ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ

Blockchain and IoT: Προβλήματα Ενοποίησης και Προκλήσεις

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Κωνσταντίνος Χαϊντούτης

Επιβλέπουσα: κα Μαρία Κοζύρη

Λαμία, Ιούνιος 2019

UNIVERSITY OF THESSALY

SCHOOL OF SCIENCE

INFORMATICS AND COMPUTATIONAL BIOMEDICINE

Blockchain and IoT: Integration Issues and Challenges

MASTER THESIS

Konstantinos Chaintoutis

Supervisor: Koziri Maria

Lamia, June 2019

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ
ΚΑΤΕΥΘΥΝΣΗ ΠΛΗΡΟΦΟΡΙΚΗ

«ΠΛΗΡΟΦΟΡΙΚΗ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ, ΔΙΑΧΕΙΡΙΣΗ ΜΕΓΑΛΟΥ ΟΓΚΟΥ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΠΡΟΣΟΜΟΙΩΣΗ»

Blockchain and IoT: Προβλήματα Ενοποίησης και Προκλήσεις

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Κωνσταντίνος Χαϊντούτης

Επιβλέπουσα: κα Μαρία Κοζύρη

Λαμία, Μάρτιος 2019

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο «Blockchain and IoT: Προβλήματα Ενοποίησης και Προκλήσεις» αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο ΔΗΛΩΝ : Κωνσταντίνος Χαϊντούτης

Ημερομηνία : 03 Ιουνίου 2019

Υπογραφή :

Blockchain and IoT: Προβλήματα Ενοποίησης και Προκλήσεις

Κωνσταντίνος Χαϊντούτης

Τριμελής Επιτροπή:

Μαρία Κοζύρη

…………………… ……

…………………… …….

Επιστημονικός Σύμβουλος:

Νικόλαος Τζιρίτας

ABSTRACT

During this emerging data era, data is being gathered, analyzed and capitalized by companies and organizations to personalize services, enhance corporate processes and to predict future trends. Nowadays, data is a valuable asset in our economy and the Internet of things (IoT) and its potential growth is one more technology evolvement that will increase the current problem of data production and security.

In 2017 the amount of online IoT devices were estimated around 7 billion and by 2030 they could exceed 100 billion. Consequently, security and privacy issues will immerge as those devices could be anything from a high end server or a smart car to a cheap temperature sensor and that is the main problem as the majority of current IoT devices are astonishingly insecure. In recent years, the Blockchain technology has taken the industry by storm and by many is considered the silver bullet that will enhance IoTs security.

In this paper I will examine the potential exploitation of the Blockchain technology that would allow securing the unsecure IoT ecosystem, discuss the advantages and disadvantages of the aforementioned technology and present some of the most important, already deployed, projects that are trying to converge the Blockchain Technology with the Internet of Things.

ΣΥΝΟΨΗ

Τη σημερινή εποχή ο κόσμος μας κατακλύζεται από δεδομένα, τα οποία συγκεντρώνονται, αναλύονται και χρησιμοποιούνται από εταιρείες και οργανισμούς προκειμένου να προσωποποιήσουν υπηρεσίες, να βελτιώσουν εταιρικές διαδικασίες και να προβλέψουν μελλοντικές τάσεις. Τα δεδομένα σήμερα αποτελούν ένα πολύτιμο επενδυτικό αγαθό της οικονομίας μας και το Διαδίκτυο των Πραγμάτων (IoT) και η δυνητική του εξάπλωση αποτελεί μια ακόμα εξέλιξη της τεχνολογίας που θα επιβαρύνει ακόμη περισσότερο το πρόβλημα της παραγωγής και της ασφάλειας των δεδομένων.

Το 2018, ο αριθμός των συνδεδεμένων IoT συσκευών στο διαδίκτυο εκτιμάται ότι είναι υπερβαίνει τα 7 δισεκατομμύρια και μέχρι το 2030 εκτιμάται ότι μπορεί να ξεπεράσει τα 100 δισεκατομμύρια. Έτσι, αναπόφευκτα πρόκειται να ανακύψουν θέματα ασφάλειας και ιδιωτικότητας καθώς αυτές οι συσκευές μπορούν να είναι οτιδήποτε από έναν τελευταίας τεχνολογίας διακομιστή ή ένα έξυπνο αυτοκίνητο μέχρι ένα απλό αισθητήρα θερμότητας και αυτό αποτελεί και το κυριότερο πρόβλημα καθώς η πλειοψηφία των τωρινών IoT συσκευών είναι εξαιρετικά επισφαλής. Τα τελευταία χρόνια, η τεχνολογία Blockchain έχει κατακλύσει το ενδιαφέρον της βιομηχανίας και από πολλούς θεωρείται η ασημένια σφαίρα που θα ενισχύσει την ασφάλεια του IoT.

Σε αυτή την εργασία θα εξετάσω την πιθανή εκμετάλλευση της τεχνολογίας Blockchain και πως αυτή θα επιτρέψει την ασφάλιση του επισφαλούς οικοσυστήματος του IoT, θα αναφέρω τα πλεονεκτήματα και τα μειονεκτήματα της προαναφερόμενης τεχνολογίας και θα παρουσιάσω κάποιες από τις ποιος σημαντικές, ήδη εφαρμοσμένες, πρωτοβουλίες που ενοποιούν την τεχνολογία Blockchain με το Διαδίκτυο των Πραγμάτων.

Table of Contents

1. Introduction

The Internet of Things, a technology that developed in the past years, is probably the greatest exhibition of computing progress that questions our adequacy to manage the security and safety of our environment. Often new technologies emerge and are being introduced into the world, but we rarely understand their full implications, or even their potential growth and predominance. Since now, in most cases we had the chance to implicate standardized security solutions to confront these new threats as they emerged alongside with new tech breakthroughs. But now we are faced with the fact that computing technology is evolving faster than our ability to address the threats we can see clearly, not to mention the threats that will come to the surface only after these technologies are fully situated.

The diversity of existing and future IoT applications and devices renders security and privacy issues a really hard puzzle that needs to be solved. Currently, IoTs security in most cases is based on centralized models (client/server), but the evolvement of its implementations will eventually demand different approaches and current trends point towards decentralized models which will be scalable and will protect user's privacy. One of the most intriguing trends to address this matter is the use of BlockChain technology as the cornerstone to secure the Internet of Things.

The rest of the paper is organized as follows; the second chapter is dedicated to IoT, its potential growth, architecture and vulnerabilities. In the third chapter, I thoroughly discuss the Blockchain Technology, trying to explain how does it work, what are its key concepts, its future applications and I persist on consensus algorithms, as they play a very important part in every potential convergence proposal I will introduce further on. In the fourth chapter I present how can the Blockchain Technology enhance IoTs security, the challenges to be met and the tools that may lead to this convergance. In the fifth chapter, I will list some of the most important projects that their products are already available for use or are still under development/testing, and finally some theoretically proposed solutions, aiming to introduce different architectural approaches towards that matter.

2. Internet of Things

The Internet of Things (IoT) is an ecosystem of various electronic devices such as wearables, security cameras, medical devices , home or industrial appliances etc. that have the ability to communicate and interact with each other as they make use of their embedded hardware, software and sensors to enhance their standard functioning by enabling mainly new automated and remote capabilities.. The number of IoT enabled devices increases with extremely high pace and currently it is estimated that it exceeds 25 billion with the forecast that it could reach 70 billion by 2025. Also the global market value of IoT may be worth more than $7.1 trillion by 2020. (1)

The distributed nature of IoT and its forecasted expansion brings us closer to a world where more and more aspects of our lives are interconnected. This will trigger massive changes in our way of living and imposes a real challenge for humanity to assimilate and integrate the new status quo.

"The Internet of things" as a term was firstly introduced by Kevin Ashton, in 1999.

2.1 How does it work?

In order to better familiarize with the Internet of Things, it is crucial to analyze some key concepts.

Sensors: convert a non-electrical input into an electrical signal that can be transported upon an electronic circuit. Sensors have the task to create information by collecting data from their environment. The sensors have to be small and energy efficient. All IoT enabled devices have one or more sensors, in example, a single thermometer, or a mobile phone that has multiple sensors (amera, accelerometer, GPS, etc)

Connectivity: Enables sensors-devices to interact with other such devices and also with other services and applications that work in the cloud. Their interconnection with the cloud may be accomplished by various methods such as: Bluetooth, cellular, WiFi, satellite, LPWAN, or by connecting via Ethernet physically to the internet.

Middleware: Merge all the elements that form the Internet of Things, enables different applications that operate on heterogeneous systems to interact.

Addressing and Scalability: Any device that is connected with the IoT network is mandatory to have a unique attribute that can distinguish it from all others. The addressing system that is used in the IoT is IPv6 (replaced IPv4) because it has the potential to support the excessive growth of interconnected IoT devices.

Data storage and analytics: The huge amount of data produced and transported within the IoT must be stored, analyzed and processed. The above mentioned processes enable utilities such as smart monitoring and real time decision making. The processes may be as simple as to check if a temperature value is within the desired range, or they could be really complex such as image analysis on video to identify objects (like burglars in your office).

User Interface: Somehow the gathered information may be sent as a notification to the user. In example, alert him that the temperature of a location is not within the desired range.

The user may also have an interface that enables him to check the system remotely. In example, a user may need to examine the surveillance recordings of their infrastructure through the internet (phone app, web browser).

Moreover, the user may also have the ability to change system settings. He may remotely alter the temperature in his house or turn on the boiler by using an app on his mobile device.

Also, some tasks could be triggered automatically. Based on predefined rules the system could act autonomously and apart from just sending a notification to alert you of an intruder in your house it could also automatically notify relevant authorities.

2.2 Standards and Protocols

Internet of Things is spread amongst almost everything, from industries and huge cross-platform lineups to stand alone home-use devices, vehicles, agriculture infrastructures and much more that are communicating in real time via the internet. In order all of these deployments to work properly and achieve the desired connectivity and functioning, various communication protocols have immerged, some of which are the result of alliances and federations that formed aiming to merge the chaotic nature of IoT (2).

Below I present some of the protocols that were developed particularly for IoT and talk briefly about their attributes:

- **MQTT** (Message Queuing Telemetry Transport) and **MQTT-SN** (MQTT For Sensor Networks) are both lightweight publish/subscribe protocols and the first is more suitable for low bandwidth-long distance communication while the latter was designed explicitly for M2M and mobile applications.
- **CoAP** (Constrained Application Protocol)

  CoAP is an application layer protocol that was developed to cover the needs of less powerful gear like WSN nodes. CoAP by design has the feature of being able to easily convert to HTTP to enhance internet interaction, and it also meets unique needs such as low overhead, simplicity and multicast support.
- **XMPP** (Extensible Messaging and Presence Protocol) and **XMPP-IoT**

  XMPP is suitable for real-time communication, able to support a plethora of applications such as instant messaging, group chat, lightweight middleware proper dissemination of XML Data. The latter has the same general features while having the ambition to make M2P and M2M interoperable.
- **SSI** (Simple Sensor Interface)

  SSI is a plain communications protocol that was developed to transfer data from smart sensors to computers and vice versa.
- **DDS** (Data-Distribution Service for Real-Time Systems)

  Is the prime global middleware standard that was developed specifically to allow publish-subscribe communications in real-time.
- **Mihini/M3DA**

  Mihini is a software module that enables the intercommunication of a M2M server with the applications running on an embedded gateway. M3DA imposes a protocol that is specifically developed to transfer M2M data and it enhances Device and Asset Management.
- **AMQP** (Advanced Message Queuing Protocol)

  AMQP is an open standard wire-level protocol and semantic framework for high performance enterprise messaging, which main attributes are message orientation, queuing, routing, reliability and security.
- **LLAP** (lightweight local automation protocol)

  LLAP allows the communication between any suitable intelligent devices with plain text messages. So unlike TCP/IP or WiFi etc, LLAP may be used everywhere ignoring any medium's restrictions.

- **LWM2M** (Lightweight M2M)

  LWM2M, was designed based on REST, is a device management protocol, it was developed for sensor networks to enable M2M communication and offer a common standard for managing less powerful objects that are a significant part of IoT networks.

- **HTTP/2** - With the use of compression of the header field it reduces latency issues by enhancing the use of network resources and also it enables the multiple use of the connection.

- **Websocket**

  WebSocket is full-duplex communication protocol that allows communication through a TCP connection were there can be intercommunication between client/server. It is supported by almost every web browser and regarding IoT implementations it deciphers the difficulties of the needed constant communication between client and server.

Within the IoT there are typically four communication models (3):

Device-to-Device communication concerns the exchange of messages between two or more directly connected devices. These communications usually use protocols like Bluetooth, Zigbee and Z-Wave, but they can be facilitated through other networks such as the Internet.

The D2D communication is most often used to transfer small data packets in closely bounded areas like small office automated systems that don't require high data rates of information to be transmitted, in example communication between a thermometer and a heating unit, or a light sensor with a light bulb.

Device-to-cloud communication concerns the interconnection of IoT devices with Cloud Services via the internet, in example to exchange data and control network traffic. The fact that the cloud services are most often at a great distance from the contacting counterpart demands the use of high data rate connections such as WiFi, Ethernet or cellular technology.

Device-to-Gateway, as IoT devices usually don't connect directly to cloud services this model concerns the use of an intermediary device that allows the communication to be conducted in a secure environment and also to execute any required protocol translations. These gateways could be either software programs or dedicated hardware devices, and apart from security they could also preprocess transmitted data to reduce network traffic.

Back-End Data-Sharing broadens device-to-cloud communication model and allows authorized third parties to gain access for aggregation and analysis purposes, over IoT devices and sensor data.

2.3 IoT architectures

The Internet of Things has the ability to interconnect various different devices through the internet and in order to achieve that it needs a flexible layered architecture. The technologies used in the IoT have such diversity that makes it impossible to acknowledge a single architecture as a fundamental principle. The most common architectures are the 3-layer architecture and the 5-layer architecture.

2.3.1 The 3-layer architecture was the first IoT architecture proposed.

The **Perception Layer** is the primary layer of IoT. This layer can collect and observe all types of information which are used in IoT environment. This information can be captured by using the sound sensors, RFID sensors, temperature sensors, camera, GPS etc. There are two parts of perception layer: i) the perception node which is used for data control and ii) the perception network which is used to sends data to the controller.

The **Network Layer** also known as transportation layer. This layer has transmission capabilities to transfer data from lower layer to upper layer (4). This layer can also transmit the information or data via the internet. So this layer can combine various heterogeneous networks (5).

The **Application Layer** also known as a service layer, this layer converts information into content and provides a good user interface (UI) to a higher level or end users. Through this layer, information is shared with communities in a secure way so no unauthorized person can read it (4). It involves Cloud Computing, intelligent processing pervasive computing, and mega databases.

The IoT evolvement through the years made the 3-layer architecture insufficient to cover all demands generated. So, other architectures were proposed.

2.3.2 The 5-layer architecture

It consists of the perception layer, the transport layer, the processing layer, the application layer and business layer. The three-layer architecture though describes the main aspects of IoT architecture, doesn't offer the necessary research ground for more sophisticated analysis of the Internet of Things (6).

In this model perception and application layer have the same use as described above regarding three layers architecture. So below there is a description of the other three layers that was introduced to form this new model.

Transport layer as indicted by its name transfers data that are gathered by sensors from perception to processing layer and backwards through WiFi, cellular, Ethernet, Bluetooth, RFID, and NFC networks.

Processing layer a.k.a middleware layer is designed to gather, process and analyze extensive data streams that are channeled to it by the transport layer. By engaging various technologies like big data processing platforms and cloud computing it can offer many services to the layers below.

Business layer administers every aspect of the IoT environment, such as applications, profit models, users' privacy and analysis (graphs, charts).

3-layer architecture	5-layer architecture
Application layer	Business layer
	Application layer
Network layer	Processing layer
	Transport layer
Perception layer	Perception layer

Table 1. 3-layer (left) and 5-layer (right) IoT architectures

2.3.4 Other models

There are also other architecture models that are used for special purposes but they can't be considered as standard architectures (7).

IoT-A, a business oriented architecture that develops various reference architectures according to the special requirements of each domain.

BeTaaS is an architecture that provides M2M communication, it consists of four layers: physical, adaptation, TaaS and service.

OpenIoT is an architecture based on the model that was suggested by IoT-A. The primary objective is to provide the framework for connecting physical or virtual sensors to the cloud.

IoT@work is a European Commision project that primarily targets to establish automated middleware systems that will support Plug & Work and self management. The architecture of the model is not static thus it is able to readjust according to where it will be deployed.

These four architectures (7) were surveyed in order to clarify a set of rules that would be mandatory for securing IoT ecosystems, and more specific, Network Security, Identity management, Privacy, Trust and Resilience.

2.4 IoT applications

The Internet of Things has expanded largely in recent years, from simple home use sensors to industrial units and wearables. It slowly penetrates many aspects of our routine. Its applications upgrade our daily lives and give us potentials that we have never previously imagined. The aroused interest about IoT led many companies to put their efforts and materialize fundamental IoT ingredients such as hardware, software and support, and gave the opportunity to the developers to build applications that enable the connection of almost everything to it. As said before, the Internet of Things has spread to almost everything and below I present some of the most intriguing instances that probably will present remarkable growth in the following years (8):

Smart Homes: In recent years many people used “smart” technology to enhance their residence commodities. In the future this phenomenon is going to escalate greatly as much more devices will acquire the capability to interact through the internet and other local networks with other devices and their owners. The owner of a smart home has the ability to manage home appliances, security systems and much more, remotely, even from the other side of earth. Moreover, he may set rules for automated procedures that are triggered if the specific circumstances are met. IoT's market regarding smart homes is probably the most developed until now.

Smart grids: With the use of smart grids, consumers and electricity suppliers will be able to interact in a more sophisticated and transparent way, to enhance the use and distribution of electricity.

Wearables: They suggest one of the most popular IoT implementations and many tech giants invest in the improvement of these gadgets. Smartwatches are probably the most well known such devices. They are easily paired with any Smartphone for entertainment and communication purposes but they also provide many other usages such as fitness, health and sleep monitoring. Wearables must be small, light, shockproof, energy-efficient and ideally waterproof. Consequently, the required attributes pose a real challenge for any company that tries to further improve this technology.

