the transfer of ownership for a product between users. By using Ethereum smart contract programming language, the other two projects add come automation capability to its integration so that some functions can be communicated and executed autonomously without human intervention.

Brands through these integration platforms can digitize, track and record the identity of its products, production, distribution, and consumption cycle transactions in such a way that the products are hard to clone or fake, stolen, lost or copied throughout the production, distribution and consumption channel. Consumers of these products, on the other hand, can easily confirm the product origin and that it is authentic and meets the stated standard before buying, therefore, preventing buying of counterfeits.

A simple example considered here is an anti-counterfeit solution developed by Linxens called dLoc, it uses a secured encrypted dLoc tag chip, NFC communication protocol, Blockchain, and a

web interfacing app to prevent the counterfeiting or forgery of documents like in banks, insurance, and other industrial sectors. [69] describes the solution in more details which involves tracking a document throughout its whole lifecycle right from issuance and the verification and authentication during transfer as shown in Figure 12. At first, the document's unique identifier is recorded using IoT plus Blockchain through a chip. During a document issuance, the tag chip identification (ID) is encrypted and recorded on the Blockchain so that the identity is immutable and hard (impossible) to fake, then this ID is used to authenticate the document by verifying that the chip has been issued by the rightful authority using the dLoc NFC enabled application through any of the three ways:

1. Using an online environment, the reader can communicate with the dLoc database system where the authentic ID of the chips is registered.
2. By comparing the digital signature of the chip ID and that of the ICN (Inventory Control Number) which have been digitally signed during pre-personalization in the Linxens production facilities and stored on the dLoc database.
3. In an offline situation using an NFC reader that is Secure Access Module (SAM) authenticated, signature stored on the dLoc database can be recalculated and compared with that stored on the tag chip to check if it is valid and rightfully issued.

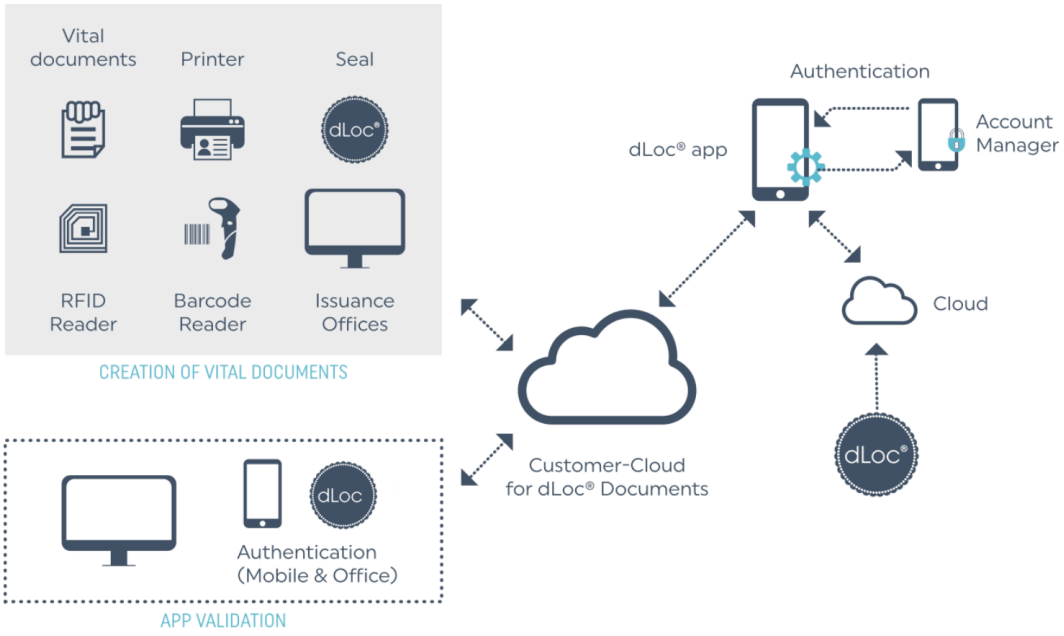


Figure 12: dLoc ecosystem [69].

There are also similar solutions like this which can be applied in food and drug authentication that operate closely to that of dLoc. In some of the solutions, however, apart from tracking the product ID in the chip, other data like manufacturing date, production, and transportation data like temperature and pressure in the case of foods like fish needs to be captured and stored in the Blockchain through an API for safety and standardization verification. These cases require sensors that require an external power source like batteries or in some rare cases passive RFID sensors that draws power from readers [Ref 31]. If a battery or other energy source is required, it means that the extra energy needs most be considered in the solution design and implementation to have a sustainable solution.

Advantages: This method of integration is very simple and seems to cost less to implement as existing IoT devices like RFID and NFC can be used to identify, track and record the product information to the Blockchain through an API. This means there is less energy requirement in the IoT part since they have been an improvement in the energy consumptions of such devices. Also, the Blockchain used is a second/third generation Blockchain with a consensus that requires less amount of energy.

Disadvantage: Since the integration is through APIs, there are security concerns that need to be considered when implementing this method. Also, since different protocols depending on third-party hardware can be used which are not compatible in most cases, the issue of having isolated solutions might result in higher overall cost for different implementation cases using different protocols. It might also result in some security vulnerability.

5.2 Integration throughout product lifecycle (Waltonchain):

Another integration method is throughout a product lifecycle used by the Waltonchain project through integrating its in-house native Blockchain IoT hardware with its Blockchain for anti-counterfeit purposes. Its core vision is to track and trace a product right from the product's raw material sourcing to production and all through the product's entire lifecycle. They have made great progress developing their ecosystem through their research and development and holds patents for developing different sets of native IoT hardware devices specifically for integration with Blockchain which can upload and read data automatically without human intervention instead of using APIs.

Also, they have made research progress in their Blockchain design to improve scalability and reduce energy through their parent chain – child chain architecture which uses a mix of 'PoW+PoS+PoL (Proof of Labour)' consensus [68]. This architectural design enables, in theory, an infinite number of child-chain across virtually all industries to be interfaced with the native parent chain for data circulation, security, exchange, query, and search, thereby creating an endless application use case. What this means is that all data across multiple industries can be securely stored on the industry or organization child-chain whereas the fingerprint of the data hashes is stored on the parent chain. This is shown in appendix B and C and it creates a platform for offline connection using RFID communication protocols meaning that virtually all data can be collected and tracked to form a data index and cluster [68]. Therefore, data and history of products can be traced securely without exposing an organization private information or identify. The ecosystem diagram is shown in Figure 13.