Retail: The implementations of IoT regarding retail are unimaginable; they could extend from a fridge that automatically orders goods that had been consumed to the complete monitoring of products supply chains. As for the latter, many companies have already released platforms that offer real-time tracking of products, storage reserves, authenticity checks and much more.

Smart Cities: They imply one of the greatest IoT manifestations that aim to enhance the urban lives of millions of people. In the near future we will have to deal with problems that are growing exponentially, such as pollution, insufficient energy, traffic, population growth etc. Smart cities will make use of most of IoT related technology innovations to offer smart transportation, more efficient energy management, advanced security systems, waste management and generally exploit the vast generation of information to better the lives of their citizens.

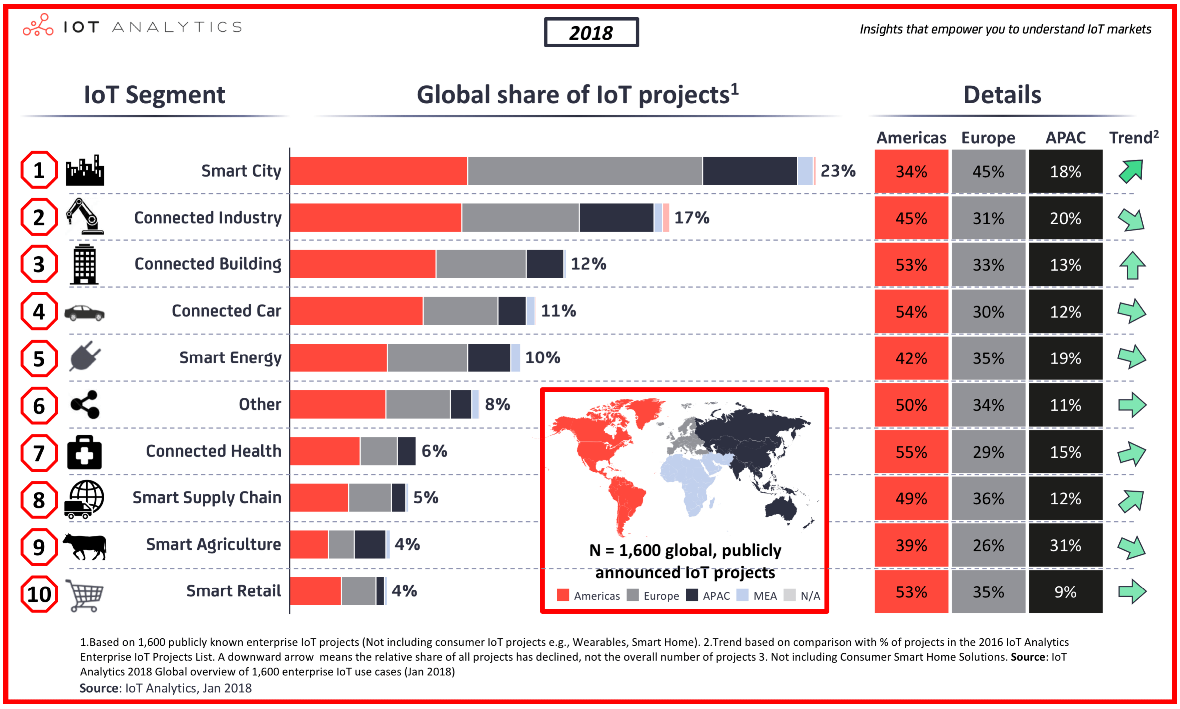
Health Care: Is one of the most valuable applications, because it will improve people's well being through connecting the health care systems and smart medical devices. Companies already offer technology that enables real-time monitoring of patients vital signs and allows immediate response to any abnormality that may occur, Future Path Medical is one of them. Moreover, if patients records are available online for every authorized treating institution, any emergency situation could be addressed fast and effectively as treating personnel will have all the available information about a patient's health background, allergies etc.

Smart Farming: It gives new potential to enhance farming workflow, as farmers will have live feeding about, temperature, humidity, soil fertility, etc., with the use of the appropriate sensors. Consequently it will help them increase yield and product quality, by using such information to better schedule watering intervals, fertilizer use and optimum estimations about harvesting.

Transportation: Firstly encountered in science fiction movies, self-driving vehicles are today a reality that promises to increase driver's comfort - security and decrease pollution. Many industry giants are investing vast amounts of money to evolve this technology and make it affordable and also more applicable for daily use. Furthermore, smart cars will also provide many more facilitations to their owners, regarding safety, entertainment, information, etc. The project of smart transportation does not only include cars but it extends to every other means such as, trains, ships and airplanes.

Industrial: Industries, made use of automation technologies far back, to increase their productivity and effectiveness. The integration of IoT technology to their production line will give to automation processes a great boost ahead. The use o smart sensors, remote connectivity and M2M communication will allow industries to further improve their workflows and avoid any possible procrastination.

Smart Retail: is based in intelligent payment solutions, in-store shopping behavior, and proximity-based advertising.



	IoT Segment	Global share of IoT projects[1]	Americas	Europe	APAC	Trend[2]
1	Smart City	23%	34%	45%	18%	↗
2	Connected Industry	17%	45%	31%	20%	↘
3	Connected Building	12%	53%	33%	13%	↑
4	Connected Car	11%	54%	30%	12%	→
5	Smart Energy	10%	42%	35%	19%	→
6	Other	8%	50%	34%	11%	→
7	Connected Health	6%	55%	29%	15%	→
8	Smart Supply Chain	5%	49%	36%	12%	↗
9	Smart Agriculture	4%	39%	26%	31%	↘
10	Smart Retail	4%	53%	35%	9%	→

1.Based on 1,600 publicly known enterprise IoT projects (Not including consumer IoT projects e.g., Wearables, Smart Home). 2.Trend based on comparison with % of projects in the 2016 IoT Analytics Enterprise IoT Projects List. A downward arrow means the relative share of all projects has declined, not the overall number of projects 3. Not including Consumer Smart Home Solutions. **Source**: IoT Analytics 2018 Global overview of 1,600 enterprise IoT use cases (Jan 2018)

Source: IoT Analytics, Jan 2018

Figure 1. Global of IoT projects by continents

Source. IoT analytics 2018 Global overview of 1600 enterprise IoT use cases, August 2018

2.5 IOT vulnerabilities

The Internet of Things is the extension of the traditional internet that was so far used to interconnect computers and the last two decades smartphones and other such devices. The real difference between an IoT enabled device and a traditional device (pc, server, smartphone) is that the first have much less computing capabilities and security specifications. These cheap devices that have functions similar to a computer enable us to create vast networks and acquire tons of information through any possible source. But, the downside is that in such a chaotic network environment data are transmitted, processed, analyzed and gathered by companies around the globe without us knowing where, when and how they will be used and that causes serious concerns about our privacy and security (9).

The above mentioned data may be used for several sophisticated and individually targeted services that enhance user's experience. But, this data also contain information that could enable the creation of an online record of our activities, exposing our habits and routines.

As mentioned above, privacy concerns that rise from IoT are intensified by the vacancy of integral security shields that the first gen IoT devices had.

Through IoT we can certainly enhance our lives, as we have conveniences that we couldn't have imagined. For instance, we can remotely observe that an elder person who lives far away from us, is moving inside the house, have knowledge of its physical condition (blood pressure and heartbeat), or even know if he went shopping(smart refrigerator).

But while there are many pros, there are also many cons as the attack surface is widen and devices that may seem innocent, in example a baby monitor or a surveillance webcam could possibly be part of a distributed Denial of Service attack.

Below we exhibit the main IoT vulnerabilities that we currently have knowledge off. (10) (11).

Vulnerable web interface: Many smart devices come with an embedded web server that is used to manage them via an appropriate web app. If the interface is not programmed correctly (bug-free) then security could be compromised and give ground for an attack. A web interface with limited security can be the cause of data loss or corruption, denial of access or lack of accountability and can be the cause of a total device takeover.

Insufficient Authentication - Authorization: IoT devices usually have flaws regarding their implementation or authorization - authentication mechanisms. Also the security features available aren't always used to their full extend by the users. The attackers can exploit such weaknesses as weak passwords, faulty procedures for password recovery, unshielded credentials or absence of access controls for specific interfaces.

Insecure network services: IoT devices may have procedures for testing and maintenance but these tools may be lightly tested, and it is possible that they run exploitable source code in the background. Attackers take advantage of vulnerable network services and may attack the device itself or to unleash attacks through it.

Lack of transport layer encryption: An IoT device that transmits sensitive data without using secure protocols to achieve that, not encrypted, has no protection and anyone that has access to local networks or the internet can read it. Some may say that local network traffic is not widely visible but this is not the case in a wireless network that was set up poorly. This highlights the need that all data transmitted are properly encrypted, or else we could endanger the device or our user account data.

Privacy issues: No encryption and poor security features mean that if an attacker has access to the IoT device, then he has access to all our stored and transmitted data that are not properly protected or had been stored unintentionally. The device should only collect and store data that are essential to complete its work.

Insecure cloud – mobile interface: Many IoT devices are able to connect to the cloud or can be accessed through our mobile phone. This means that they have a cloud or/and mobile based management interface that adds one more probable security vulnerability. In order to confront that, if possible, the device management interface should be embedded to the device as it would enhance security because the attacker most often doesn't have direct access to the local network but has to bypass the router's firewall.

Inadequate security features: First generation IoT devices often lack the security features that are vital to keep them safe. The attacker may use the absence of access control mechanism to acquire data or take over the device. A device is insecure if the users are not able to adjust security settings at their own will. Possible dangers arouse also from lack of encryption, lack of password options (obliged to use strong passwords, wrong password used policy, etc).

Unprotected patches and upgrades: A serious security threat is present if the device is not going to be supported for further updates by the manufacturer. Devices should be able to get updates if a vulnerability is discovered, but even in this case the software and firmware updates may be insecure too if the network connection they are reached from is not protected. And in any case we should avoid any possible threats such as malicious updates via DNS hijacking, by monitoring the traffic of the network while the update takes place and also by crosschecking with a hex editor that the downloaded file is the one that we intended to download originally.

Erasing personal data: Another serious issue regarding privacy of the user comes when for example we want to sell an IoT device. Similarly to when we want to sell our mobile phone to buy a new one, what are the steps that we should follow to be certain that all our personal information and data that are stored in it through the years will be wiped out.

Poor physical security: Another major security issue regarding IoT devices is the fact that depending on where it is installed an attacker may have physical access to it. Attackers may possibly use USB ports, SD cards or other portable storage interfaces or even disassemble the device to gain access to the operating system and to the data stored in it.

2.6 Things to keep in mind when using IoT devices.

The matters discussed in the previous section concern the developers as well as the consumers/users. But a user should also keep in mind when purchasing a IoT device that there might be hidden terms regarding the functioning of the device that aren't desirable for most. Also regarding security features of the purchased IoT device, we can't simply rely to the fact that there are available/supported, but we should take all appropriate measures to fully take advantage of these features.

As the Internet of Things evolves, we have a plethora of devices that promise to better our everyday life, these devices are manufactured by many developers, and often the consumers choose devices that are cheap, friendly to the user and offer more capabilities. They don't pay much attention in regard with security specifications and settle with the fact that they may endanger their privacy and possibly their health.

Even top branded manufactures may exhibit indifference regarding customer's privacy (12). Vizio, a consumer electronic firm has come to an agreement to pay to US regulators 2.2 million dollars, as they didn't manage to have their users consent in order to monitor their viewing habits on TV. In 2017, the Consumer Council of Norway discovered that a toy doll recorded all conversations that the children had with it and then transmitted them to a company in the US. As they found out the involved company had retained the rights of sharing and using the collected data for various purposes. Also it was later revealed that the same doll had a security defect that enabled attackers to gain access and speak or listen through it. Such defects and poor security controls can be very dangerous and may lead to severe damages in the virtual but as well as in the physical environment.

IoT devices had been exploited during few of the biggest DDoS attacks, like the attacks against "Dyn" (internet company) and Brian Krebs (security researcher) were largely supported by hacked IoT devices. Nevertheless, hacked IoT devices may pose possible weaknesses and be dangerous solely, in example, Fiat Chrysler in 2015 was forced to recall 1.4 million vehicles after it was proven that their systems could be hacked and the attacker could take over the control of major functions of the car such as the brakes (12). The attacks have expanded further as there are cases were the offenders aimed at healthcare devices, traffic lights, energy and industrial systems.

Another issue is that sometimes the device you buy is never really completely yours. Most devices come with pre installed software and sometimes some parts of software are mandatory for the operation of it and cannot be altered in any way. In majority such software is licensed, meaning that the buyer kind of rents it, and the terms granted with license agreement may prohibit users from repairing or modifying their devices.

Anyone who buys an IoT device or any smart device should have in mind that there are ways to protect and fortify his digital presence and footprint. The measures we use to protect our internet activity in general, are good to start with, but there are also some other things we should keep in mind regarding the use of IoT devices, as in this case we may endanger not only some online assets or our privacy but also our physical lives (hacked door lock, hacked car).

Below we present some ways to protect our IoT enabled devices against various threats (13):

- Implement each and every security feature available
- Keep your devices firmware updated all the time
- Always create strong passwords
- Change passwords often/change default

- Disable the use of every port that is not used
- Always use encryption (devices, networks)
- Power Dependency issues (Buttery powered/ possible black out)
- Buy trusted brands/trusted hardware

3. Blockchain Technology

The technology that enables the functioning of Bitcoin and of many others cryptocurrencies is a distributed, immutable ledger database that offers timestamped transactions. It is a set of blocks, placed one after another that are used for recording and distributing data. There is a vast variety of data that may be stored in the ledger database including payment history, contracts and personal data.

Blockchain technology has gathered much attention in recent years from various sides, including academics and professionals in many sectors, such as (finance, insurance, law, informatics technologies), and this happened because of its enticing features like decentralization, immutability and security. A late article states that Blockchain technology may impact 36 different industries (14).

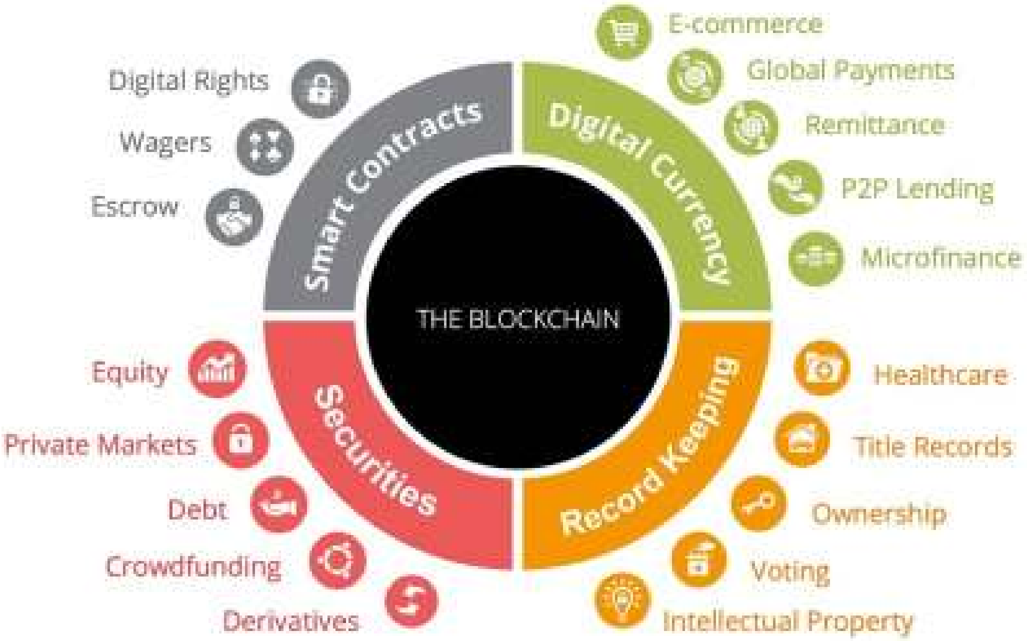


Figure 2. Blockchain affected industries. (Source: BTCS.com)

3.1 General Information about Blockchains

As mentioned above the Blockchain is a distributed ledger database that allows the conduction and validation of transactions without the need of an intermediate authority. The pioneer idea of the Blockchain was introduced in 2008 by a person who used the alias Satohi Nakamoto with a paper under the title “Bitcoin: A peer-to-peer electronic cash system” (15).

The digital ledger of transactions is distributed across all participating nodes. The blocks shape a linear chain and every block indicates the hash of the block before it. The Blockchain network is preserved by a set of nodes that may execute and record the same transactions. Every node can have access and read the public information regarding a transaction. All new transactions are validated by other nodes that participate in the network, and this allows it to function without the necessity of an intermediate. Introducing/attaching new blocks to the Blockchain demands that a computational expensive puzzle would be solved. The puzzle must be difficult to solve, but it must be verified easily and fast (16). The use of this method enables us to achieve trust in a trustless environment of nodes by using a trustless consensus algorithm. The computing demands needed to join and "compete" to solve this puzzle may be of an extremely high degree, and that narrows the amount of blocks that could potentially be mined by a single node and moreover protects the ledger from mischievous miners. The procedure of figuring out the solution to the puzzle includes a mechanism that brings up volatility between miner nodes that "compete" to create the next block of the chain. Current Blockchain applications adopt mainly one of these two coconsensus algorithms: Proof of Work (POW) or Proof of Stake (POS). Proof of Work needs extremely demanding computing resources, while Proof of Stake requires computing as well as memory resources to figure out the cryptographic puzzle (16). The exchange of messages/data that takes place among all nodes of the network is done with the use encryption to avoid from being intercepted. Blockchain users are able to use different Public Keys, in order to avoid being tracked.

3.2 How do Blockchains Work?

Blockchains are distributed data structures which are copied and shared to every member of a network and they were used in Bitcoin to confront with the double spending problem (that is the case when digital tokens are used more than once to pay for two or more different things). Blockchains though may work also independently, or be used in other fields apart from the cryptocoins market.

If you consider that the blockchain is a log whose data files are put into blocks that are chronographically signed. Every block has a unique cryptographic hash that acts as its identity and it also contains a hash indication of the previous block. This fundamental structure of the ledger connects each block with its one step far neighbors and creates a chain of blocks, the blockchain - Figure 3. Every node that has access to the blockchain has the ability to go through the data that the ordered chained blocks contain and clarify if the ongoing transactions in the network are valid or not (17).

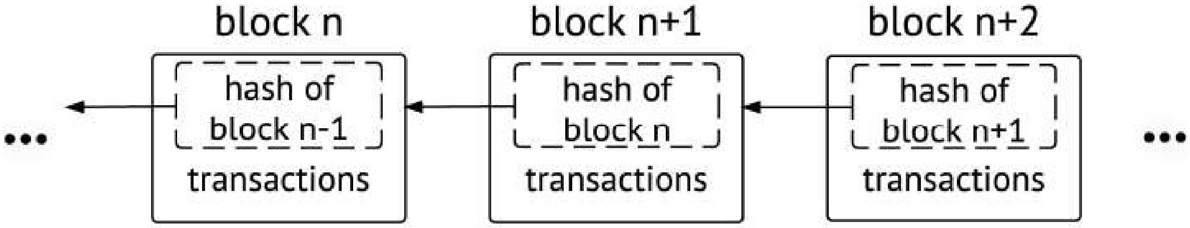


Figure 3. Every block contains a transactions catalogue plus a hash reference of the past block (17).

In a blockchain network that is a set of nodes that works in the blockchain through the image that every node has. We assume that each user makes transactions through his personal node, and all the nodes together assemble a P2P network. The users have a set of public/private keys that enables them to interact with the blockchain. With their private key they sign their transactions, and their public key is used so that they would be identifiable in the blockchain network. Public/private key cryptography enhances the network with security features such as authentication and integrity. All signed transactions of a user are broadcasted from his node to the nearby nodes that are one-hope away. Those nodes confirm that the broadcasted transaction they receive is legit, and only then they transmit it further; if it is not legit then it is discarded. The transactions that finally got stored after being validated by the blockchain network following the previously discussed procedure and in a pre-agreed time frame, are put arranged into a timestamped block that is called a candidate block, concluding the mining procedure. Then the miner sends the candidate block to every node of the network, and if they confirm that it contains legit transactions and valid references, proven by the correct hashing of their previous block, and this procedure is continuous. If there are no problems the nodes accept the candidate block and add it to their chain wile updating their world view. Otherwise, the candidate block is discarded (17).

In order for a blockchain network to be able to reach consensus the transactions made need to fulfill a specific set of rules. These rules help each blockchain client to determine if an incoming transaction is legit, and consequently forward it and when it is verified by all nodes they add it to their database as an authenticated and timestamped block. The fact that consensus is achieved between non trusted nodes and without the presence of a trusted intermediate authority is the key feature of the blockchain networks.

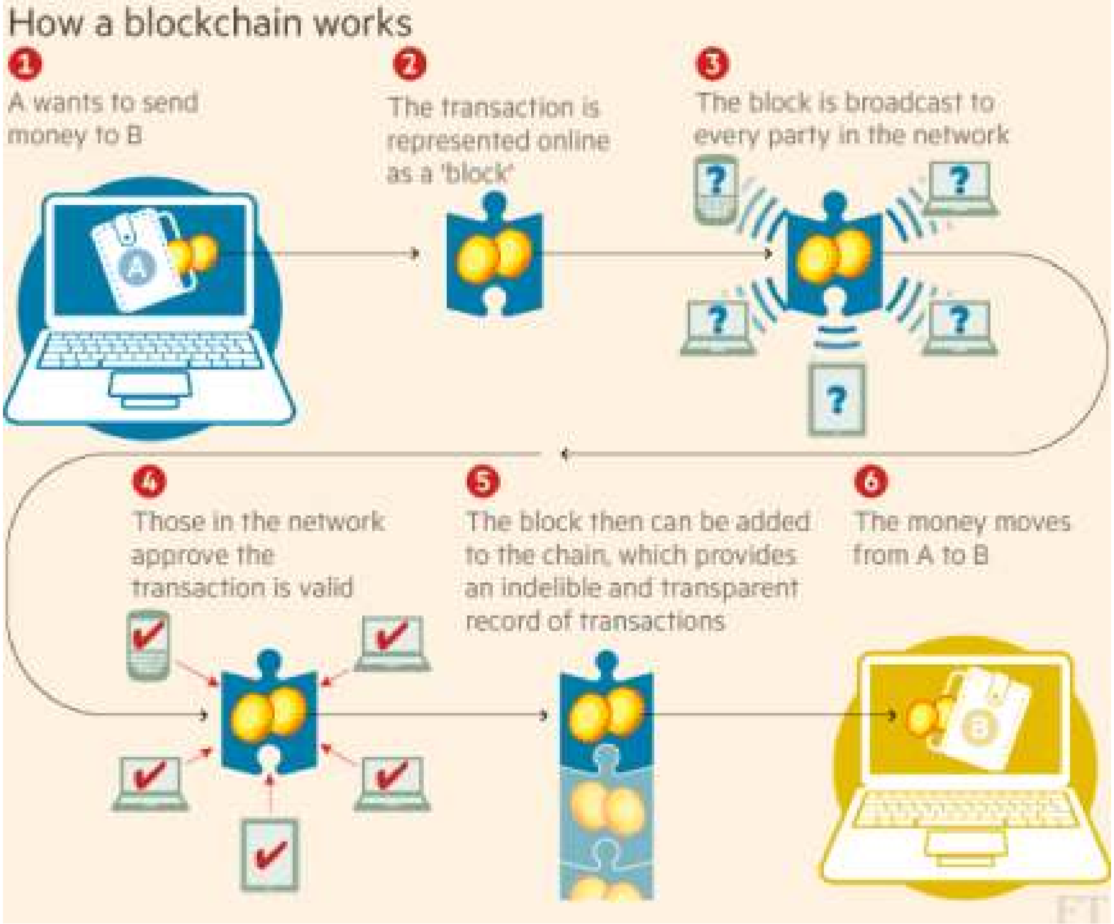

How a blockchain works
1
A wants to send money to B
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
A
B
FT

Figure 4: How a blockchain works (source: agenda.webforum.org)

In every blockchain network, the consensus mechanism that allows it to work properly needs to be distributed. In a public network that anyone can enter with multiple ids can manipulate the validation process (voting) to achieve his own purposes (Sybil Attack). The solution to this problem is given in Bitcoin and many other cryptocoins by making the mining process computationally expensive. If a node wants to make it's processing block the next mined block in the chain it has to solve the cryptographic puzzle and generate it's Proof of Work, that is to "calculate" the right random number of the block's header that will make the used one way cryptographic hashing algorithm export the value that the is expected by the network.

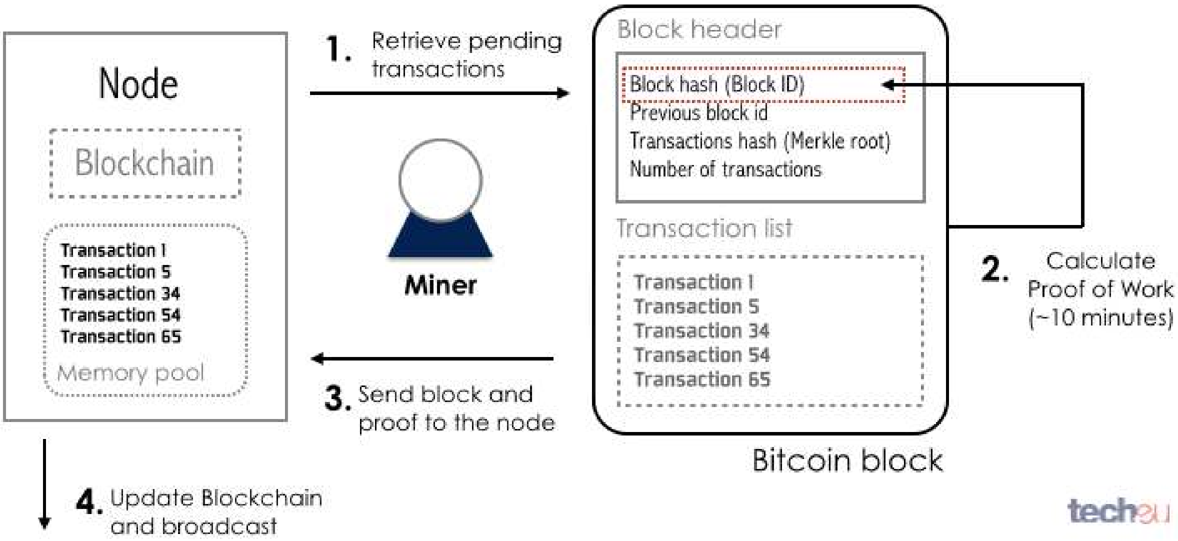


Figure 5. Bitcoin's Proof of Work
Source: http://tech.eu/features/808/bitcoin-part-one/

In case two nodes are mined simultaneously, a fork can appear in the chain. If that occurs then the nodes will choose the "correct" node to adopt depending on which node will grow faster, as it is pretty impossible that both forks will produce a new block synchronously.

3.3 Explaining key Concepts of the Blockchain technology

The Blockchain technology involves many concepts, some were mentioned earlier in this paper, but here we will to try to demystify most of the main terms that we will come across next.

Blockchain Block: A block contains a number of the recent transactions that still have not been recorded in any prior blocks. After a block is introduced into the blockchain, it gives way for the next to come. Blocks therefore are permanent instances of records which, once written, cannot be changed or deleted. Blocks are chained to each other in chronological order.

Blockchain Transaction: Transactions are signed pieces of data that are broadcasted in the network and if they prove to be valid they are added in the blockchain. Transactions usually associate the turnouts of the latest completed transactions and use them as new transaction inputs and attach them to new values. The fact that they are not encrypted, offers to everyone the ability to read any transaction that was stored in a block.

Distributed Ledger Technology: A Distributed Ledger is nothing more than a database that is synchronized and common to everyone at all times in a network that may be expanded to many locations. The transactions that are made are public and therefore make a cyber attack more difficult. All changes that happen on the ledger are broadcasted to every node that participates in the network, the longest, within a few minutes.

Mining: Is the procedure of adding transactions to the blockchain. Mining involves compiling late recorded transactions into blocks and solving a computationally difficult puzzle. Whoever solves the puzzle first is allowed to place the next block on the chain and is rewarded.

PoW(Proof of Work): Is the first consensus algorithm that was adopted in a Blockchain network and is pledged to validate transactions and add new blocks into the chain. Is a part of data that it is demanding to produce but is easily verified.

Decentralized consensus: A decentralized design exploits the advantages of a distributed network thus enabling its nodes to record transactions that occur at all times, on blocks that are stored on a public ledger. Each successfully stored block includes a hash of the latter block's data that helps determining the authenticity of the source of the transaction and eliminates the necessity for an intermediate authority.

Blockchain services: In a Blockchain you can store data in a semi-public manner into the chains blocks. Everyone is able to verify that you placed that data because the header of the record is signed by your public key, but what is below the header can be only accessed by you since you are the only one that has the private key to unlock it.

Smart contracts: Smart contracts are some kind of application scripts that contain a unit of value (token or money), have a unique address and functions that control this value. We can set off the execution of a smart contract when we sent a transaction towards its address. Then it executes autonomously on all the nodes of the network as ordered by the content of the triggering transaction. Smart contracts were introduced so that a transaction's contractual governance among two entities could be verified electronically through the blockchain, instead of through a trusted intermediary. One great feature of smart contracts is that the two entities can set the terms of their in-between arrangements under predefined conditions that were embedded into their code, and could allow automated payment transfers as soon as the agreed services are delivered, or incur penalties if not.

3.4 Brief history of Bitcoin

A paper that was titled "Bitcoin: A Peer-To-Peer Electronic Cash System" (15) was published in 2008 and the author used the pseudonym Satoshi Nakamoto. In this paper he described a peer to peer equivalent of virtual money that would support direct payments without the need of an intermediate financial institution. The first implementation of this suggestion was Bitcoin, as a pioneer of the many cryptocurrencies that followed.

Few months after the publication of the paper, open source software that adopted the proposed protocol was released and it started with the formation of the original 50 coins block. Everybody could download and install this software, joining the Bitcoin P2P network, and since then it has developed significantly. Its value has even reached 19.000 $ per coin in 2017.

2008		2009	
August 18th	bitcoin.org was registered	January 3rd	Formation of the genesis block 18:15:05 GMT
October 31st	Bitcoin design paper published	January 9th	Bitcoin v0.1 released and reported on the cryptography mailing list
November 9th	Bitcoin project registered at SourceForge.net	January 12th	Bitcoins first ever transaction, in block 170 from Satoshi to Hal Finney

Table 2. Bitcoin's History (18)

3.5 Blockchain Taxonomy

A general categorization of blockchains would be to divide them depending on who has access on them and they would be distinguished as follows:

Public or permission-less network, can be joined by anyone, while in a private or permissioned network; this is not the case unless he is admitted after meeting specific requirements. Everyone can read or write data. In public networks we need more security as there is no trust among the nodes. Therefore, the consensus mechanism needed, demand higher computing costs and has to reward the miners. This is needed in order to confront the possibility of a Sybil attack (19).

Private networks are not open for everyone and in order for someone to join he has to be invited. All the participants in a private network are considered trusted and this enables the network to work with less demanding consensus mechanisms increasing throughput.

Permissioned networks, also known as Consortium Blockchain, are hybrid versions of public and private blockchains, were the consensus is achieved by a preselected set of nodes which are invited, but all transactions are public. Access rights regarding reading Blockchains data may be assigned to one participant or be distributed among all participants of the consortium. Also they support hybrid routes, in example the root hashes of the blocks that anyone can read.

Blockchains can be categorized in many more different aspects depending on their architectural characteristic, below we present most of them briefly in two tables (3, 4) based on the categorization suggested by Paolo Tasca and Claudio J. Tessone (20).

Consensus	Transaction Capabilities	Native Currency	Extensibility
Topology Decentralized Hierarchical Centralized	**Data Structure (Block Header)** Binary Merkle Tree Patricia Merkle Tree	**Native Asset** None Own Crypto Convertible Multiple assets	**Interoperability** Implicit Explicit None
Gosiping Local Global	**Transaction Model** Unspent Transaction Output Traditional Ledger	**Tokenisation** None Third party addons Tokenisation	**Intraoperability** Implicit Explicit None
Communication Synchronous Asychronous	**Server Storage** Full Nodes Thin nodes	**Asset Supply Management** Limited – Deterministic Unlimited – Deterministic Pre-mined	**Governance** Community Technical Alliance
Finality Non – Deterministic Deterministic	**Block Storage** Transactions User balance		**Script language** • Turing Complete • Generic non TC • Application Specific non TC • Non TC + External Data
	Scalability Limits Number of transactions Number of users Number of nodes Confirmation time		

Table 3: Blockchain Taxonomy part 1

Security/Privacy	Codebase	Identity Management	Charging/Rewarding
Data Encryption SHA-2 ZK-SNARKS	**Coding language** Single Multiple	**Access/Control Layer** Public Private Permissioned	**Reward System** Lump-sum Reward Block + Security
Data Privacy Built-in Add-on	**Code License** Open Source Closed Source	**Identity Layer** KYC/AML Anonymous	**Fee System** Optional Mandatory None
	Software Architecture Monolithic Design Polylithic Design		**Fee structure** Variable Fees Fixed Fees

Table 4: Blockchain Taxonomy part 2

3.6 Blockchain Technology advantages

The Blockchain technology has many advantages that can help enhancing the cyber security in many aspects. They offer an efficient way to secure data from being accessed without proper authorization, protect them from manipulation and guarantee availability. Here we will describe briefly some of the main benefits of the Blockchain Technology (21), (22).

Decentralization: As a P2P network technology that supports distributed consensus protected by encryption, it eradicates the obligatory involvement of a trusted intermediate, since every user is able to see the transactions.

Track and trace: All blockchain transactions are signed digitally and get a time-stamp, and that enables all the network users to run back and examine previous transactions and track a records state during the requested time. And that is an aspect that is great for companies as it gives them the ability to get accurate data about their products state or delivery status.

Confidentiality: Blockhain network users have elevated confidentiality as they use public-key cryptography to authenticate and encrypt their transactions. The fact that a user is addressable in the network as some of his data are public does not mean that they can also reach his encrypted data. Even if a user forget or lose his private key, though his data can't be erased they are still protected in terms of confidentiality as no one can decrypt it.

Fraud and data manipulation security: The merged usage of cryptography, hashing and decentralization make it impossible for anyone to manipulate the data on the ledger, and an attempted hack is easily identifiable. Blockchain networks are believed to be unhackable as attackers can only manipulate the network if they somehow get to control the voting majority of the network nodes.

Sustainability: In a Blockchain network the term “single point of failure” doesn’t imply, as even in an attempted DDoS attack, the system will continue to work as intended due to the multiple instances of the ledger.

Integrity: The distributed ledger safeguards the user’s data from being modified or deleted. Blockchain tech guarantees validity and permanence of every concluded transaction and that the generated blocks after being encrypted contain changeless data that are hack proof.

Resilience: Being a P2P network guarantees that it will operate 24/7, as even if few nodes have been compromised or offline, it will not affect the networks functionality.

Data quality: Blockchain technology is able to ensure that the encrypted data kept on the ledger by its users are accurate.

Protected network access: The use of blockchains can also protect our home or business network from the danger of losing control of our private keys, there are startups i.e REMME that provides SSL certification stored in the blockchain for the user’s equipment, so there is no need for an authentication server or a password database. This eliminates the need for users to remember passwords and makes it really hard for an unauthorized person to access to the network.

Protected communication: Blockchains can help protect the communication of governance, military, business and individuals, as they all send and receive sensitive data through communication networks. The use of the blockchain technology minimizes the danger of eavesdropping while communicating.