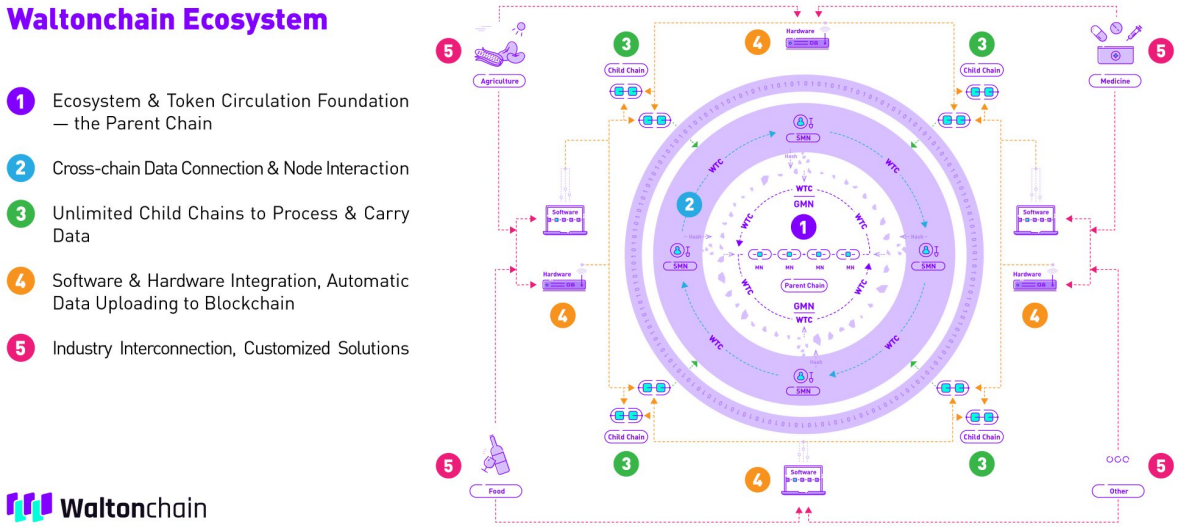


Figure 13: Waltonchain ecosystem diagram [71].

As shown in the ecosystem diagram, the in-depth integration of hardware with Blockchain, combined with the flexibility in its architecture means that Waltonchain's integration process can be applied across virtually all industries where customized traceability for any product is needed. Most of the hardware used for the integration are shown in appendix A, and they are mostly RFID based while other devices that are not can be connected using an encrypted data collector they developed shown in figure 14.

Figure 14: Encrypted data collector [68].

With this data collector, it means that existing IoT network nodes can be connected and its data read and uploaded directly to the Blockchain thereby solving the existing connection challenges like privacy and security while using the most minimal amount of energy as RFID IoT devices used in the ecosystem are specifically designed to be integrated directly with the Blockchain.

Chapter 4, stated the most energy-intensive part of Blockchain to be the consensus and hardware used for PoW, but recent development in ASICs for mining has improved over time and have reduced the energy consumption. A major part of Waltonchain ecosystem hardware is its ASIC miner for its customized consensus algorithm called KirinMiner. It consumes just 135W maximum power (that is 3.24kWh daily max) and hashes at an average hash rate of 400MH/s. This power (energy) is very small when compared with what most server hardware devices consume. It will be an interesting academic exercise to compare how this hash rate and power compare with other networks like Bitcoin that consumes annually about 22TWh [70] (Bitcoin have existed for over 10 years compared with Waltonchain which network is about 2 years).

Advantages: The major advantage of this integration method is that the data is incorruptible since it is uploaded automatically to the Blockchain. This means that the data is credible and authentic and can be accepted by the different parties involved. Also, having specific hardware devices for

the integration means that the energy consumption by these devices can be improved and reduced over time.

Disadvantage: The disadvantage that comes with this integration type is the complexity in implementation and the high initial cost that might be involved in switching from an old solution. Since most other IoT devices especially those used to trace products are passive RFID and those used for data collection like sensors consume little amount of energy which has kept reducing with research breakthrough, it leaves servers and data centers used for local and cloud processing and storage of the raw data as the major energy-intensive devices to be seriously considered when integrating Blockchain with IoT in either of the two methods above. Table 3 below summarizes a comparison of both integration methods.

SN	Property/Feature	Linxens, Smartrac & Vechain	Waltonchain
1	Set-up and cost	Easy and cheaper	More complex and expensive
2	Hardware Specific	No, general hardware	Yes, application-specific
3	Compatibility	Restricted	All protocol, Bluetooth, ZigBee
4	Application	Industry-specific	Across virtually all industries
5	Scalability	Low	Infinite child-chain
6	Consensus	More energy-intensive (POW)	Less energy-intensive (POW+POS+POL)

Table 3: Comparing the two integration methods

5.3 Proposed Ideal Integration Method

A perfect Blockchain and IoT integration solution that perfectly considers power consumption should consume the very minimal power while securely acquiring, storing and authenticating the origin and history of a product's data. This means that an appropriate balance should be achieved between securely acquiring and exchanging of the data and the energy demand. The three criteria used in this work to justify an ideal integration method are:

- **Blockchain Consensus:** If billions of things (products) end up being connected through a Blockchain that uses Proof-of-Work as consensus, the power need will be massively huge and hard to sustain as tremendous amount of daily transactions will be collected and processed. This raises the need for a very energy-efficient consensus system that utilizes PoW (because of its security) and PoS (because of its energy-efficiency) or any other consensus or combinations of a sustainable consensus system (for efficiency).

- **Data Originality:** If a product's authenticity depends on the data collected about the product, then there is a need to collect this data right from the origin automatically such that there are little chances for data corruption posed by human intervention. Therefore, a good integration method must consider and achieve true data acquisition right from the source and using a minimal amount of energy.
- **Data Interconnection:** Data acquired and used for anti-counterfeit purposes should also be able to be interconnected with other industrial data and used across other industries and purposes like in the insurance sector for product warranty claim. This will make the data more valuable and serve as a better value proposition for integration with Blockchain.

Comparing the two integrations methods covered in this thesis against these three criteria shows Waltonchain method of integration as a more preferable integration method as it met almost all the criteria as examined below:

- **Blockchain Consensus:** While other integration projects integrate on top of Ethereum Blockchain which uses solely a PoW consensus or its own natives' Blockchain that uses PoS consensus, Waltonchain innovatively integrates on its native Proof-of-Labor (PoL) consensus Blockchain which uses a perfect combination of PoW and PoS. Their PoL consensus uses a unique x11 (most energy efficient PoW) algorithm that keeps the hashrate at a minable rate over time as the network grows and a PoS that offers mining with stacking economic model which means that miner that has a masternode, receive a lower mining difficulty. A masternode is node status that is obtainable by storing and locking a certain amount of the network token in a wallet.