Smart contracts: As mentioned earlier the smart contracts are small pieces of code, placed on the distributed ledger, that guarantee compliance with the terms embedded in the contract and also cross-checks transactors.

Availability: Our sensitive data are always secure because they are saved in many sites of the blockchain network and we can access it at any time and from everywhere.

Authenticity: Blockchain networks implementation, the distributed ledger of data transactions as well as the miners PoW reduce the possibility of identity theft and data loss.

3.7 Consensus protocols

The PoW consensus protocol introduced by Bitcoin is a computing power based protocol that enables non trusted nodes on the network to reach consensus as it tolerates Byzantine failure, meaning that some nodes may behave in Byzantine manner. Since then, many other consensus protocols were proposed and developed for blockchains that make use of different techniques to get the desired results and some are designed specifically for use in IoT ecosystems.

On the opposite side of computing power based protocols, are the purely communication based protocols and primarily the PBFT (23), here nodes have equal votes and they communicate with each other many times circularly in order to reach consensus. They are mainly used in private networks as for their operation they assume that all participating nodes are trusted.

All the other proposed protocols are somewhere in the middle of the above two, and potentially they are hybrid versions of them. Below I present the most common protocols (24), (17), (25), (26), (27).

3.7.1 Computing Power Based - PoW

The PoW like protocols demand from miners to solve a cryptographic puzzle so that they prove their legitimacy, safeguarding the functioning of the blockchain based network as described earlier in this paper. The first protocol introduced in Bitcoin adopts SHA-256 to authenticate hash values. The increased computing power required to calculate the needed hash computation has led to the development of designated hardware (ASIC)[1] which accelerate the process. Alternative cryptocurrencies adopted memory-intensive hash functions, i.e. Ethereum uses Dagger-Hashimoto function[2], Zcash uses Equihash[3], Dodgecoin and Litecoin use scrypt[4] and Cryptonight[5] for Monero. These functions are supposed to be resistant to ASIC, as instead of computing power demand

[1] An Application-Specific Integrated Circuit (ASIC) is an integrated circuit (IC) customized for a particular use, rather than intended for general-purpose use. (source: Wikipedia)

[2] Dagger Hashimoto is a proposed spec for the mining algorithm for Ethereum 1.0. Dagger Hashimoto it has two goals: 1) ASIC-resistant 2) Light client verifiability(source: Github)

[3] Equihash is a Proof-of-Work algorithm devised by Alex Biryukov and Dmitry Khovratovich. It is based on a computer science and cryptography concept called the Generalized Birthday Problem. (source: Github)

[4] Scrypt is a password-based key-derivation function created by Colin Percival, originally for the Tarsnap online backup service (source: Wikipedia)

[5] Cryptonight is a memory-hard hash function. It is designed to be inefficiently computable on GPU, FPGA and ASIC architectures. (source: Github)

high memory capacity and are also easy to verify. Recently a Chinese Technological giant Bitmain announced that an Ethereum ASIC miner will be released under the name “Antiminer E3”, and already rumors have arouse that many users propose to execute an Ethereum fork, in other words altering the hash algorithm to keep it ASIC resistant.

The pace of block creation in a chain depends on the difficulty of the cryptographic puzzle, the time for the creation of a new Bitcoin block is set to 10 minutes, other coins like Litecoin and Zcash demand 2-2.5 minutes for the creation of new blocks but the demanded time could not be decreased too much as it could lead to unwanted forks on the chain. Forks lead to unnecessary use of resources as well as to possible double spending issues. Ethereum uses GHOST[6] protocol that enables the creation of new blocks in under a minute without a high impact on its security. The latter might lead to branches on its blockchain, but this is acceptable as long as they don’t contain conflicting transactions.

3.7.2 PBFT variants

One problem of PoW is non-finality. Even if a block is generated, and attached to the chain it has to be extended by many other blocks to be considered confirmed and even then, in case of a fork it may be finally ignored (i.e. Eclipse attack on Bitcoin (28)). Opposite to the probabilistic nature of PoW the PBFT allows no randomness. It was used in Hyperledger (v0.6 – previous version), PBFT guarantees that every block that had been attached to blockchain, is final and there is no way that it would be replaced or altered. It is important to mention though that the pioneer version of this protocol didn’t scale at the required rate and sometimes crashed before leaving the networks boundaries.

There are many other protocols that tried to improve the PBFT, like Tendermint were every node could be granted with unequal voting power, depending on the portion of the network that they possess. Other protocols are Zyzzyva, HoneyBadger and XFT, although.

3.7.3 Proof of Stake

PoS reduces the cost of mining in comparison with PoW as it decides who will create the next block using a combination of different factors such as age and wealth and

[6] Ethereum uses a modified version to that originally proposed by Yonatan Sompolinsky in 2013(source: Github)

random selection (29). Proof of Stake, differently to the above mentioned GHOST, retains a unique branch but alters the difficulty of the puzzle inversely and that means that miners who have a smaller stake in the network, get to solve harder puzzles. In this system, new blocks are referred to as forged or minted and not mined.

Usually in PoS cases, the cryptocoins are generated at the time that the currency launces and the exact number is predefined. So, instead of rewarding the users with newly mined coins, the forgers are rewarded with transaction fees, but in some cases new coin units can be created later and may be given to the forgers as a reward. Nxt, BlackCoin, Peercoin and Lisk are some cryptocurrencies that use the Proof of Stake System.

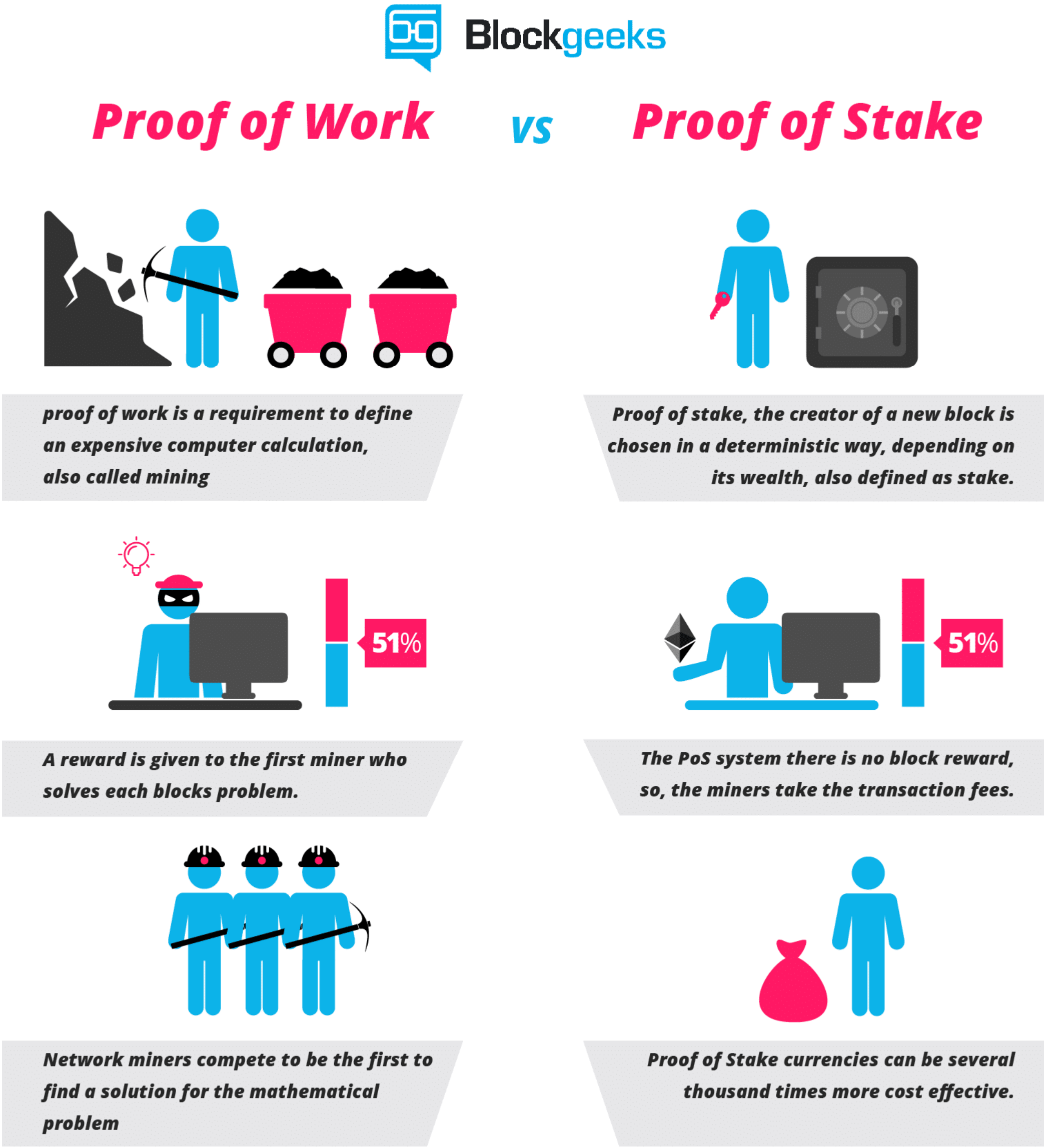

Blockgeeks
Proof of Work
vs
Proof of Stake
proof of work is a requirement to define an expensive computer calculation, also called mining
Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.
51%
A reward is given to the first miner who solves each blocks problem.
51%
The PoS system there is no block reward, so, the miners take the transaction fees.
Network miners compete to be the first to find a solution for the mathematical problem
Proof of Stake currencies can be several thousand times more cost effective.

Figure 6: PoW Vs PoS. source: https://blockgeeks.com/guides/blockchain-consensus/

The processes of validating transactions and creating new blocks require from a forger to put his own coins at stake. By doing this they are allowed to participate in the forging process and since they have their own coins at stake they are hypothetically obliged to validate the right transactions, as differently they may lose their holdings and get banned from the network. Ethereum is about to implement a PoS protocol under the name Casper that will offer to any miner the opportunity to be a validator if they deposit Ethers to the Casper account. Currently there are two implementations of Casper PoS on testnet by Ethereum clients, one in Python and one in Harmony's Java. The process will require from each validator to place a "bet" on whether a specific block will be validated, if it does then he is proportionally rewarded, if it doesn't then he don't get back his deposit, it's wasted. With this technique the systems avoid the problem of having nothing at stake deterring validators from betting on multiple possible branches.

PoS systems are friendlier to the environment as they do not require much electricity or expensive hardware compared to PoW systems. New users are encouraged to join such systems as it is an easy process with low costs and this will result in more decentralization.

3.7.4 Delegated Proof of Stake - DPOS

DPoS - Delegated Proof-of-Stake was firstly introduced by Daniel Larimer, it's a consensus protocol that requires from coin holders to elect "delegates", and these delegates are then tasked with the job to validate the transactions made in the network. It is an alternative to Proof-of-Stake (PoS) model and the miners pay someone to keep the network safe instead of betting their own "money" in order to be able to validate transactions themselves.

The consensus process is pretty different from more traditional mechanisms as the users elect some "witnesses". Witnesses are then obliged to safeguard the generation of new blocks and get paid for doing so. Users can vote for as many witnesses as they want, as long as at least 50% of the users perceive that sufficient decentralization has been achieved regarding the number of elected witnesses. The process of voting for witnesses is perpetual, and that motivates them to complete their function to the highest standard or they risk being replaced.

Apart from witnesses, there are also “delegates” who are elected in a similar manner to them, however, they are responsible for maintaining the network and may even propose changes that should be made to keep it running smoothly. Those changes could be alternation of the size of the blocks, the payment that witnesses should get and transaction fees. The implementation of these changes must then be validated by the users.

Some of the cryptocurrencies that currently use DPoS are EOS, Lisk, Steem, Bitshares and Ark.

3.7.5 Delegated Byzantine Fault Tolerance (dBFT)

The dBFT (Delegated Byzantine Fault Tolerance) algorithm was invented by Erik Zhang, This mechanism similarly to the DPoS demands from stakeholders to elect delegates to represent them and that process is repeated so if the elected delegate is not appropriate he is replaced. A speaker is selected at random among the previously elected delegates, and then he examines the various transactions made by the token holders, and decides to create a new block. He then calculates the hash of the new block and if it matches the hash calculated by the delegates then the block is approved thus being created, else it is discarded. The percentage of the confirming delegates must be no less than 66% or else the creation of the block is not validated. In that case a different speaker is elected and the procedure restarts.

In order for a user to be successful delegate candidate, he must satisfy certain qualifications, such as owning proper hardware, enough coins and use his internet connection specifically and exclusively for this purpose.

3.7.6 Proof of activity

Proof of activity is a hybrid version of PoW and PoS. In proof of activity the miners begin to mine in PoW manner, trying to figure out the solution to the given cryptographic puzzle, faster than the others. The newly mined block, that wins the competition, do not contain transactions but only a header and the reward address of the miner.

For the second stage the system uses PoS, it randomly selects the validators that will sign the fresh block, depending on the information that the header contains. Rich users have increased chances of being chosen as validators. The block is added to the chain at as soon as it is signed by all the validators.

In case not all chosen validators are present and able to sign the new block, a 2nd wining block is chosen and a fresh team of validators is selected. This procedure is repeated until a block receives the demanded signatures. Both the miner and the validators split the collected fee for newly added block.

Proof of activity requires as much energy as proof of work for mining new blocks and on the contrary of PoS, validators have nothing at stake so they are able to double sign. Proof of activity is used by Decred coin.

3.7.7 Proof of burn

Proof of Burn requires from users to send coins in an address where they are irretrievable, literally "burn" them, in order to earn miners rights. The rights do not have an expiration date but they fade, so a user must occasionally burn more coins, to enhance the chances of being randomly chosen by the system to mine new blocks.

The continuous demand for coin burning pushes the mining privileges to the users who burn more money, similar to Bitcoin where the users that spend more money to acquire better equipment get to farm more coins. Also, it is accused of wasting resources without a particular reason.

Only slimcoin uses the PoB protocol, it implements a combination of PoW, PoS and PoB.

3.7.8 Proof of capacity

Proof of capacity relates the chances to be chosen as a miner with the available disk drive space that a user offers to the system. The system creates extensive data sets that are called "plots" that are saved on the miner's disks. The chances for a user to create the next block and collect the reward is proportionate to number of blocks he owns, the more the better.

Some negative aspects of this protocol are that if a user has really high available disk space may create duplicate blocks and fork the chain. Also, Poc does not have any mechanisms to address the nothing at stake issue in order to deter but actors.

Proof of storage and Proof of space are some other variants of Proof of capacity. Currently, only Burstcoin uses a scheme of Proof of capacity.

3.7.9 Proof of elapsed time

PoET was developed by Intel, it operates similarly to the PoW but it requires much less energy. On contrary to PoW the algorithm operates in a trusted execution environment (TEE) like SGX, to make sure that the new blocks are generated randomly, but without the need of the intensive computing calculations.

This protocol relies on the specified wait time assigned by the TEE, and as they claim it can scale without problems to thousands of nodes that use an Intel processor that supports SGX.

3.7.10 Proof of Authority

PoA is a modified version of PoS where instead of the money that a user puts at stake, he puts at stake his own identity. So the list of validators referred to as "authorities", are a group of accounts/nodes that are allowed to take part in the consensus, as long as their digital identities are officially linked to their physical identities. In other words the system must be certain that a validator is exactly who that persons claim he is.

Staking identity means that a user must voluntarily reveal his true identity in order to gain the right of being a validator. This means that the privilidges a user obtains are public and so are any possible malicious actions he may do.

3.7.11 Directed Acyclic Graphs (DAGs)

DAGs serve as consensus mechanisms but they do not implement the traditional blockchain data structure and handle transactions mainly in an asynchronous way. Theoretically they could scale infinitely but early implementations show strengths and weaknesses as all other consensus mechanisms.

NXT was the first community that decided to try and change the chain-like architecture of blocks into a DAG. The blockchain convergence with DAGs originates from the suggestion of using side-chains to where transactions are executed at the same time on different chains according to their type. IoT Chain (ITC), IOTA, and Byteball introduced an alternate way to store transactions without the need of using mined blocks. They suggest that every transaction should be stored in a way that would maintain the sequence of the database.

At the time a transaction is validated, it must be linked to an existing and “fresh” transaction on the DAG network. If it was linked to older transactions every time, it would cause the network to be too wide for validating new transactions. A DAG network should choose an existing validated transaction to link it with a new transaction. The networks width should be kept within a certain range in order to support fast transaction validation.

The DAG mechanisms thus support quick transactions, do not require mining and can support fee-less transactions.

Consensus Protocol	Network Settings	Description
Proof-of-Work (PoW)	Public	Bitcoin make use of proof-of-work that directs to scalability issues. Others are Litecoin, Dogecoin and Ethereum though the latter will migrate to PoS. + we know it works, - slow throughput, high energy demands
Proof-of-Stake (PoS)	Public	Popular implementations are Decred, Peercoin and Ethereum (soon). + low computing cost - Nothing at stake, may cause frequent forks in the chain
DPoS	Public	Popular implementations are Steemit, EOS and Bishares. + Cheap transactions, scalable, energy efficient - Partially centralized
Proof-of-Burn (PoB)	Public	PoB is used by Slimcoin, based on Peercoin. + low computing demads - waste of resources, potentially centralized
Proof of capacity	Public	Burstcoin is the only coin using PoC today + Decentralization, energy efficient, low cost - not tested in real conditions
Delegated Byzantine Fault Tolerance (dBFT)	Public	Neo is the first implementation that uses the dBFT. + high throughput, energy efficient - Partially centralized
Proof-of-Authority (PoA)	Private	Popular implementations are POA.Network, Ethereum Kovan Tesnet and Parity. + high throughput, scalable – centralized sytem
Federated Byzantine Agreement	Federated	Popular implementations are Stellar, Ripple and Dispatch. + high throughput, low cost, scalable - Semi trusted
Directed Acyclic Graphs (DAGs)	Public	Popular implementations are Iota, Hashgraph, Raiblocks/Nano + Network Scalability, low cost - Depends on implementation
Others	Public	Proof-of-Activity, Proof-of- Luck, Proof of Existence, Proof of Security, Proof of Time, Proof of Retrievability etc

Table 5: Summary table of Consensus protocols

3.8 Blockchain present and future applications.

Blockchain technology was introduced through Bitcoin and other cryptocurrencies and enabled the conduction of financial transactions without the need of an intermediate authority, without paying any fees and with exceptional security features. Until today it is believed that the blockchain is immutable, although there had been some incidents that don't always involve insufficiencies of the technology itself but also human mistakes, so it has attracted the interest of many researchers and developers and it is expected to impact many industries in the following years. In addition, some startups have already implemented the blockchain features and advantages in their products such as Slock.it, Shopin and Ripe. Below we present some of the industry sectors that the blockchain technology could influence or transform (30), (31), (32), (33).