  This unique energy-efficient consensus is possible because they designed the mining chip and hardware themselves that consumes about 135W of power and hashes at about 400MH/s. Such energy need in mining is very low when compared with other PoW hardware used to mine Ethereum for example that consumes 150-250W for just 30-45MH/s. This is very important as PoW is considered a more secured consensus because it has major resilience to major known network attacks when compared to PoS and considering the amount of data collected and stored in such integration application and the security need, the use of a secured Blockchain consensus is paramount.
- **Data Originality:** A true data is needed to prove if a product is authentic and true data should be traceable back to the origin (source) and at the same time tamper-proof. Whereas

Blockchain tends to provide a perfect tamper-proof solution, collecting and uploading data right from the origin is very difficult and energy-intensive to achieve and is the reason most integration solution relies on APIs on the application or software layer to collect and upload data to the Blockchain. While this might seem to be more energy-efficient as the interface to data collection is normally done using a combination of passive (RFID or NFC) tags and readers which have low energy need, there exists a high risk for data corruptibility since the data are not collected and uploaded automatically right from the source. The method which Waltonchain is using to solve this is by collecting, processing and uploading data automatically solely on the hardware layer. They developed an improved communication chips specifically for Blockchain application that can upload data directly to a central server system and the hash (data fingerprint) simultaneously uploaded to the Blockchain. These hardware consists of sensors, cameras, and other data collectors as shown in figure 14 specifically designed for Blockchain application and known as Blockchain-enabled devices. Through these devices, all sort of data originating from the product's raw material, manufacturing, warehousing, and distribution can be uploaded directly to a Blockchain and by using a two-way read-write tag that have a unique and encrypted identification, attached to the product means it will be very hard or impossible to replicate such products with fake.

- **Data Interconnection:** The data collected through IoT and Blockchain will be more valuable if it can be applied in other industrial applications and not just for anti-counterfeit purposes considering the amount of energy needed to collect, process and store such data. Waltonchain again seems to be paying close attention to this through its parent-chain - child-chain architecture that allows multiple chains across different industries (child-chains) to be interconnected to its parent-chain and upload data. This creates the possibility of multiple industries chains that independently runs different Blockchain types (private or public) or consensus peculiar to the industry requirement to upload its data on the parent-chain (public-chain), interconnect and exchange data with other industrial chains thereby building an ecosystem of industries as shown in figure 13 and expands the application of the collected data. This will also eliminate the scalability (TpS -throughput) issue faced with Blockchain application because different industrial chains can process and approve its transactions and just uploads the hash to the parent chain. If this is rightly done, it means that information about every product can be uploaded on the Blockchain and queried by

any party with the right access just like people's information is queried on the internet (Google). If these products information is rightly uploaded on the chip layer automatically, it means they are authentic and can be trusted, therefore only information of authentic products will be available when searched and fake (counterfeit) product will be easily discovered and eliminated.

5.4 Ideal Application Scenario (case):

An ideal integration solution should have authentic data collection and traceability systems not just to be used for anti-counterfeit purposes but other applications. A State's standard organization like FDA, for example, might in the future depend on such data on a public Blockchain to confirm if a pharmaceutical drug product by a company like MitoQ meets certain required standards. If the drug organization like MitoQ has a counterfeit system that also collects data about its product right from production, logistics, and storage, such data can be used by any private and public organization with the necessary access rights for other applications and purposes. An illustration is shown in figure 15 where a product is attached with a two-way-read-write tag that uniquely identifies it and makes it impossible to clone right in the production stage. With the tag, the product identify can be uploaded directly to the Blockchain on the chip level. The product's package also is attached with a tag for easier tracking and supply chain management across the distribution channels while needed distributed information about the product, for example, is automatically written on the product's tag such that a consumer can access all this information at the consumption end. This makes it easy for a fake product to be easily detected both at the distribution and consumption ends because when a fake product's information is queried at both ends no information will be found about the product which automatically labels the product as a counterfeit and easily eliminates such product. Also, since the tag is attached in the product such that it can be easily damaged while trying to detached or replaced the tag from the product means that a damaged tag destroys the product and makes it fake.

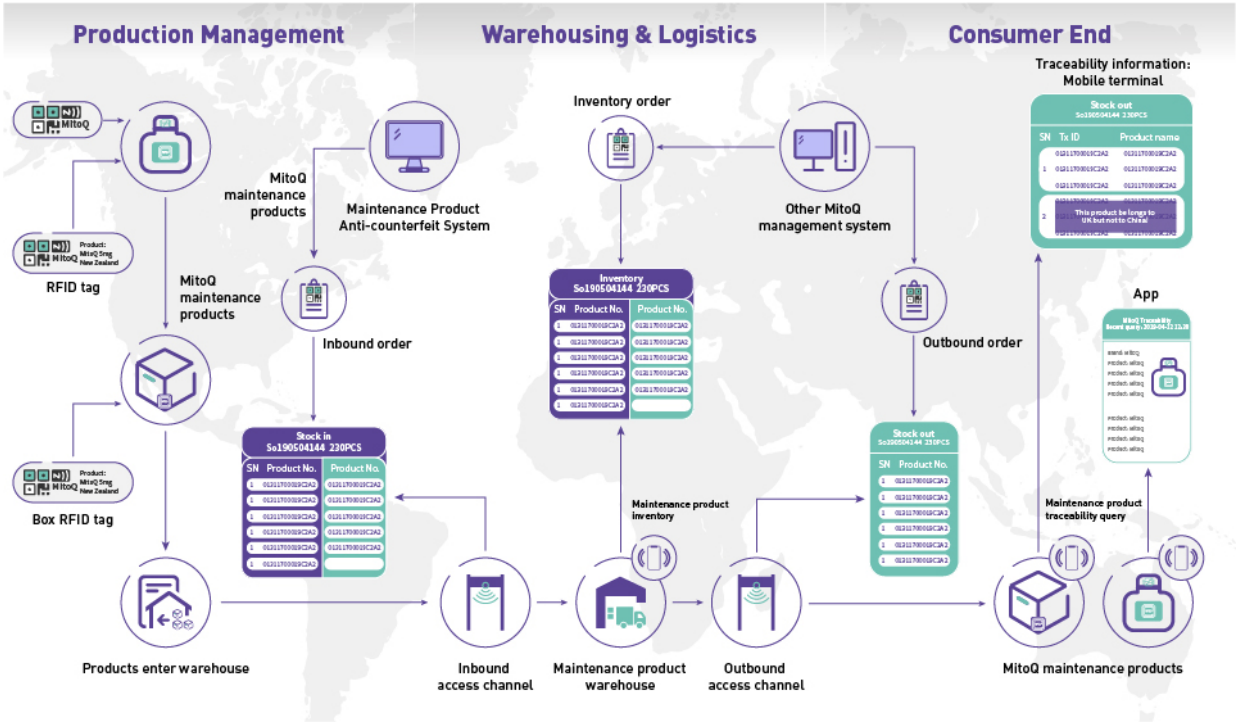


Figure 15: An Ideal application in pharmaceutical industry [71].

5.5 Energy Consideration for the Scenario (case): The power need for the major devices in the demo case are as follows:

- Tag (RFID) – Passive tags draws RF power from readers during communication
- Readers (RFID) – Uses 12V (3A) from DC source (battery), energy harvest like solar or transformed from 220V AC mains.
- Sensors – Passive sensors draws RF power during data upload and ideal other time while active sensors can use 12V DC from battery or transformed from 220V AC or from energy harvest source (solar).
- Data Collector – The data collector used to process and automatically upload sensors data to the Blockchain can be powered by a 1.5Ah battery that get recharged by energy harvest sources like solar and can last about seven (7) days when fully charged.

For the scenario considered above, there are lot of power sources available for the different devices, some are more applicable under certain application need and environment. For example, for a location like Finland, a solar energy source might not be applicable during winter season. For a portable application, where there is surface area constraint, a (12V, 3A – about 3*12*24*365*10(years)/1000 – 3,153kWh energy for a 10 years battery lifespan) rechargeable

battery cell is enough to power the RFID reader shown in appendix A, while the tags attached in the product are passive tags that draws power from the reader during communication. The same is true for other portable application cases or handheld IoT devices. For other applications like agriculture, where high number of sensors data needs to be uploaded to the Blockchain and there is little restriction on surface area, then, solar, RF or wind energy harvesting source could serve as an energy source to fit the large energy need. Also, irrespective of communication protocol used (low power, sub-G or NB-IoT, Bluetooth, Wi-Fi), devices should be kept at low-power mode when ideal to maximize power usage.

On the Blockchain end, the Blockchain storage architecture have a big impact on energy, the way and the amount of data stored determines the energy requirement for unloading and retrieval of such data. This means that traceability applications as considered in this work needs just the fingerprint of the processed data only uploaded to the Blockchain for authentication, such that the network is not congested, thereby resulting in difficulty increase of the network and high energy consumption by mining devices. This is because the data collectors used also serves as nodes which increases the network difficulty of forming a block as more data is uploaded to the Blockchain. For the block time (amount of time between each block) to be constant, the difficulty of a Blockchain network have to adjust to the total network hashrate that result in a higher difficulty to form a block.

6. CHALLENGES AND CONCLUSION:

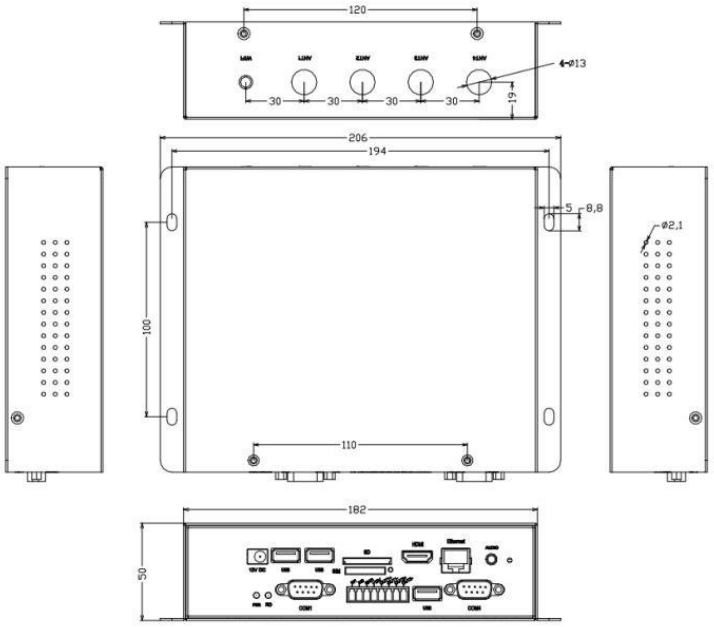
It was very challenging to complete this thesis work because both IoT and Blockchain are two developing technologies. This makes it hard and nearly impossible to publicly access academic materials which can be attributed to concerns of intellectual infringement or no academic activity at all in most cases partly resulting from vague legislative laws on Blockchain technology or the misconception that it is used solely for illicit activities. However, some degree of progress has been made in academic institutions in countries like China and South Korea where there seem to be more academic activities and clear legislative guidelines. Language, however, creates a big barrier to access this progress as most of the academic activities are not done in English. Also, some of the projects or institutions are not willing to share their progress because of concerns on intellectual rights (infringement). All these make it quite hard to ascertain quantitively, the full energy consumption when integrating Blockchain with IoT which is the main interest of this thesis. Nonetheless, it's justifiable to conclude that the progress and research milestones in the integration of Blockchain with IoT are developing properly in the right direction with projects paying close attention to energy consumption in their solution designs. This is why most project uses a third-generation Blockchain instead of a first which architecture is more energy-intensive. Those using the second generation are researching ways of migrating to a third-generation or using a second layer solution to improve efficiency. Other ongoing researches on efficient energy consumption are in data center and transport or radio access network devices, how to invariable improve the energy efficiency of these devices.

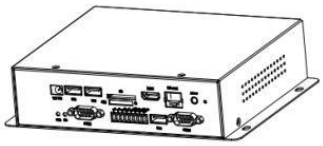
Two major integration methods were considered in this thesis but it was very hard to estimate how much amount of energy is consumed in both methods or quantitatively, which one is more energy efficient. The criteria in 5.3 and the possibility of extending the use cases of Waltonchain in other fields makes its architecture more feasible and viable as it can compensate for cases where high energy needs might grow over time as the Blockchain network expands.

More academic works can explore quantitively to discover more on this topic. Future work can be a proof-of-concept (PoC) developed for a simple Blockchain integrated with IoT application so that the energy consumption can be measured and then extrapolated for larger applications or network cases. Also, other integration use cases in the area of supply chain and retail management can be explored or better still, a combination of use cases like that of anti-counterfeit and supply chain management and how this combination might upset the energy need.