Identity

Companies like Onename and Keybase already offer blockchain identities that can be used for verification and sign in apps, websites or as a digital signature. When we buy something online we disclose a great deal of our personal data, regarding our identity personal preferences and many more. The companies acquiring our data often sell them to advertisers, who use them to bomb us with targeted ads. With a blockchain ID similar to an openID you can disclose only the required personal information that is needed to complete each purchase, login etc.

Financial Services

The majority of the financial systems that are used today beside the ones that are powered by crypto currency features are bulky, slow and usually costly. Many users and subsequently many companies believe that the blockchain could be cheaper and more efficient than traditional systems. Initiatives around the globe are taking advantage of the blockchain to introduce and implement tools such as smart bonds and smart contracts. These tools allow automatic payments and are self-executed when pre confined terms are met.

An example is **Asset Management** that can be expensive and risky, especially regarding international transactions. The data are encrypted in the blockchain ledger thus are protected and there is no need for intermediaries.

Regarding **Insurance** the blockchain could allow, as a third-party, users to enroll in customized micro-insurance through social networks when exchanging valuable items through the sharing economy.

Cross-Border payments are another example as there are expensive and could impose dangers such as money laundering and terrorism financing. Companies like Abra, Allign, Commerce and Bitspark already provide blockchain powered remittance services.

Smart Property

Any property like buildings, cars, boats, property titles and shares may be manufactured/issued with embedded smart technology. These records may be saved on the blockchain ledger together with binding directives of those who will be granted access towards this property. In case the property is a house or car, the use of smart keys would offer access to the owner or visitor. Another great advantage of the blockchain technology is that even if a key is lost it could be replaced or replicated from the chain.

Supply chain

Companies already use sensors to track, trace and even check the condition of their products that are in transit. The ledger records the full path of the transferred goods and can prevent delays, added costs and human errors. Also, consumers can be informed before purchasing a product about the route it followed to their hands and protect them against illegal trade or counterfeit products.

Healthcare

Our health records could be encrypted and stored on the ledger and the access would be granted only by the use of a private key. In case of a medical emergency the health practitioners could have access to the patient's health records, securely and from anywhere. Also if the data are stored in a manner that is protecting the privacy of the "patient" they could be used for research purposes. Treatment receipts could be also stored in the ledger and when needed transmitted to the insurance providers.

Music

The music industry has always had problems with piracy, copyright, distribution and transparency. A blockchain database for music rights could help copyright issues and automate purchase of creative work through the use of smart contracts.

Voting

Blockchain technology could provide the security enhancement needed for all elections that are conducted with the assistance of electronic means. Voters should be authenticated and votes should be counted correctly and in an indisputable manner. The ledger can make this possible as governments and voters will have access to data ensuring that no votes were changed, deleted or added illegally.

Decentralized notary

The Blockchains timestamp feature is able to verify the state of data at a specific time. In other words it can prove that something existed for a specific period of time.

Distributed Storage

Currently many users rent storage space in the cloud, services such as Dropbox, Onedrive and many others to securely store their data. The real ownership of the data stored in the cloud and how private they remain in reality is a big question. You don't really know where your data is stored, or who has access on them, and there is always a chance where a government can make the companies disclose this data. Blockchains offer distributed storage protected by encryption and ensure that your data is stored securely and in many places, usually for less fees. Also if a user has extra storage available and not used, he can rent it through platforms like Storj.

Cloud Computing

Blockchain technology can also enable distributed processing features through which the users get paid for renting their CPU capacity. One example is the Golem project that rewards its users with tokens.

Energy management

Traditionally energy management is an industry that is vastly centralized, and in order to buy, sell or generate energy one must come in an agreement with a power company or a reseller. Through the blockchain technology and smart contracts, the prosumers may transact without the need of an intermediate, thus reducing costs.

Charity-Crowdfunding

The benefits of blockchains, could enhance charity procedures as a donor can track and verify where exactly his money end up. Also regarding crowdfunding this technology enables individual investors to participate in crowdfunded projects, from movie productions to real estate and startup business (OpenLedger), as their deposits are recorded in the ledger permanently associated with the project and is sure to receive their payment if it ends up a success.

3.8.1 Smart Cities

One of the most intriguing future challenges is securing the so called smart cities. During the previous years they have been called by various names, such as intelligent cities, knowledge cities or ubiquitous cities. Whatever they are called the idea of being a smart city relies not just to the fact that they use cutting edge technology, but that they do so in order to confront the rise of urbanization. Sooner or later big cities will have to deal with various problems such as poor resources of electricity and water, slow government services, high cost of living, high traffic and crowded public transportation and other pollution issues.

Though the blockchain technology cannot affect directly all the above mentioned issues, it may play an important role in securing the smart cities digital services and support the natural growth of the "sharing economy" that will immerge by the exponential spread of IoT. It is said that data is the new currency and towards that way the blockchain could offer a secure and automated procedure to buy and sell data without compromising security and privacy.

The authors of (34) sum up the attributes of the administration and of sharing services and computing that are based on the blockchain technology through the triangle framework of service orientation (Zhao et al. 2008). The service relationships between humans, technology and organization are divided in six categories (figure 8), every pointer shows a category of service relationship, the administration of blockchain-based sharing services primarily handles people oriented relationships, on the other hand computing of blockchain based sharing services mainly handles technology oriented relationships.

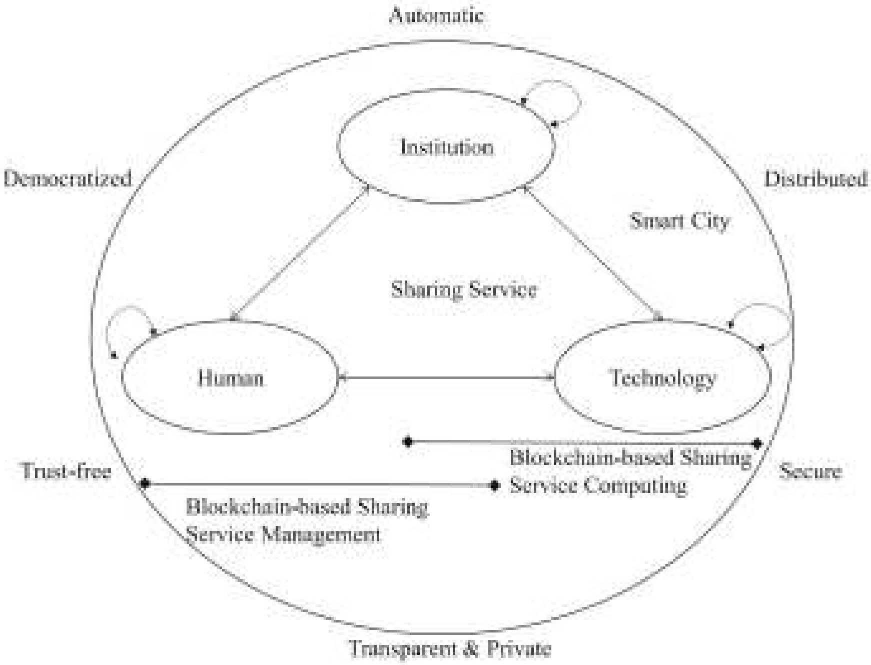


Figure 7: Features of the management and computing of blockchain-based sharing services
Source : Blockchain-based sharing services:What blockchain technology can contribute to smart cities (34)

Smart payments are probably the most important feature of a sharing economy. As we have already mentioned the blockchain enabled smart contracts will allow the trading of data gathered by various sensors automatically and the fee could be either just other data or a predefined currency. For example, Nokia already launched a project called Sensing as a Service (SEaaS), where various sensors spread in cities exchange or sell data and the payments are made automatically through their blockchain. Of course, smart payments could also be enrolled to pay for city programs, assistance, tolls, parking, welfare, payroll, etc.

Other areas that could be affected are all government services (voting, taxes, ownership etc), smart energy (on demand powering of public facilities or energy trading by individuals), identity, transportation and waste management.

4. Enhancing IoT security with Blockchain technology

As mentioned in chapter 3.7 the possible uses of the BlockcChain technology seem to be endless and it is expected to affect many industries, and utterly transform services as we know it. Regarding IoT networks it is very difficult to achieve high security nowadays as the variety of IoT devices and the potential exploitation of their purely designed security features gives breeding ground to attackers.

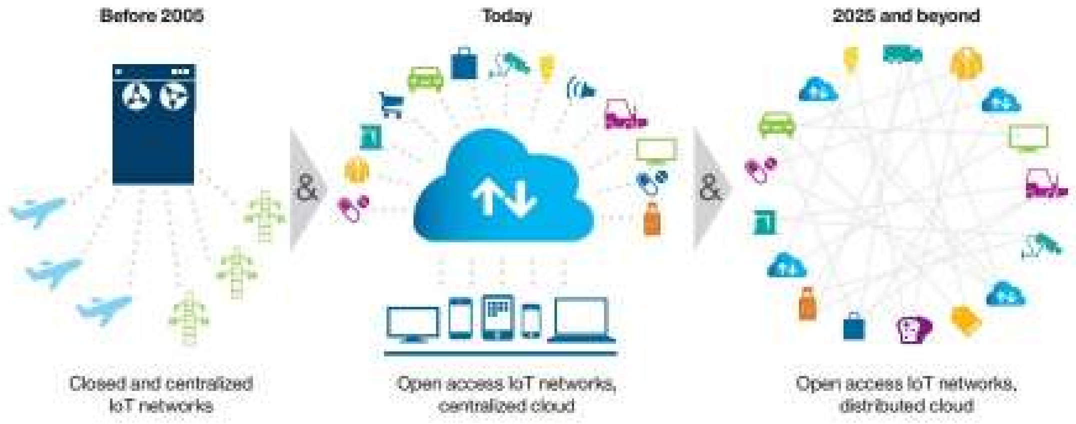

Before 2005
Today
2025 and beyond
&
&
Closed and centralized IoT networks
Open access IoT networks, centralized cloud
Open access IoT networks, distributed cloud

Figure 8: The IoT network infrastructure past/present/feature
Source:http://www.ibmbigdatahub.com/blog/what-blockchain-and-what-does-it-have-do-internet-things

Current trends for securing the IoT network are mostly centralized models that are costly and non interoperable. The increased demand and production of new devices can make privacy and trust more difficult to achieve. Security deficiencies in the IoT may lead to malicious attacks on authentication and secrecy, silent attacks on service integrity, or network availability attacks, i.e. Denial of Service (DoS). Privacy and anonymity are also really important for IoT users and they should be considered thoroughly when designing such devices or network architectures, users should be provided with proper tools to protect their privacy. IoTs security is a really complex issue and the proposals for strengthening it vary, but one of the most intriguing tendencies is the use of Blockchain technology to address this issue. Some of the key challenges that need to be dealt with are the absence of a basic authority instrument, diverseness of specifications and capabilities of most current IoT devices, huge surface range vulnerable to attacks, risks associated to context and also scale issues.

4.1 What the Blockchain technology can offer to IoT.

Millions of new devices are purchased and connected in IoT's networks in daily basis. The risks that are emerging include not only digital instances of our lives but also physical ones, i.e. locks and other security systems of our houses or our cars, may be hacked putting us into physical danger. One more problem is the fact that there are perhaps too many protocols and interfaces (web, cloud, mobile) in IoT's ecosystem in order to allow devices and sensors to interconnect that are handled by different applications. Handling the excessive amount of data produced by the daily (24/7) functioning of IoT devices is a really difficult task. Here it is important to mention that despite the fact that IoT produces huge amounts of data, in many cases they are considered to be highly valuable for real time exploitation but have less value afterwards, and this is a factor that may eventually allow the use of a blockchain like or inspired solution in the forthcoming years. Dealing with the imminent complexity of the management of the hundreds of devices that are expected to connect in IoT networks soon, is also a really hard task.

In chapter 3.6 we presented some of the main advantages of the BlockChain technology. Here we will emphasize in the benefits that the implementation of the Blockchain technology has to offer to IoT's security (17), (35), (36), (37), (38).

Decentralization: The use of blockchains will allow the IoT networks to disembark from centralized data centers approaches and verify transactions through the distributed ledger. Distributed cloud data storage will allow data to be stored in multiple nodes eliminating the threat of Single Point of Failure. The adaptation of a standardized P2P scheme to handle the millions of transactions that will be required among IoT devices will cut down the required economic resources that will be needed to make and preserve big centric data centers as computing and storage needs will be distributed to countless devices that are part of an IoT network. The conducted transactions will be self validated and they will also have the authority to ensure that they will not bypass any set constraints.

Transparency: A blockchain based approach for data storage and transaction processing, makes it virtually impossible for any vicious user to alter the recorded data. In a public blockchain certain data parts on the ledger regarding transactions and records are visible to all the participants and if one tries to alter or delete something he will be noticed.

Privacy: In current blockchain implementations every user manages his keys (public, private) and on a given node are recorded encrypted copies of the user's data. This enables an integrated rate of privacy as the data are always under the users control and no one else can access them. Especially regarding IoT devices intercommunication that usually involves wireless communications between interacting nodes, blockchain's cryptography and validation safeguards the procedure.

Security: The security benefits of the blockchain technology are of proved value as they served Bitcoin and other cryptocurrencies over the past years, with no issues regarding the technology itself as most of the succeeded attacks exploited other parameters such as user carelessness and software bugs. In IoT the firmware of any device could be stored as a cryptographic hash in a private blockchain ensuring its integrity, and that could be used as an extra measure before it is allowed to interact further. Access and identity management systems that base their functioning on a Blockchain can delegate IP address forgery or spoofing and prevent any non trusted or fake device from connecting to the network. Its decentralized nature as mentioned before will help avoid the consequences of attacks in cloud servers. The blockchain ledger can only be extended and not altered, and that gives such a huge advantage over many possible attacks. This feature is also crucial to support stricter compliance and regulatory requirements of industrial IoT applications in a decentralized scheme. The constant verification of transactions is also a big plus in security as all are cryptographically signed and verified, excluding possible malicious users.

Improve of QoS: Blockchains can enable on demand usage of resources just by executing the equivalent algorithm that links to the associated smart contract, and instruct payment after the completion of the requested service. Consequently, aided by the traceability feature of the blockchain we can verify that the use of resources has met the agreement terms between the client and the provider.

Reduced fees: The P2P nature of the blockchain will allow transactions to be completed without the need of an intermediate authority, and transaction costs could be reduced or even eliminated. Another example apart from transactions is storage, where distributed blockchain storage could cost significantly less than those provided by major cloud storage companies.

Automatic transactions: The use of blockchain will enable smart devices to work actually autonomously as they will automatically exchange data and execute financial transactions without the need of a centralized authority or constant tuning by the owner-user. The blockchain will verify that a transaction is valid by following the principles that the nodes have to follow to reach consensus on the network. For instance, smart devices such as fridges could automatically place orders on online supermarkets for the products that are needed, or a smart car that will be able to produce a complete report of the parts that needs replacement when prompted in a garage.

4.2 Challenges to be met and overcome enabling convergence

The blockchain technology has attracted great interest from many sources, we have already mentioned many of the industry fields that find its features attractive and try to embed it in their own implementations. The blockchain unique attributes as mentioned in the previous section make it a really promising solution to face the growing IoT security challenges. However, there are many matters that have to be resolved to make such a convergence feasible. This is due to the fact that current usage of the blockchain, and the field that the technology has proved its worth, is primarily in the Bitcoin and all other cryptocurrencies that despite their divergences in order to function securely and independently require confined resources and doesn’t include lower computing capability devices in the networks topology. In IoT though, it is estimated that the amount of the devices that will be interconnected will increase too many billions in the forthcoming years and their computing capabilities will not resemble those used in cryptocurrency chains. Below we will try to present a thorough evaluation of the problems that must be addressed to enable the efficient use of Blockchain technology for securing IoT (16), (18), (17), (39).

Complex consensus algorithms: The algorithms that are used to succeed consensus in Blockchains (POW and POS) demand moderate to high computing resources, and that is not the case in the majority of IoT devices, as they usually have limited computing resources.

Storage: In cryptocurrency implementations of the blockchain technology, the ledger is stored on the nodes themselves, but the vast number of transactions that are expected to be generated by the millions of IoT devices will escalate the size of the ledger proportionally and will be beyond the capabilities of most smart devices.

Scalability: Typical blockchains are designed in such a way were every block is broadcasted and also has to be validated by every node that participates in the network. This process creates major scalability matters as the broadcasted data and computing needs will rise dramatically since the amount of participating nodes would increase as well. The associated overheads would pose a hard to solve puzzle as the larger portion of IoT devices have limited bandwidth connections and processing capabilities.

Latency: In cryptocurrencies the confirmation and verification of a transaction doesn't have strict time limits to complete. For example in Bitcoin paradigm a transaction may take up to 30 minutes to complete. In IoT applications however this is a major problem as for example if you are using a blockchain based smart lock to get in your house, you can't stand outside the door and wait for the lock to open for such a long time.

Security overheads: In traditional blockchain implementations there are some compute-intensive security procedures to avoid double spending. These mechanisms are crucial for the correct function of cryptocurrencies blockchains but not much needed in the IoT scenario.