Appendix A Waltonchain Hardwares

A IoT-RU20 – UHF Android smart RFID Reader/Writer: [71]

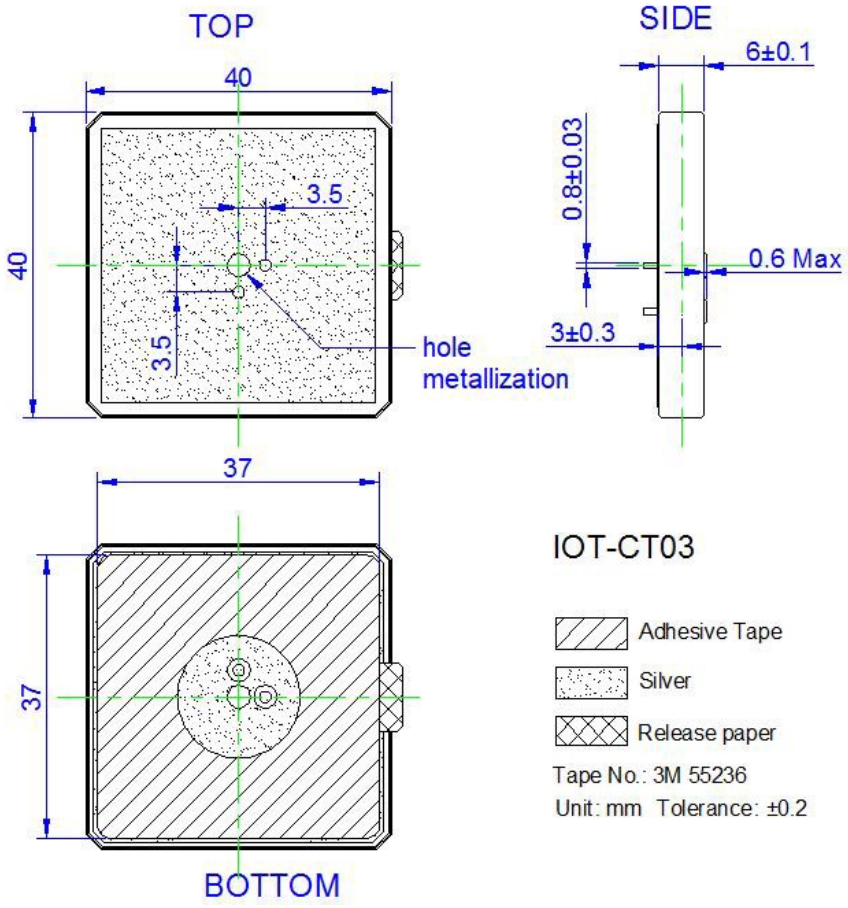




Specifications			
Interface Protocol	ISO/IEC 18000-6B/C EPC Class1 Gen2		
RF Output	31.5 dBm (max)		
Tag Reading Distance	≥15 m	12 dBi antenna (6C protocol)	Writing distance is ~40% of the reading distance (in special cases, it depends on the tag performance)
Network Interface	10M/100M Ethernet with auto-negotiation		
Tag Recognition Rate	>450 tags/s		
EPC Code	96 to 496 bits		
Embedded Android OS			
Power	DC 12V, 3A		
Storage Temperature	–40 to 85 °C		
Operation Temperature	–20 to 70 °C		
Relative Humidity	5 to 95%, no condensation		
Protection Rating	IP56		

IOT-RU20 Configuration

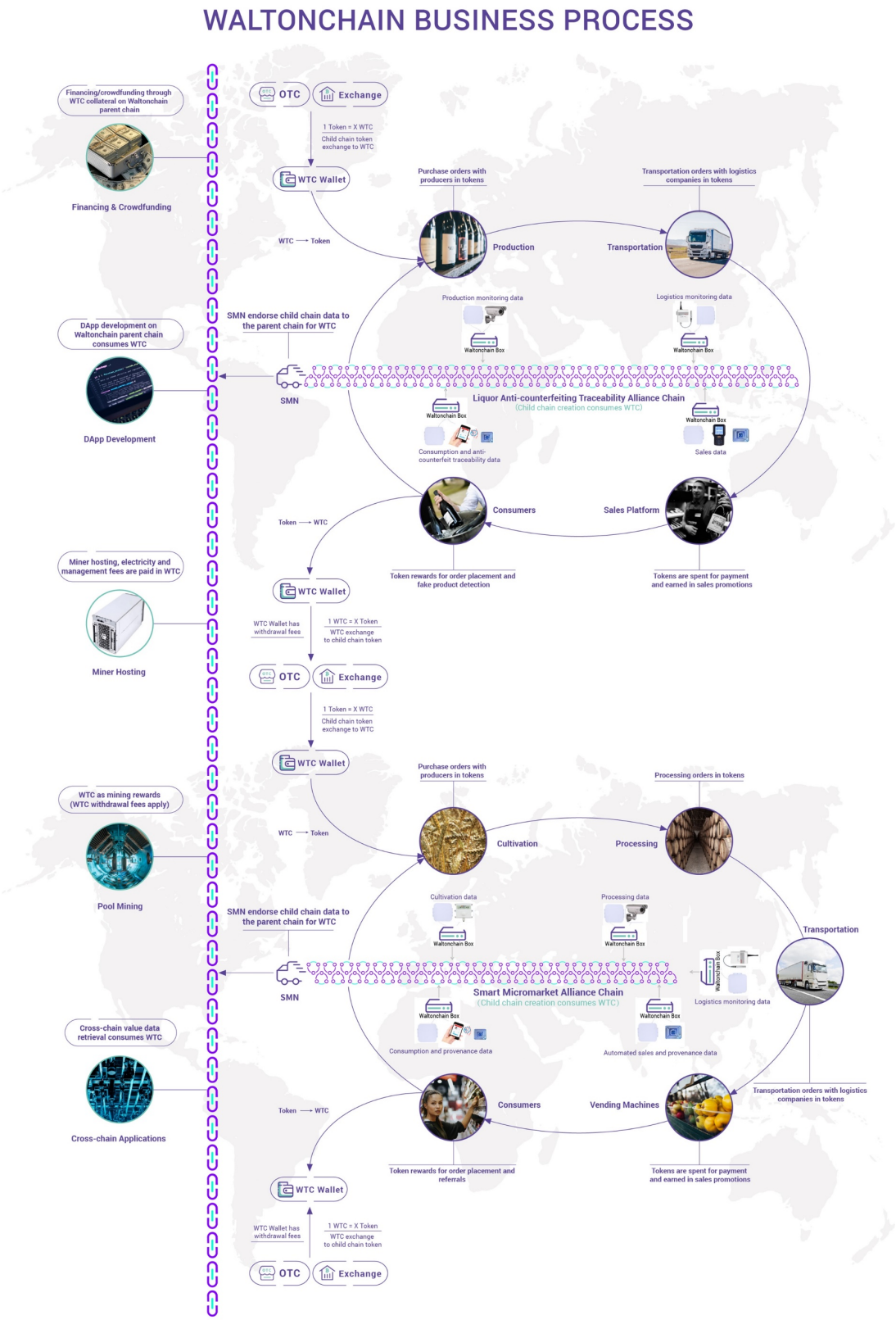
IoT-CT03 – UHF RFID Ceramics Antenna [71]