Throughput: The term throughput in Blockchains stands for the number of transactions that are considered completed and verified and can be stored on the chain ledger in a specific time period. For instance, Bitcoins throughput is somewhere around 5-7 transactions per second and Ethereum supports up to 15 per second, while currently VISA processes and verifies almost 2000 transactions per second. Taking under consideration that the amount of the devices that are estimated to connect into IoT networks will increase exponentially in the forthcoming years, it is obvious that this is not sufficient.

Sustainability: The required energy for the proper functioning of the current blockchain implementations especially in cryptocurrencies require colossal amounts of energy. It is estimated that in order for the Bitcoin network to successfully process and verify 5-7 transactions per second, it requires 32 terawatt hours of electricity every year, about as much as consumed by the country of Denmark. An estimated escalation to the number of transactions that an IoT network would require is not possible from either a technical or energy perspective.

Behavior change: The Blockchains have introduced a way for entities to transact without the need of an incarnated third authority. So the users have to acclimatize in a new world were their daily electronic transactions, not just financial, are completed securely without the need of an intermediate company like Visa and Mastercard, which in many people's minds pose a trusted pillar were they can turn to for help and auditability issues.

Bootstraping: If we want to use smart contracts for all our arrangements and agreements and also use the Blockchain ledger as a notary, the transition of all existing contracts, business or personal documents would require a strenuous migration procedure, with possibly high costs in time and money.

Government Regulations: If the Blockchain based transactions propagate widely, it will force the governments around the world to take new measures that will allow them to monitor and regulate the industry for compliance. Currently there is no legal framework to follow, and this is certainly a problem from manufacturers and service providers. Regarding smart contracts, their enforceability is still limited and not legally binding to all parties, and there is always the danger were a transacting entity doesn't recognize the result of an automated smart contract despite the verifiability of it through the pre determined process. A way to work around this problem is by including a reference of the physical instance into the smart contract and this method is known as dual integration (40).

Illegal Activities: The anonymity offered by a blockchain based transaction system can be enticing to "malicious" users who try to exploit this feature to conduct illegal activities. The ability to move valuable assets or cryptocoins anonymously and quickly can make misdeeds such as money laundering and trafficking an easy task. As mentioned before, with proper regulations and technology support, legal authorities will be capable to monitor and prosecute such illegal actions.

Quantum Computing: One of the strongest aspects of the Blockchain technology is that the cryptographic puzzle that a miner has to solve needs high computing resources, thus making it hard for a single user to influence an established network of thousands of nodes. But with the use of quantum computing (41) the latter could be possible, through cracking the cryptographic keys in a reasonable time with a brute force attack, and the procedure of voting – consensus could be manipulated.

Maintaining Privacy: We have discussed earlier that each user who participates in a blockchain network and each device participating in an IoT BC enabled network, is spotted from their public key or its cryptographic hash. In public blockchain networks each user doesn't have to know the keys of all the entities in it but only the one of their transacting counterpart. But, as all transactions are made publicly, by analyzing this data a "curious" user may identify patterns and identify links between addresses, managing to make informed guesses about the true identity of a user. Companies, already offer such tools such as Elliptic (42) that developed software to monitor and track possible illegal activities in Bitcoin blockchain. However there are ways to mitigate this at some degree, by using a different private key in each transaction for public networks and by using different blockchains for each set of transactions that need to be done with a specific user in a private network.

Malicious Miners: Due to PoW, miners are not capable of completing fabricated transactions or alter the blockchain contents. However, they are able to block new transactions from being validated and inserted into the chain by blacklisting them if they have control over enough Byzantine nodes as the tolerance of consensus mechanism is limited against it. So a big problem arises when a user decides not to follow the rules that the rest of the participants do.

Autonomy: The autonomy provided by a public blockchain network is considered to be a valuable feature, but one should be very careful when using i.e. smart contracts as many dangers may impose if you don't exactly know what you are doing. The programming of a smart contract should be done thoroughly and a fail-safe mechanism should be used to prevent dead ends. A smart contracts functioning could be altered depending on the inputs it receives. Also, a privileged user may be allowed to damage it and eventually delete it. If such features aren't included originally in the programming of the contract, then this can never be altered and though it is not necessarily a bad thing if it is programmed the wrong way any mistaken call to its functions will probably cause errors that can't be repaired. Moreover, any possible programming faults can cause the contract to be irreversibly "damaged" and a user may lose all its containing assets. This is another autonomy generated issue and it adds up with the possible loss of a user's private key that would utterly lock him out of his own "wallet".

Adoption: Currently there is a lack of maturity and standards and it is not possible to achieve interoperability among developing blockchain based implementations for IoT.

Another factor is that billions of smart devices are already available in the market, manufactured by different industries with different standards making the possibility for convergence cloudy. The architecture design of such networks should have the ability to properly readjust its functions into a possibly changing environment and escalate them accordingly in order to successfully deal with the continuously growing demands of the industry.

4.2.1 Cryptokitties, a dApp that overwhelmed Ethereum Network

Cryptokitties is an online blockchain-based game built on top of Ethereum that offers users the ability to buy, sell and breed virtual cats. It came online on November 28, 2018 and in a very short time became the most popular smart contract that is estimated to have reached up to 20% of all transactions traffic on the Ethereum network. The result of this unexpected popularity of the game was to clog the Ethereum network, increasing the time needed to complete transactions for all the users of the blockchain.

It is interesting to mention that one of the reasons AxiomZen developed this kind of game was to give the opportunity to the users to interact with the blockchain technology in a simplified and easy way, aiming to promote the adoption of the technology and inform average users of the types of applications that it can support.

After the launch of the game, new blocks became 100% full and the number of pending transactions reached almost 30,000, to avoid a complete collapse either users would be forced to increase gas prices[7] or miners to suffer from a massive increase in the default gas limit[8]. As the Ethereum throughput is estimated to cap at around 15 transactions/per second the sudden success of the game could be devastating for Ethereum. The result was as mentioned above that the miners increased the gas price, making transactions more expensive and that made the fee needed to buy the cryptokitties to cost more that the kitty (digital asset) itself.

[7] measure of computational effort

[8] Every transaction has a gas limit reference that sets the highest price (gas) that the trader will pay for. So if the amount of the required gas caps the amount that was set by the buyer while the procedure has not concluded the system immediately stops the procedure. In this case the trader is obliged to pay for the computing procedure that took place, however there is a mechanism that protects them from exhausting all their funds. Blocks also, have such a reference for gas limit and it is used to specify the highest load of gas that the entire block will be permitted to consume, combining the gas that was needed to conclude all of its transactions.

Despite the fact that the popularity of the game went down and it's developers made some corrections to the code to cut the transactions needed in half, the games explosion highlighted an important weakness of the Ethereum ecosystem that just gives us an indication of the potential problems that could be aroused by trying to adopt blockchain technology to secure IoT ecosystems.

4.3 Tools that could be used to aid convergence.

The convergence of IoT and blockchain technology will not be acquired easily and though the potential benefits appear to be really promising, as we seen in the previous chapter there are several issues to mitigate and make this possible. Several tools had been proposed that aim to assist this possibility and make it feasible (25).

4.3.1 Trusted Hardware

The need for faster consensus mechanisms in blockchain based networks has led some developers to use trusted hardware devices taking advantage of the trusted computing technology. Such examples are Intel's SGX and ARM's TrustZone, these implementations improve performance without losing much regarding security. Proof of elapsed time (PoET) was introduced by Sawtooth Lake to replace PoW. TownCrier (43) uses SGX for creating a credible base to evaluate incoming data sources and allow them to be imported into the blockchain. The above mentioned schemes base their functions on a weaker trust models than those used in plain cryptographic systems. The security of such systems depends on a trusted computing base (TCB) that operates on the trusted hardware.

Every system that relies its functioning on trusted hardware uses remote attestation protocols. It is a public – private key pair that is called **Endorsement Key** (EK), the private key is burnt into each device during manufacturing and it is never visible outside of the trusted hardware. As the EK can only be used for encryption, the possession of a private key can only be proved indirectly, by decrypting data that where encrypted with the public pair of the EK.

Endorsement key ensures trusted communications and it enables the creation of temporary keys. Before any data is loaded, it is measured by hashing the content and then it is digitally signed and sent to a remote party. The remote party verifies the received hash and checks that it corresponds to approved sources. This protocol requires that the certificate authority maintains an updated list of valid certificates. An EK is much more constrained from general RSA keys, as it can only be used by the trusted hardware to decrypt very specific structures.

The use of trusted devices may enable really high transaction rates as it eliminates the need for a resource demanding consensus algorithm. Their use is estimated to significantly help securing IoT ecosystems, but for this to be possible certain standards should be established so as to support interconnectivity and interoperability between different manufacturer's implementations.

4.3.2 Thin Clients

Thin clients are lightweight computers, optimized for functioning in a server-based computing environment. The linked server is tasked with more computational demanding tasks like running applications and storing data. Thin clients foremost are elements of larger computational frameworks, whose servers are used to lighten the clients workloads. This scheme defines what we refer to as cloud-based systems, in which its clients have to access central data centers and make use of their resources. The main advantages of this model are proper use of hardware resources, easier software updates, and enhanced surveillance (44).

Regarding Blockchain technology implementations thin clients have already been introduced by Bitcoin. There thin clients are some kind of Bitcoin wallet programs that connect to Bitcoins network but they do not verify transactions or blocks, meaning that they do not act as clients for the networks nodes. They do not store the whole Blockchain ledger on their hard drive but they usually adopt the Simplified Payment Validation (SPV) mechanism in order to certify that validated transactions have been permanently written on blocks. To achieve that, thin clients reach to a single peer server of the Bitcoin network and query it by sending a Bloom filter that matches all the transactions that involve every address of the wallet of the client.

After a block is mined, validated and confirmed, the thin client asks for a lightweight version of it that is known as a Merkle block. The latter contains a block header, some hash values, single-bit flags and the ascending number of the transaction. With this data, that usually do not exceed 1KB, clients are able to create a partial Merkle tree. In case the root nodes hash that is stored in the partial Merkle tree is the same as the block headers hash of the merkle root, thin clients have verification that proofs the presence of the transaction in the specific block. After that it needs to get six affirmations, before there is a change at the networks state, and when it receives them it is almost certain for the validity of the transaction that is added into the blockchain network (45).

Though more vulnerable to the problem of double spending, they are more potent regarding storage use, bandwidth and transactions throughput. With that said, they are more suitable for smartphones and other space limited devices. But, the majority of current thin clients cannot guarantee privacy as they have to communicate the IP address plus the addresses linked with the wallet of the user to the SPV server.

Appropriately designed thin clients could be used in IoT ecosystems, as they could solve the problem that most smart devices have, and that is limited capabilities (storage, computing power, bandwidth connections) and enable them to be part and interact in a secure blockchain based IoT network.

4.3.3 Sharding

The current blockchain protocols store in each node all the states i.e. account balances, contract code and storage and also each node processes all transactions. This model has proved its security features are of the highest grade but it also very deterring towards scalability. This is due to the fact that a blockchain can only process simultaneously as many transactions as a single node can. This among others limits the transactions throughput for Bitcoin to 3-7 per second and Ethereum to 7-15.

The concept of sharding is that instead of using all nodes to verify each transaction we could use only a small subset of nodes to do the job. This would require putting some rules such as, what percentage of network nodes should be considered sufficient to verify securely each transaction. If this implementation's security proves to be sufficient then we would have greatly increased the blockchains throughput as the blockchain will be able to validate at the same time as many transactions as the number of sharded subsets of nodes.

Ethereum is the most know blockchain platform that tries to materialize this idea (46). Other sharding proposals are the ELASTICO sharding protocol (47), Zilliqa (48) and the Merklix tree (49) (proposed for Bitcoin) that will try to shard the transaction processing or the data state. Previous mentioned approaches just solve half of the problem as we want to be able to process thousands of transactions without requiring from each node to have extreme computing resources and also without expecting from every node to save large amounts of state data. It would require one complete approach in which the workloads of processing, downloading and re-broadcasting transactions and also the data state repository, would be disseminated to the networks nodes (50).

4.3.4 Fog and Mist Computing

The rise of fog computing seems in many ways seems to be a natural evolvement as it extends cloud computing and brings computing capabilities to the IoT's networks limits where data is created and acted upon. It can be described as a distributed framework that has significant computing capabilities as it has powerful hardware devices that are interconnected. This devices are called fog nodes and it can be anything that has computing capabilities, storage and network connectivity, such as industrial controllers, switches, routers etc (51), (52), (53) (54), (55).

Considering the burst of the number of available IoT devices, sending large amounts of unprocessed IoT data to the cloud requires the use of gigabytes of network traffic and increases latency issues. By processing this data closer to the location that they were generated, we can mitigate these problems as latency issues are far less noticeable, core network is relieved from unnecessary traffic and sensitive data are kept inside the local network. This way we can have real time or near real time data assessment and send to the cloud only the information that are needed, without worrying about delays. But, even in this case scenario the issues of huge data traffic and energy consumption needs could be significant enough to cause problems and many researchers try to find ways to mitigate and minimize them. Such like initiatives are found for example in the work of (56) (57) were researchers propose algorithms to tackle these problems, indicating at the same time how difficult it is to address latency or energy consumption issues without significantly degrading one, when targeting the other.

Cisco is the first company that introduced the Fog computing term, and suggested that the fog layer could reduce the latency in hybrid cloud scenarios but later realized its possible implementations in IoT ecosystems. In 2015, major cloud infrastructure vendors (ARM, Cisco, Dell, Intel, Microsoft) formed the OpenFogConsortium in order to create a cross-industry model that would enable end to end IoT deployments.

Fog computing allows the analysis of data closer to their source and in many cases (industrial implementations, autonomous driving and healthcare) this prospect is invaluable as if an occurred incident is not address properly and in the mentioned cases in a matter of milliseconds it could be disastrous.

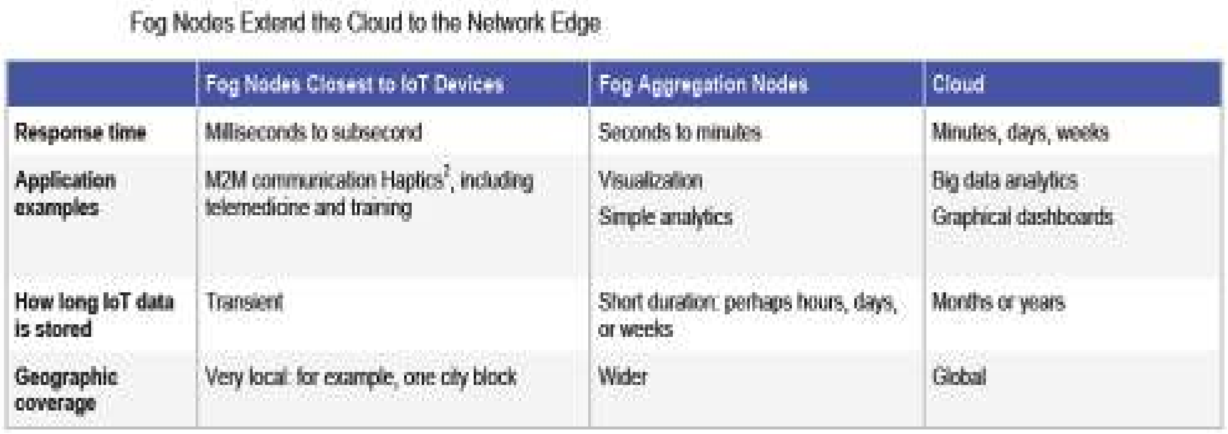
Fog computing key characteristics are minimum latency, high scalability, proper distribution, interoperability, flexibility, decreased network traffic, heterogeneity and swiftness of the clustered fog nodes.

Monica Paolini, president of Senza Fili Consulting, wrote on LinkedIn, “In recent years, there has been a strong push to move everything to a centralized cloud, enabled by virtualization and driven by the need to cut costs, reduce the time to market for new services, and increase flexibility. In the process, we lost sight of how important the location of functionality is to performance, efficient use of network resources and subscriber experience. Physical distance inevitably increases latency.”

4.3.4.1 How it works?

Programmers create IoT apps specifically address to the fog nodes at the networks limits. Then the transmitted data from IoT devices are gathered by the closest fog node, and the IoT application appropriately distributes them for analysis according to their type, Figure 9.

Usually the closest fog node processes the most sensitive data and leaves the lesser ones to be analyzed within a time frame of several minutes. These are transmitted to a gathering node for processing. Data that don’t require instant or nearly instant analysis are transmitted for archiving and analysis.



Fog Nodes Extend the Cloud to the Network Edge

	Fog Nodes Closest to IoT Devices	Fog Aggregation Nodes	Cloud
Response time	Milliseconds to subsecond	Seconds to minutes	Minutes, days, weeks
Application examples	M2M communication Haptics[2], including telemedicine and training	Visualization Simple analytics	Big data analytics Graphical dashboards
How long IoT data is stored	Transient	Short duration: perhaps hours, days, or weeks	Months or years
Geographic coverage	Very local: for example, one city block	Wider	Global

Figure 9. (Source: Cisco)

4.3.4.2 Mist Computing

Fog computing reduces transmission costs, latency and potentially security, but the increased demand for geographically scattered, low-latency computational resources led to the creation of tailor made nodes that have lower computing resources but specific commitments. They are less powerful fog nodes and are known as mist nodes. These nodes form mist computing layer and are used as an intermediate between IoT devices and higher-end fog nodes, and are usually placed next to the smart end - devices they service.

The whole concept of mist computing is that there is computing power on the extreme edges of the network, on the actual sensors of the device. The computing power of those end devices is usually the microchips or micro-controllers embedded on the device. And this is why their processing capability is much more limited than that of the fog nodes.