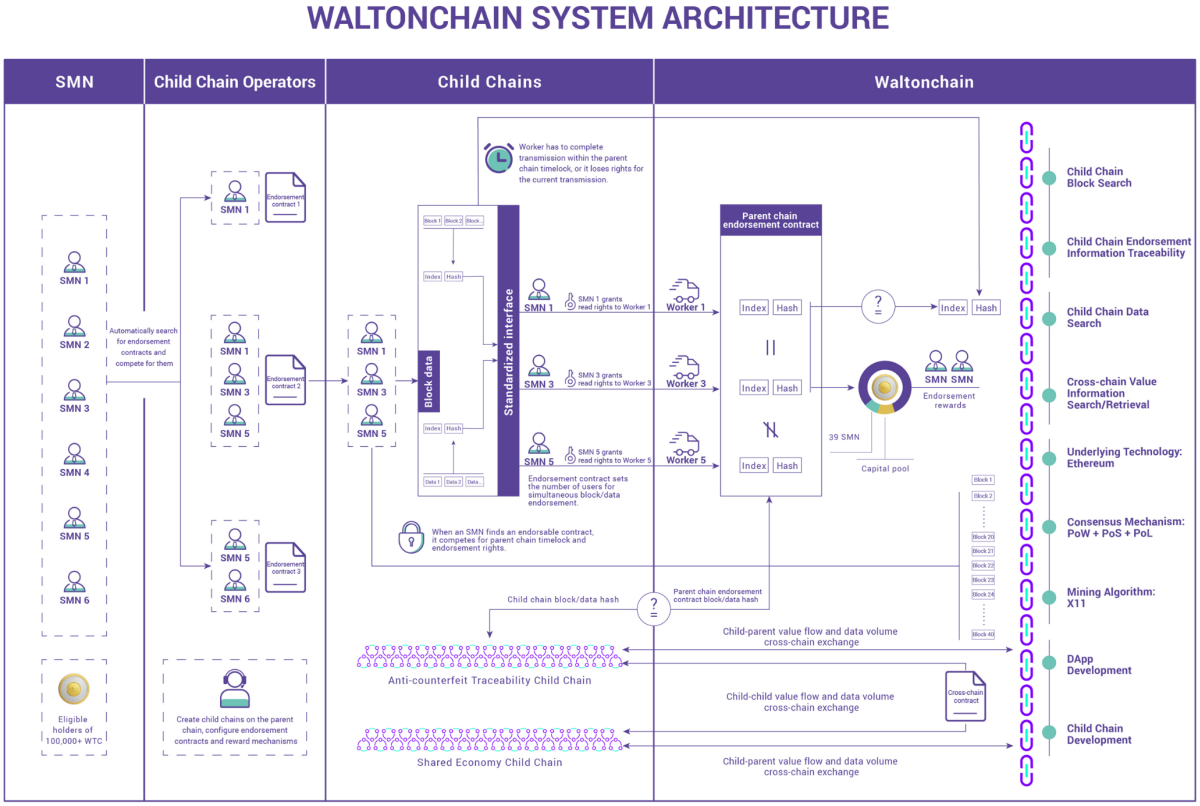
Specifications			
Dimensions	40 mm x 40 mm x 5 mm	Gain	3 dBi typical
Weight	25 g typical	Polarization	Circular
Material	Ceramics	Axial Ratio	<3 dB
Operating Frequency	902~928 MHz	Operating Temperature	–40~80 °C
Standing Wave Ratio	≤1.3:1	Storage Temperature	–40~80 °C

IOT-CT03 Specifications

B Waltonchain Business Process [72]



C Waltonchain System Architecture [72]



REFERENCE

1. OECD/EUIPO. 2016. Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact, OECD Publishing, Paris. Retrieved from https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/Mapping_the_Economic_Impact_study/Mapping_the_Economic_Impact_en.pdf. Accessed 31 March 2019

2. Business Wire. 2018. Global Brand Counterfeiting Report 2018-2020, Dublin. Retrieved from https://www.researchandmarkets.com/reports/4438394/global-brand-counterfeiting-report-2018 Accessed 31 March 2019

3. Smartrac. The True Cost of Counterfeiting. Retrieved from https://www.smartrac-group.com/files/content/Newsletter/Q1-2018/The_true_cost_of_counterfeiting_Infographic.pdf. Accessed 31 March 2019

4. Ali M.S. Vecchio M. Pincheira M. Koustabh D. Antonelli F. Rehmani M.H. November 2018. Application of Blockchain in the Internet of Things: A Comprehensive Survey. Retrieved from https://www.researchgate.net/publication/329763546_Applications_of_Blockchains_in_the_Internet_of_Things_A_Comprehensive_Survey. Accessed 31 March 2019

5. Corcoran P.M. April 2017. Third Time is the Charm – Why the World Just Might be Ready for the Internet of Things this Time Around. Retrieved from https://arxiv.org/ftp/arxiv/papers/1704/1704.00384.pdf. Accessed 31 March 2019

6. Chase J. September 2013. Texas Instruments. The Evolution of the Internet of Things. Retrieved from http://www.ti.com/lit/ml/swrb028/swrb028.pdf. Accessed 31 March 2019

7. Alkhatib H. Faraboschi P. Frachtenberg E. Kasahara H. Lange D. Laplante P. Merchant A. Milojicic D. Schwan K. September 2014. IEEE CS 2022 Report. IEEE Computer Society: Washington, DC, USA.

8. Sethi P. Sarangi S.R. January 2017. Internet of Things: Architecture, Protocol, and Application. Retrieved from https://www.researchgate.net/publication/312957467_Internet_of_Things_Architectures_Protocols_and_Applications. Accessed 31 March 2019

9. Burhan M. Rehman R.A. Khan B. Kim S. September 2018. IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. Retrieved from https://search-proquest-com.libproxy.tuni.fi/docview/2126878548?pq-origsite=summon. Assessed 31 March 2019

10. Suo, H. Wan, J. Zou, C. Liu, J. Security in the Internet of Things: A review. In Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE), Hangzhou, China, 23–25 March 2012, Volume 3, pp. 648–651
11. Kozlov, D. Veijalainen, J. Ali, Y. Security and Privacy Threats in IoT Architectures. In Proceedings of the 7th International Conference on Body Area Networks, Oslo, Norway, 24–26 February 2012, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering): Brussels, Belgium, 2012, pp. 256–262
12. Xiaohui, X. Study on Security Problems and Key Technologies of the Internet of Things. In Proceedings of the 5th International Conference on Computational and Information Sciences (ICCIS), Shiyan, China, 21–23 June 2013, pp. 407–410.
13. Bharathi, M.V. Tanguturi, R.C. Jayakumar, C. Selvamani, K. Node Capture Attack in Wireless Sensor Network: A survey. In Proceedings of the 2012 IEEE International Conference on Computational Intelligence & Computing Research (ICCIC), Coimbatore, India, 18–20 December 2012, pp. 1–3
14. Zhu X. Mukhopadhyay S. K. Kurata H. A Review of RFID technology and Its Managerial Applications in Different Industries. Journal of Engineering and Technology Management, vol. 29, no. 1, pp. 152–167, 2012
15. Welbourne E. Battle L. Cole G. 2009. Building the Internet of Things Ssing RFID: the RFID Ecosystem Experience. IEEE Internet Computing, vol. 13, no. 3, pp. 48–55, 2009
16. Yannuzzi M. Milito R. Serral-Gracia R. Montero D. Nemirovsky M. Key Ingredients in an IoT Recipe: Fog Computing, Cloud Computing, and More Fog Computing. in Proceedings of the IEEE 19th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD ’14), pp. 325–329, Athens, Greece, December 2014
17. Gupta S. Gupta B.B. Cross-Site Scripting (XSS) Attacks and Defense Mechanisms: Classification and State-of-the-art. Int. J. Syst. Assur. Eng. Management. 2017, 8, 512–530
18. Bandyopadhyay D. Sen J. May 2011. Internet of Things: Applications and Challenges in Technology and Standardization. Retrieved from Assessed https://www.researchgate.net/publication/51890865_Internet_of_Things_Applications_and_Challenges_in_Technology_and_Standardization. 31 March 2019
19. Fewtrell P. Hirst I.L April 1998. A Review of High-cost Chemical/Petrochemical Accidents Since Flixborough 1974”, in: Loss Prevention Bulletin. Retrieved from

http://www.hse.gov.uk/comah/lossprev.pdf. Accessed 31 March 2019.

20. Sethi P. Sarangi S. January 2017. Internet of Things: Architectures, Protocols and Applications. Retrieved from https://www.researchgate.net/publication/312957467_Internet_of_Things_Architectures_Protocols_and_Applications. Accessed 31 March 2019

21 Cook D. J. Youngblood M. Heierman E. O. MavHome: An Agent-based Smart Home, in Proceedings of the 1st IEEE International Conference on Pervasive Computing and Communications (PerCom '03), pp. 521–524, March 2003

22. HanandJ D.-M. Lim H. Design and Implementation of Smart Home Energy Management Systems Based on ZigBee, IEEE Transactions on Consumer Electronics, vol. 56, no. 3, pp. 1417– 1425, 2010

23. Dimitrakopoulos G. Intelligent Transportation Systems Based on Internet-connected Vehicles: Fundamental Research Areas and Challenges, in Proceedings of the 11th International Conference on ITS Telecommunications (ITST '11), pp. 145–151, IEEE, Saint Petersburg, Russia, August 2011

24. Hauber-Davidson G. Idris E. Smart Water Metering, Water, vol. 33, no. 3, pp. 56–59, 2006

25. Liu J. Li X. Chen X. Zhen Y Zeng L. Applications of Internet of Things on Smart Grid in China, in Proceedings of the 13th International Conference on Advanced Communication Technology: Smart Service Innovation through Mobile Interactivity (ICACT '11), pp. 13–17, February 2011

26. Bo Y. Guangwen H. Supply Chain Information Transmission Based on RFID and Internet of Things, in Proceedings of the Second ISECS International Colloquium on Computing, Communication, Control, and Management (CCCM '09), pp. 166–169, Sanya, China, August 2009

27. W. Z. Khan, Y. Xiang, M. Y. Aalsalem, and Q. Arshad, "Mobile Phone Sensing Systems: A Survey," IEEE Communications Surveys & Tutorials, vol. 15, no. 1, pp. 402–427, 2013.

28. Sundmaeker, H. Guillemin, P. Friess, P. Woelfflé, S. (2010). Vision and Challenges for Realizing the Internet of Things. Cluster of European Research Projects on the Internet of Things, European Commission, 3(3), 34-36

29. Roman, R. Zhou, J. Lopez, J. On the Features and Challenges of Security and Privacy in Distributed Internet of Things. Compute. Network. 2013, 57, 2266–2279

30. Stankovic, J.A. Research directions for the Internet of Things. IEEE Internet Things J. 2014, 1, 3–9

31. Borgohain, T. Kumar, U. Sanyal, S. Survey of security and privacy issues of Internet of Things. arXiv, 2015; arXiv:1501.02211

32. Microsoft. 2018. 5 Ways Blockchain is Transforming Financial Services. Retrieved from https://azurecomcdn.azureedge.net/cvt-ac32f4ee3b822380cab6779654f512595b82c56474f4d57be61e4b54a277a208/mediahandler/files/resourcefiles/five-ways-blockchain-is-transforming-financial-services/five-ways-blockchain-is-transforming-financial-services.pdf. Accessed 31 March 2019

33. Conoscenti M. Vetro A. De Martin J.C. Blockchain for The Internet of Things: A Systematic Literature Review, in IEEE/ACS 13th International Conference of Computer Systems and Applications, 2016, pp. 1–6

34. Reyna A. Martín C. Chen J. Soler E. Diaz M. On Blockchain and its Integration with IoT: Challenges and Opportunities, Future Generation Computer Systems, 2018

35. Fernaa T.M. Ndez-Caramal A. Fraga-Lamas P. A Review on the Use of Blockchain for the Internet of Things, IEEE Access, vol. 6, pp. 32 979–33 001, 2018

36. Panarello A. Tapas N. Merlino G. Longo F. Puliafito A. Blockchain and IoT Integration: A Systematic Survey, Sensors, vol. 18, no. 8, p. 2575, 2018

37. Cha S.C. Chen J.F. Su C. Yeh K.H. A Blockchain Connected Gateway for Ble-Based Devices in the Internet of Things, IEEE Access, 2018

38. Zyskind G. Nathan O. Pentland A. Enigma: Decentralized computation platform with guaranteed privacy, 2015, Last Accessed: December 12, 2018. [Online]. Available: https://enigma.co/enigma_ full.pdf

39. Shafagh H. Burkhalter L. Hithnawi A. Duquennoy S. Towards Blockchain Based Auditable Storage and Sharing of IoT Data, in Proc. of the Cloud Computing Security Workshop, 2017, pp. 45–50

40. Ali M. S. Dolui K. Antonelli F. Iot Data Privacy via Blockchains and IPFS, in 7th International Conference for the Internet of Things, 2017