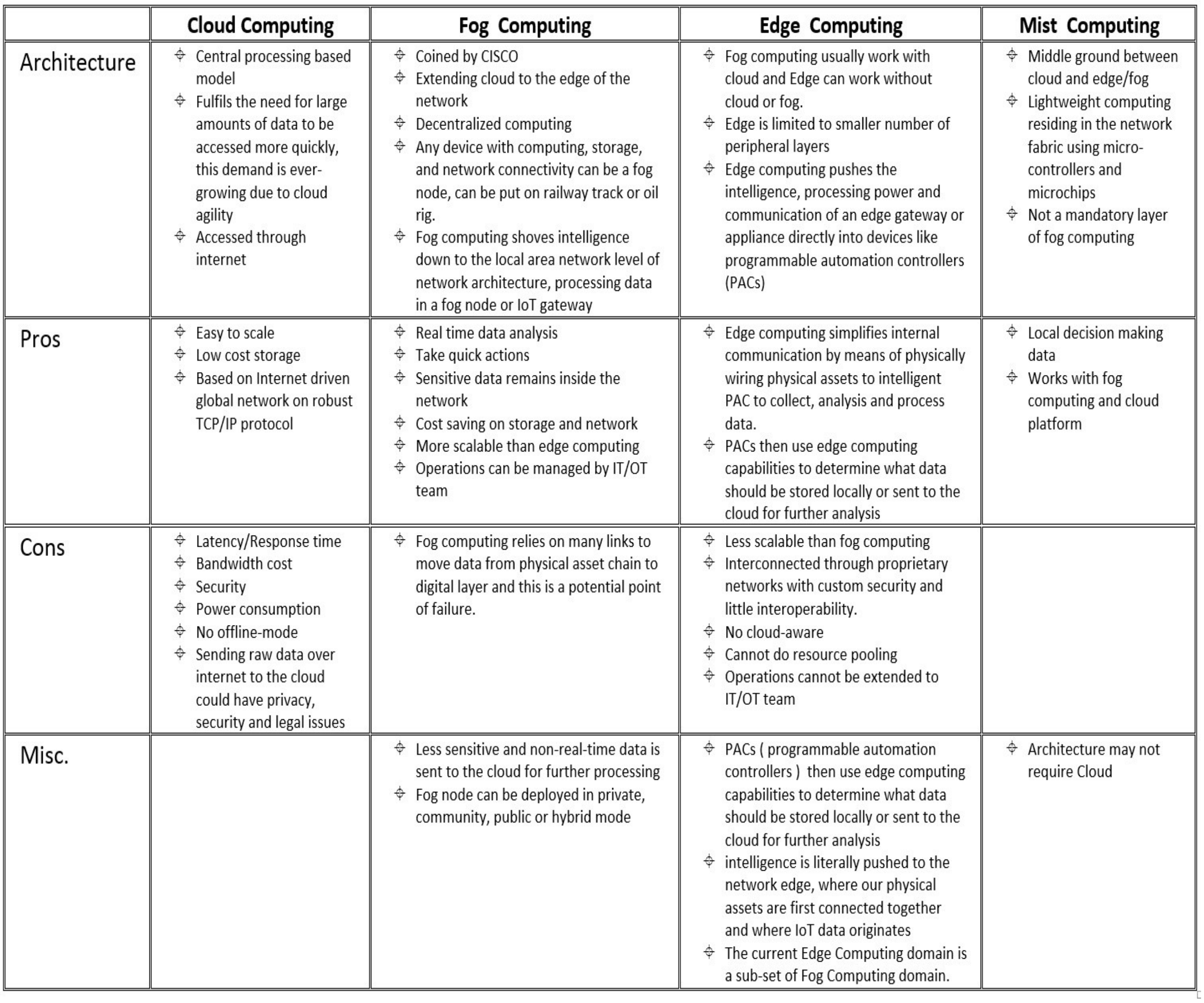
Mist computing network is a subnet of the fog computing network and its architecture is designed according to the application demands that operate over it. How far the information generated through it travels depends as well on the needs of the application, but often the information is only reaching as far as the Fog computing layer.

4.3.4.3 Edge Computing

Often many people confuse Fog computing with Edge Computing, as both schemes are pushing processing capabilities and analysis towards the edge of the network, but there are key differences between them.

In Edge computing each device may play the role of a fog node as it can decide which information should be transmitted to the cloud and which should be locally analyzed. This is made possible by connecting the sensors to a PAC – Programmable Automation Controller that executes the tasks of processing and communications.

So if we try to explain it further, in edge computing the devices that are collecting the data do the processing and analysis themselves, i.e. sensors in a self-driving car analyze the data locally to achieve real time responses so as to avoid accidents. In fog computing we have intermediate nodes that are able to process and analyze data or send them to the cloud for analysis.



	Cloud Computing	Fog Computing	Edge Computing	Mist Computing
Architecture	Central processing based model Fulfils the need for large amounts of data to be accessed more quickly, this demand is ever-growing due to cloud agility Accessed through internet	Coined by CISCO Extending cloud to the edge of the network Decentralized computing Any device with computing, storage, and network connectivity can be a fog node, can be put on railway track or oil rig. Fog computing shoves intelligence down to the local area network level of network architecture, processing data in a fog node or IoT gateway	Fog computing usually work with cloud and Edge can work without cloud or fog. Edge is limited to smaller number of peripheral layers Edge computing pushes the intelligence, processing power and communication of an edge gateway or appliance directly into devices like programmable automation controllers (PACs)	Middle ground between cloud and edge/fog Lightweight computing residing in the network fabric using micro-controllers and microchips Not a mandatory layer of fog computing
Pros	Easy to scale Low cost storage Based on Internet driven global network on robust TCP/IP protocol	Real time data analysis Take quick actions Sensitive data remains inside the network Cost saving on storage and network More scalable than edge computing Operations can be managed by IT/OT team	Edge computing simplifies internal communication by means of physically wiring physical assets to intelligent PAC to collect, analysis and process data. PACs then use edge computing capabilities to determine what data should be stored locally or sent to the cloud for further analysis	Local decision making data Works with fog computing and cloud platform
Cons	Latency/Response time Bandwidth cost Security Power consumption No offline-mode Sending raw data over internet to the cloud could have privacy, security and legal issues	Fog computing relies on many links to move data from physical asset chain to digital layer and this is a potential point of failure.	Less scalable than fog computing Interconnected through proprietary networks with custom security and little interoperability. No cloud-aware Cannot do resource pooling Operations cannot be extended to IT/OT team	
Misc.		Less sensitive and non-real-time data is sent to the cloud for further processing Fog node can be deployed in private, community, public or hybrid mode	PACs (programmable automation controllers) then use edge computing capabilities to determine what data should be stored locally or sent to the cloud for further analysis intelligence is literally pushed to the network edge, where our physical assets are first connected together and where IoT data originates The current Edge Computing domain is a sub-set of Fog Computing domain.	Architecture may not require Cloud

Figure 10: Difference Between Cloud, Fog, Edge and Mist Computing
source:https://medium.com/@YogeshMalik/fog-computing-edge-computing-mist-computing-cloud-computing-fluid-computing-ed965617d8f3

4.3.5 SDN and NFV

Another prospective is the exploitation of technologies such as Software Defined Network (SDN) and Network Functions Virtualization (NFV) that will offer a cheaper software defined solution to manage networks in comparison with current high-cost hardware methods, as it will offer the ability to apply rules to unique devices or over entire networks or even create distinct network domains powered by a virtual network layer, that will enhance security i.e by segmenting the network and reduce breach impacts. Also, with the use of SDN-enabled adapters it will be possible to isolate end devices and dynamic policies can be implemented in real-time, i.e. portable devices will connect to the network faster and download new policies automatically. Moreover, an enterprise may govern bandwidth needs by using SDNs elastic nature to redirect networks traffic when needed.

5. Approaches converging IoT with Blockchain Technology.

5.1 Already launched products

The integration of Blockchain technology with IoT has already started and some companies have delivered products and services that make use of this technology to enhance services and increase the security of transactions and communications. Below I present briefly two of the first companies that have such products available for consumers – businesses.

5.1.1 Filament

Filament started as one of the many companies in the field, aiming to integrate the blockchain technology to the Internet of Things, their first goal was to leverage the bitcoin blockchain so as to create unique identifiers for specific devices. Today Filament sell hardware systems and software applications that provide secure interactive communication-transactions between machines and devices based on a blockchain network.

Filament offers a pioneer Blocklet™ USB Device that enables current industrial machines to interact and execute transactions on blockchain networks, and is also planning to release their so called Blocklet Chip™ that is a Trusted Execution Environment for IoT that has low power requirements and at a low cost. Moreover, their Blocklet software is a secure contract system designed for embedded devices. This software administers a chain-of-custody garbled scheme throughout the whole path from stand alone devices via printed circuit board (PCB) assemblies, device manufacturing, shipment to clients and on-site support (58).

They use techniques to enhance privacy i.e. communities of devices, that restrict malicious users from gaining access to sensitive information regarding interactions among devices. Every device in a Filament network is able to interact and transact with other devices without having to connect to a server or to the cloud. The devices can complete transactions by using various value metrics such as cryptocurrencies, network access, data, arrangements for current services, certified handshakes for new devices etc.

The key technologies and methods that are used by Filament are the following as described in their webpage (58):

Telehash offers communication among credible devices, without worrying about the nature of the transmitting network (Ethernet, Wifi, UHF etc.), it achieves that by deploying sophisticated encryption and public key cryptography to make sure that all transmitted data remain private and secure.

"TMesh is a method for self-forming mesh networks over radio links; it provides encoding of communications data into radio parameters, shared management of available spectrum among any number of devices, and establishment of networking relationships among those devices."

"Blockname is a technique for decentralized resolution of endpoint addresses in electronic communication using the Bitcoin blockchain and public notaries to verify the authenticity of name/address bindings".

"Blocklet is an electronic accounting system that builds upon the blockchain to provide autonomous, decentralized equivalents of traditional methods for commercial transactions, including contracts, agreements, receipts, and escrow arrangements".

The distributed blockchain features of Filament take advantage of open protocols and enable devices to process and record transactions independently by providing digital trust. The Blocklet software combined with the Blocklet Chip(Beta) will allow the communication and interaction of Filament enabled devices with multiple blockchain technologies natively. The Blocklet Chip will enable industries to use their data and conclude transactions at the edge of the network.

Filament, currently cooperates with other partners on other promising implementations aiming to create a platform for future industry blockchain projects. An example is the open-source business blockchain framework, Hyperledger Sawtooth, that is hosted by The Linux Foundation, on its own native hardware. Hyperledger Sawtooth is a platform that was created for constructing, implementing and executing adaptable and extensible distributed databases that securely holds digital files in an environment that has no supervising authority[9].

Filament is promoting a solely distributed network, whose endpoint devices are autonomous and with the use of smart contracts and private microtransactions they communicate and transact with each other securely. (59).

[9] https://www.hyperledger.org/projects/sawtooth

Smart contracts implemented by Filament allow specifying the predefined terms that will guide the device through its possible interactions with others, eliminating the need to go through a cloud service. Such conditions can include price, time intervals that they can be accessed, number of times a function could be called and any other term that may be coded into it and is significant for the transactors. The standardized format for these contracts is JSON Web Token. The headers of a smart contract and its cryptographic signature may be stored in a blockchain providing proof for contractual obligations and strengthen its credibility. Filament used its own Blocklet protocol to create such proof.

Microtransactions on the other hand allow the conduction of private and secure transactions between devices that act autonomously. Such transactions incur when the data that will be exchanged or transmitted, i.e. humidity or temperature values, do not have any resemblance to value that would be required to be spent for a transaction that is verified through the Bitcoin network. Blocklet offers two solutions for such cases. Such transactions run in private side chains to avoid paying the transaction fees that would emerge if they went through Bitcoins public blockchain. Also, both entities that engage in a microtransaction mutually agree to set guarantees for fixing exchangeable values, preventing any of them to alter these values before their initial agreement is concluded.

5.1.2 Watson Internet of Things

Watson IoT Platform (60) developed by IBM will enable companies to have overall control of their IoT environments and enhance their business decisions in real-time. The platform claims to offer security, distributed data over the globe, cloud amenities, edge facilities and also an elegant environment of providers and suppliers. Moreover, it features machine learning, natural language processing and other analytics capabilities to enhance the development of IoT applications.

The IBM blockchain platform is one of the first business ready platforms that addresses the full life cycle (Develop – Govern – Operate) of a multi organization blockchain network. The platform is optimized with the Hypeledger Fabric and the Hyperledger Composer enhancing development. Governing is made with a consensus process for better control when onboarding and manages access with ease, their blockchain is fully managed combining reliability, scalability and ultra high security to protect against malware and insider attacks. IBM has already enhanced applications from food provenance to trade finance and supply chain to digital rights management.

According to IBM Blockchain technology may offer to business the same boost as the World Wide Web offered to communication. And the Hyperledger is a tool that aims to aid this transformation. As said earlier it is hosted by the Linux Foundation, it features innovators in banking, supply chains, finance, IoT, production and technology. The main characteristics of Hyperledger are the following:

Permissioned network: that offers privileged access to its members after they have been admitted into a business network.

Confidential transactions: that enables businesses to work securely and with great elasticity, as they can share (using encryption keys) transaction information with specific associates.

No cryptocurrency: as the transactions do not require mining or any expensive computations.

Programmable: as the users may make sophisticated improvements into the code of the smart contracts, enhancing the use of automatically executed transactions into their network.

Hyperledger Composer: it can translate business logic into code thus allowing developers that do not have prior experience to be blockchain programmers.

	Bitcoin	**Ethereum**	**Hyperledger Fabric**
Cryptocurrency required	bitcoin	ether, user-created cryptocurrencies	none
Network	public	public or permissioned	permissioned
Transactions	anonymous	anonymous or private	public or confidential
Consensus	proof of work	proof of work	PBFT
Smart contracts (business logic)	none	yes (Solidity, Serpent, LLL)	yes (chaincode)
Language	C++	Golang, C++, Python	Golang, Java

Table 6. *Hypeledger differences from Bitcoin and Ethereum Blockchains*
Source: https://www.ibm.com/blockchain/se-sv/hyperledger.html

IBM® IoT on Blockchain permits to IoT devices to transmit data over a business network towards a private blockchain ledger. The ledger is allowing the associates to save transactions in a decentralized manner and the data log is kept safe on the computers that form the network. Through the IoT registry, the users are able to access the device data in real-time allowing them to monitor the state of products or components in the supply chain. And also enables business associates to send and receive relevant information regarding the via IoT monitored data without any central administration. Moreover, all of them are able to recheck any transaction, avoiding conflicts and assuring that every associate will be obliged to behave in a proper manner regarding his part in all the transactions that he participates.

The Watson IoT™ Platform has an embedded feature that allows the users to write new IoT data into a private blockchain. This data are protected and is visible only to the transacting counterparts, whilst the device data is replicated in the blockchain which also validates the transactions through secure contracts.

The main goal of IBM is to leverage blockchain and allow it to effectively hold IoT data and create innovative methods in order to automate business procedures between partners avoiding at the same time the establishment of costly central IT premises.

5.2 Approaches under deployment

Below I will present some of the most promising projects that aim to materialize the convergence of Blockchain technology with IoT. Some are based on already operating platforms such as Ethereum and others are adopting completely new methods and architectures inspired by the blockchain technology.

5.2.1 Slock.it

Slock.it (61) is a German startup that offered smart locks, referred to as "Slocks", which are controlled by Ethereum public platform. The owner of a Slock is able to put his property available for renting and a customer can rent it by paying the required fee via a transaction in the Ethereum Blockchain and acquire access over the Slock. The locks (smart objects) operate through the automatic execution of blockchain enabled smart contracts, allowing procedures such as leasing apartments that are available for renting to complete without the need of user-owner interaction.

The Slock.it IoT Layer resolves the issues of securely linking smart objects to the blockchain and offers all the required capabilities that allow average users to use them.

Furthermore, it offers enhanced interoperability in a decentralized manner with many other devices.

Devices may be anything that is smart enough to conduct communication. The Slock.it IoT Layer operates like a firewall that scans and manages all transmitted messages. Private keys are always used to sign all sent messages enabling them to access the blockchain and request for permission from the access control mechanism.

All Devices have a digital twin in the form of a smart contract that contains the required guidelines and terms that will allow the passage of messages that are referring to the device. The contract can manage with safety any existing business process or allow renting or managing an approved list based on a predefined set of rules.

The IoT Layer takes advantage of the ENS (Ethereum Name Service) to oblige the use of exclusive IDs and by doing so it enables the use of a completely distributed repository for every device. Despite the fact that the central registry operates on the Main Net of Ethereum, the contract needed to handle accesses may be executed on any other Ethereum Virtual Machine - based blockchain such as EWF, Rinkeby and many other private chains.

Slock.it will be able to offer services in all possible ways such as Human to Machine, a Human can rent an apartment form a smart lock. Machine to Machine, an autonomous car pays for parking and also Machine to Human as an autonomous car may pay humans for a service check. In that way it claims to build the next generation sharing economy platform enabling the economy of things.

The main effort of the slock.it developing team currently is that instead of using a full client or a pruned full node that are profoundly not fit for the IoT ecosystem (demand a lot of storage, high bandwidth and a lot of CPU power), or a light client (less demanding) or a remote client (that lacks this disadvantages but is not trustfree, meaning you have to trust the information you receive from the server), they came up with what they call INCUBED (IN3), which they describe as an incentivized remote node network that will always provide the right response. In detail it works like this (62):

- I am a full node. I register at the registry smart contract and pay a deposit, which I would lose if I lied. Several nodes will do the same.
- An IoT device, running the Slock.it client now sends an RPC request to one of those nodes. There are three things the device needs to know in order to verify that the information is true: 1. The Merkle proof, similar to a light client. 2. The

current block header. 3. A signed blockhash (from that blockheader) from several incubed nodes which are specified by the device.

- The device can publish this information. If someone finds this to be wrong, he can claim the deposit of this node. This is done by so called watchdogs. The node which received the initial request from the client also acts as a watchdog.
- Since the IoT device, running the Slock.it client, asked other incubed nodes to sign the blockhash as well, it can verify the response and claim the deposit in case a wrong blockhash was signed. This happens in the convict function within the registry smart contract. (The only piece of information within the Ethereum virtual machine which you can get from the past are the blockhashes from the last 256 blocks. This is what Slock.it is using to build a fully decentralized system without any central authority or central node controlling the system.)