41. Yu B. Wright J. Nepal S. Zhu L. Liu J. Ranjan R. Iotchain: Establishing Trust in The Internet of Things Ecosystem Using Blockchain, IEEE Cloud Computing, vol. 5, no. 4, pp. 12–23, Jul 2018

42. Bocek T. Rodrigues B. B. Strasser T. Stiller B. Blockchains Everywhere a Use Case of Blockchains in The Pharma Supply Chain," in IFIP/IEEE Symposium on Integrated Network and Service Management (IM), 2017, pp. 772–777

43. Biswas K. Muthukkumarasamy V. Securing Smart Cities Using Blockchain Technology, in 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, 2016, pp. 1392–1393

44. Vechain Foundation. May 2018. Development Plan and Whitepaper. Retrieved from https://cdn.vechain.com/vechainthor_development_plan_and_whitepaper_en_v1.0.pdf. Accessed 31 March 2019

45. Nakamoto S. January 2009. Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf. Accessed 31 March 2019

46. Zheng Z. Xie S. Dai H.N. Chen X. Wang H. October 2018. Blockchain Challenges and Opportunities: A survey. Retrieved from https://www.researchgate.net/publication/328338366_Blockchain_challenges_and_opportunities_A_survey. Accessed 31 March 2019

47. Lamport L. Shostak R. Pease M. (1982) The Byzantine Generals Problem, ACM Transactions on Programming Languages and Systems (TOPLAS), Vol. 4, No. 3, pp.382–401

48. Vasin, P. (2014) Blackcoin's Proof-of-Stake Protocol v2, https://blackcoin.co/blackcoin-pos-protocolv2-whitepaper.pdf

49. King S. and Nadal S. (2012) Ppcoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, Self-Published Paper, August

50. Microsoft. 2018. How Blockchain Will Transform the Modern Supply Chain. Retrieved from https://www.retailinsiders.nl/docs/6f69823f-662f-4b18-9268-61e908b6f388.pdf. Accessed 31 March 2019

51. KPMG. 2018. Blockchain and The Future of Finance: A Potential New World for CFOs – And how to Prepare. Retrieve from https://advisory.kpmg.us/content/dam/advisory/en/pdfs/blockchain-future-finance.pdf

Retrieved from Accessed 31 March 2019

52. DHL Trend Research. 2018. Blockchain in Logistics: Perspective on the Upcoming Impact of Blockchain Technology and Use Cases for the Logistics Industry. Retrieved from https://www.logistics.dhl/content/dam/dhl/global/core/documents/pdf/glo-core-blockchain-trend-report.pdf. Accessed 31 March 2019

53. Deloitte Global Blockchain Lab. When Two Chains Combine: Supply Chain Meets Blockchain. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/strategy/us-cons-supply-chain-meets-blockchain.pdf. Accessed 31 March 2019

54. Deloitte. Key Challenges: Blockchain Enigma, Paradox, Opportunity. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-key-challenges.pdf. Accessed 31 March 2019

55. Gauer M. December 2017. Bitcoin Miners True Energy Consumption. Retrieved from https://www.researchgate.net/publication/322118225_Bitcoin_miners_true_energy_consumption. Accessed 31 March 2019

56. Zibin Z. Shaoan X. Xiangping C. Huaimin W. 2018. Blockchain Challenges and Opportunities: A Survey Retrieved from https://www.henrylab.net/wp-content/uploads/2017/10/blockchain.pdf. Accessed 31 March 2019

57. Visa. Visa Acceptance for Retailers. Retrieved from https://usa.visa.com/run-your-business/small-business-tools/retail.html. Accessed 31 March 2019

58. 5G IoT. Key Issues: Energy. Retrieved from https://whatis5g.info/energy-consumption/. Accessed 31 March 2019

59. Baliga J. Ayre R. Hinton K. Tucker R.S. June 2011. Energy Consumption in Wired and Wireless Access Networks. Retrieved from https://ieeexplore.ieee.org/abstract/document/5783987. Accessed 31 March 2019

60. Cha H.J. Yang H.K. Song Y. October 2018. A Study on the Design of Fog Computing Architecture Using Sensor Network. Retrieved from https://www.researchgate.net/publication/328550159_A_Study_on_the_Design_of_Fog_Computing_Architecture_Using_Sensor_Networks. Accessed 31 March 2019

61. Kaur N. Sood S.K. June 2017. An Energy-Efficient Architecture for the Internet of Things (IoT). Retrieved from https://ieeexplore.ieee.org/abstract/document/7293596. Accessed 31 March 2019

62. CeeT (Center for Energy-Efficient Telecommunication). June 2013. Whitepaper: The Power of Wireless Cloud. Retrieved from https://ceet.unimelb.edu.au/publications/ceet-white-paper-wireless-cloud.pdf. Accessed 31 March 2019

63. Fehske A. Fettweis G. Malmodin J. Biczok G. August 2011. The Global Footprint of Mobile Communications: The Ecological and Economic Perspective. Retrieved from https://ieeexplore.ieee.org/document/5978416 Accessed 31 March 2019

64. Zhang Y, Yu R. Nekovee M. Liu Y. Xie S. Gjessing S. Cognitive Machine-to-Machine Communications: Visions and Potentials for the Smart Grid. Network, IEEE, 26(3):6–13, 2012. ISSN 0890-8044

65. Zhang P. 2013. Energy-Efficient Clustering Design for M2M Communications. Retrieved from http://www.diva-portal.org/smash/get/diva2:706229/fulltext01.pdf. Accessed 31 March 2019

66. Ambrosus Blockchain Whitepaper. Retrieved from https://ambrosus.com/assets/en/-White-Paper-V8-1.pdf. Accessed 31 March 2019

67. Wood G. Whitepaper – Ethereum: A Secure Decentralized Generalized Transaction Ledger (EIP-150 Revision). Retrieved from https://gavwood.com/paper.pdf. Accessed 31 March 2019

68. Waltonchain Whitepaper. 2018. Retrieved from https://www.waltonchain.org/en/Uploads/2019-04-25/5cc171763aebb.pdf. Accessed 31 March 2019

69.Linxens Whitepaper - dLoc: Document Authentication Solution. Retrieved from https://www.linxens.com/dloc/Linxens_dLoc_Solution_for_Document_Authentication_White_Paper.pdf
. Accessed 31 march 2019

70. The Economist. July 2018. Why Bitcoin Uses So Much Energy. Retrieved from https://www.economist.com/the-economist-explains/2018/07/09/why-bitcoin-uses-so-much-energy. Accessed 31 March 2019

71. Waltonchain Medium Post. Retrieved from https://medium.com/@Waltonchain_EN Accessed 19 December 2019

72. Waltonchain Business Processes. Retrieved from https://www.waltonchain.org/en/sys/cate/48.html. Accessed 19 December 2019