5.2.2. Streamr

Streamr is a European based company that has developed a technology that allows the streaming of live data in exchange for payment. Being more specific “it provides a complete system to tokenize the value of real-time data thus giving the opportunity to traders, people or machines, to complete their transactions in a decentralised P2P network”. As an example a car can earn tokens (money) by streaming data from its sensors to other interested parts (cars, weather stations) and purchase data that it needs from other likewise sensors creating a healthy ecosystem which prevents getting data without participating.

Currently they are cooperating with the team behind Golem[10], and they also cooperate with Zipper to build the first blockhain smartphone[11], aiming to replace our well known Apps with Dapps which are Decentralized applications that will have much more respect to user’s privacy.

Streamr (63) is a companion network which uses a blockchain for security-critical things like value transfers, access control and data integrity verification. The blockchain that they currently use is Ethereum due to its wide adoption and great smart contract features. But in case Ethereum is discontinued it could theoretically run alongside any blockchain (or at least alongside any smart contract platform).

[10] https://golem.network/ A global open source decentralized supercomputer that anyone can access.
[11] https://zippie.org/ Bye bye apps, hello dapps

The Streamr Network is a decentralised P2P network that transfers real-time data from producers to consumers. In order for someone to use the networks services, publish – subscribe, he must pay some DATA tokens. The nodes that give life to the network by offering data transportation services are rewarded with the collected fees. This incentivizes people to run nodes in the Network, offering them a way to monetize their idle bandwidth.

Moreover, the Streamr Marketplace enables data producers to collect fees in DATAcoin when a consumer asks for permission to access some of his stored data. Data licenses can be purchased or sold on the Marketplace among businesses, institutions, single users and machines, allowing them to make profit from the content of their data. The token will probably have more complicated uses too, related to staking and reputation mechanisms at play within the P2P network. DATAcoin is an ERC20 token running on the Ethereum blockchain, so the only mining necessary for token transactions is ETH mining.

Currently the Streamr consists of the following major components:

- Streamr Network: the infrastructure layer used for scalable real-time messaging between apps/machines/users.
- Streamr Engine: allows raw data to be processed and connected to APIs, smart contracts, visualisations, etc.

The Streamr will use the blockchain for payments (and validation of payments), but also identity, access control, data licenses as smart contracts, implementing the node incentivisation mechanism (nodes periodically report proofs of correct operation and earn rewards), and network control. In general, smart contracts on the blockchain act as a decentralized single source of truth and consensus for the static/slowly changing aspects of the Network. The dynamic functioning of the Network, including the data payloads, stay off-chain for reasons of performance and scalability.

Regarding time issues when used for IoT it is said that the Streamr Network runs, and will continue to run off-chain. Only some operations (e.g. user authentication and paying) will go to the blockchain. The actual raw data will never be put through there. So, the low amount of transactions handled by Ethereum per second shouldn't be an issue.

5.2.3 INT

Internet Node Token (INT) is trying to evolve IoT blockchains to a network environment that is similar to TCP/IP that will be able to solve problems from the most fundamental layer. INT is able to transmit on a variety of IoT networks and successfully complete required communication tasks, thus INT minimizes the problems for the developers of IoT blockchain to progress and enhance its expansion (64) .

In early 2018, INT released INTchain, that is the pioneer public blockchain for IoT in China, and took part in the foundation of Global IoTchain that was introduced by the Chinese Academy of Sciences Institute of Computing. In June 2018 they released INTchain 2.0 that takes advantage of technologies such as fog computing, blockchain and software-defined network SDN, to offer a scalable, elastic, effective and secure decentralized cloud scheme that efficiently moves computing resources towards the networks boundaries, sooths traffic on the central network routes, enables faster D2D communication speed and reduces the power needs of the IoT devices (64).

INT chain 2.0 will be used as the base for further development and open source. Moreover, the technical team of INT will engage with the creation of appropriate hardware devices such as routers and others, preparation of sample products, application testing and will also try to unfold new dimensions and enhancements regarding cross-chain communication architecture (cross-heterogeneous systems) that will enable them to create a network of industrial partners that will allow them to promote their products, and create a secure and self sustained IoTecosystem. (65).

Regarding consensus mechanisms, according to their whitepaper (66) they created a new consensus algorithm that they named “Double Chain Consensus” after studying thoroughly the core of DPoS (consensus algorithm) and based on the INTchain’s expected application scenarios and on the present technology state level of IoT devices. The Double chain scheme will be consisted by the “thearchy chain” which is formed by the servers that the manufacturers of the devices offer, community leaders and Thearchy Nodes, that will be created after community voting, and common chains that are formed by IoT device nodes coming from a variety of devices of disparate producers, which will be associated to or contain every node that belongs to the thearchy chain. The thearchy chain will be mainly tasked with the creation of new blocks based on dBFT/DPoS consensus algorithm and also it will have to harmonize its operation with those of ordinary chains at minor operating layers. Nodes that are part of ordinary chains must always review the data that are written on the thearchy chain to enhance their working performance.

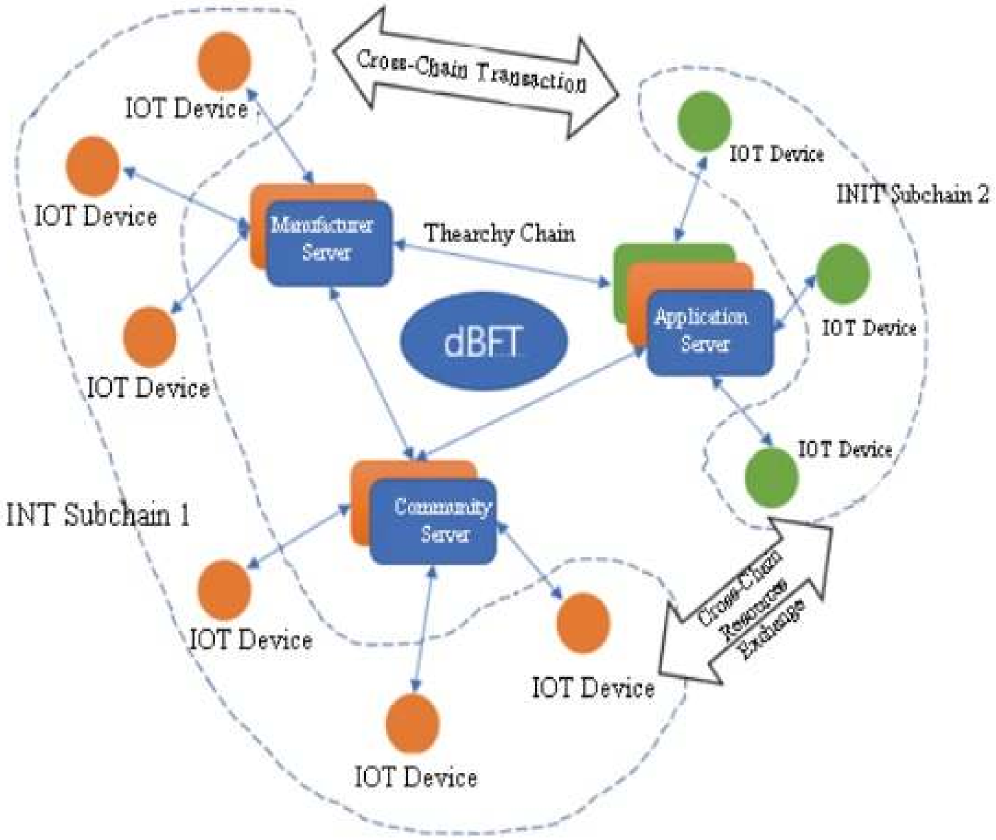


Figure 11. INT Architecture of Consensus Mechanism
Source: https://intchain.io/whitepaper/INT-whitepaper-release-EN.pdf

The new gen peer-to-peer protocol that is used by INT has the capability to switch smoothly from TCP to UDP and vice versa. Also it promotes the use of a distributed Thearchy Node mechanism that enables flip-flop connections, allowing to INT Chain to assure its users that the there will be no serious communication or connection issues despite the complexity that may be generated into environments of multiple computer rooms and operators as well as multi-line BGP. The network of INT Chain adopts a cluster-based distributed architecture that is formed neighboring to the Thearchy Nodes. INT also supports the use of specifically created smart contracts and cross-chain protocol technology, to sustain a wider development area for unlike devices in a public chain environment.

5.2.4 IoTeX

IoTeX is claiming to be a blockchain environment that was designed to enhance privacy and also it can scale automatically to meet up with current and future of IoT. IoTeX developing team is trying to create various innovative elements that will lead to blockchain 3.0. These elements include Roll-DPoS consensus that will offer sharpness and adaptability, an architecture that will support heterogeneous computing featuring blockchain in blockchain schemes and also light mechanisms that will ensure privacy. They suggest that their product will offer automated device management for everyone, in their words by “connecting the physical world, block by block.” (67)

As said above IoTeX is based on a adjustable, privacy-oriented blockchain environment developed especially for IOT, that exploits a blockchain-in-blockchain scheme with cryptoeconomic incentives that guarantee privacy and block possible losses of IoT data. It also implements embedded privacy mechanisms that use light cryptography methods and instant consensus with immediate finality, that raise the number of the transactions that the network is able to conclude, cut down needed transaction fees, and offer fast and secure communication among many chains. Moreover, it implements Subchain-as-a-service (SAAS) to support fast creation of application prototypes for IoT.

Their first Testnet called “StoneVan”, was released on the 20th of April, 2018 and their following version called “ Testnet Alpha” (codename Strive) last June, this version included for the first time their full Roll-DPoS consensus scheme that supports voting. Their future plans include the development of IoTeX subchains, SDKs and also they will try to cooperate and make alliances with manufactures of IoT products and DApp developers to further exploit the potentials of the IoTeX platform.

IoTeX team had also chosen to build their blockchain project completely from the start as they believe that the future of global IoT on blockchain demands a fundamentally different design and implementation than any existing projects. So IoTeX’s upfront design tries to find the balance among security, scalability and decentralization but also tries to assure that privacy and interoperability is prioritized. In order to achieve the latter two they propose three innovations.

1. Lightweight privacy-preserving techniques: full transaction privacy (i.e., encrypt sender, receiver, value) using lightweight cryptography—fun fact: Raullen (Co-

founder) and Xinxin (Head of Cryptography) focused their Ph.D research at UWaterloo on lightweight cryptography!

2. Roll-DPoS consensus mechanism: fast consensus and massive throughput with a more decentralized approach than normal DPoS.
3. Blockchains-in-blockchain architecture: permissionless root chain which enables cross-chain communication between flexible, interoperable sub-chains of IoT device networks, with ability to add any number of sub-chains for high scalability.

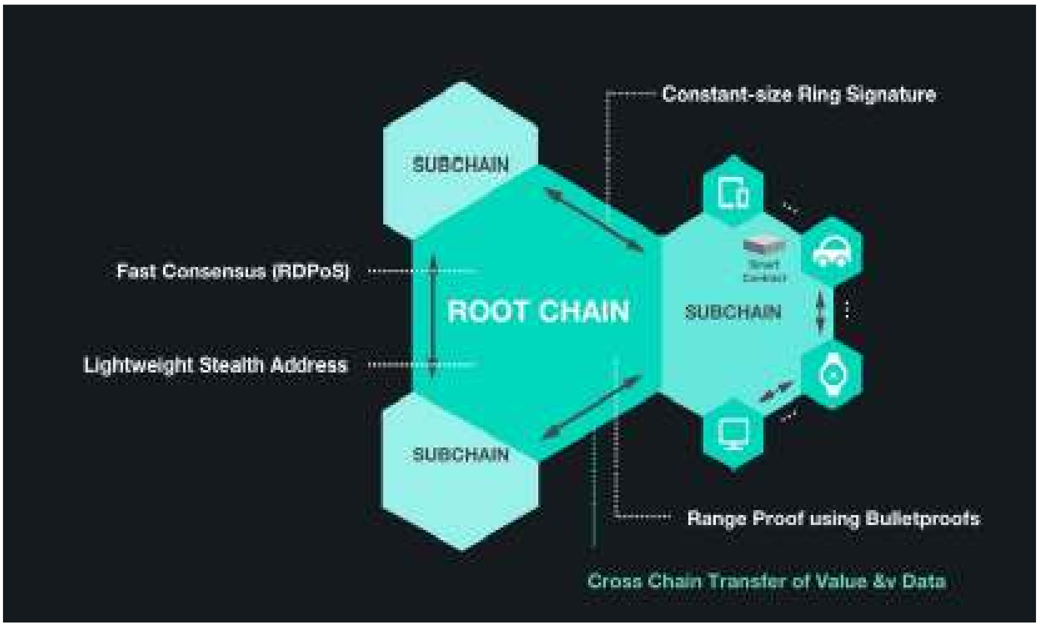

Constant-size Ring Signature
SUBCHAIN
Fast Consensus (RDPoS)
ROOT CHAIN
SUBCHAIN
Smart Contract
Lightweight Stealth Address
SUBCHAIN
Range Proof using Bulletproofs
Cross Chain Transfer of Value &v Data

Figure 12: IoTeX Architecture
Source: https://iotex.io/

The target of using blockchains in blockchains is to maintain a well balanced distributed network that maximizes scalability and privacy in a cost-effective way. IoTeX consists of a network of many blockchains that are hierarchically arranged and inside this network many blockchains can run at the same time while retaining interoperability. In IoTeX network, the root blockchain manages many independent blockchains, or subchains. A subchain is able to connect and interact with IoT devices that share something in common and if a subchain does not function properly, the root chain is unaffected. Also the network supports cross blockchain transactions meaning that data or value may be transferred from subchains to the root chain or to another subchain through the root chain.

5.2.5 IOTA

IOTA started up as one of the most promising projects for IoT and gathered lots of attention from the community, it is based on a permissionless distributed ledger and its developers suggest that IOTA is the pioneer open-source distributed ledger made to set in motion the evolution of the Internet of Things, by enabling costless microtransactions and security for IoT devices According to their webpage Blockchain technology's evolution will be based on distributed networks that are adaptable to any given changes and that offer Peer to Peer transactions with no cost or central authorities. But as we discussed thoroughly in this paper there are many limitations in the adaptation of the blockchain technology for IoT, mainly slow transaction rates, interoperability and high fees. Also, as the competition for validating blockchain transactions and consequently collect the financial rewards increased exponentially, most popular cryptocurrency blockchain networks turned from distributed to highly centralized, as the most powerful nodes gather the majority of the generated rewards (68).

The unique future of IOTA is that instead of using a traditional blockchain ledger architecture it integrates a different technology, called the Tangle, which they claim that supports feeless transactions, is secure and can be extremely scalable. The distributed ledger of IOTA, as said above, is not formed by blocks that contain transactions data concatenated one after the other in a chain like style, but it rather consists of standalone transaction entities that are entangled with each other.

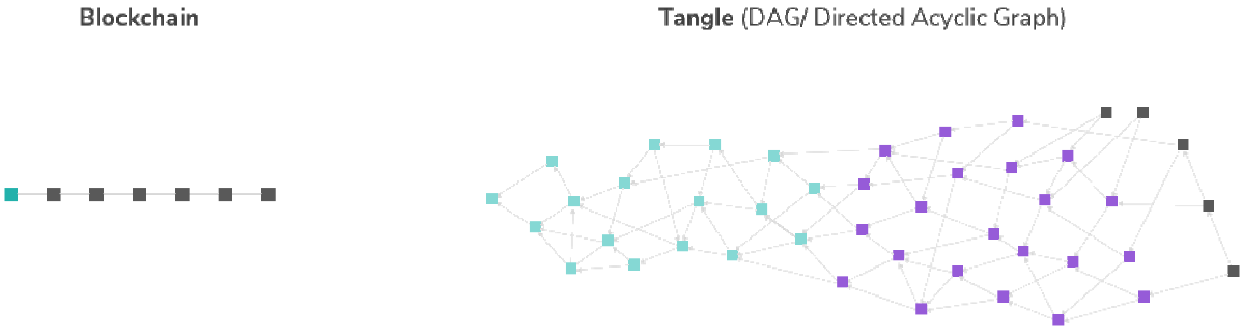


Figure 13: Blocchain and Tangle
Source: https://www.iota.org/get-started/what-is-iota

In order for someone to take part in the Tangle, he just has to execute a minor computational task so as to verify a couple of two earlier transactions. The Tangle does not distinctively rank actors or distributes responsibilities thus allowing everyone to be able to collect the same payments and assuring that no one will be left without motives. To perform transactions within the Tangle, you just have to validate two previous transactions, and the payment you receive for that is the validation of the transaction you are making by some of the following ones that will occur in the Tangle. This payment system for validating transactions, called 'pay-it-forward', does not require any financial rewards, subsequently enabling IOTA transactions to be completely fee-free. In addition, as there are no requirements for token rewards, IOTA has no restriction regarding transactional value settlements thus allowing data to be stored securely within Tangle transactions and also it offers the possibility to distribute the storage of bigger data records into many linked or grouped transactions. Moreover, this architecture provides great transaction scalability. They associate Tangle's throughput with the total activity of the network, increased activity leads to faster confirmation rates (68).

The Tangle holds essential blockchain features like the distributed ledger and security of transactions, though instead of working with blocks it implements the scheme of Directed Acyclic Graphs (DAGs). For example in a traditional blockchain, PoW is completed when miners verify transactions bundled up within a block. While the Tangle uses a different protocol: each transaction forms a new block and practically verifies itself and to complete a transaction the user must first verify two other pending transactions, allowing for an extremely simple version of proof of work to take place. Other projects that base their functioning in DAG are IoT Chain and Byteball.

The offline transactions that would be extremely helpful in a future IoE world are achieved through the use of sub-tangles that become interwoven with the main tangle at a later time (69).

The main benefits of IOTA are a) it is extremely scalable as the more activity the network has the faster the transactions are completed b) it does not need significant computing resources as it was developed in order to operate well even in simple sensors c) Fee-less transactions, the amount of money you send to someone will be delivered intact d) Security, all data transmitted is encoded e) it supports off-line transactions – devices never need perfect connectivity and f) it is Quantum immume by using special signatures.

By reading all the above, IOTA seems as the ideal solution for every possible problems in a future IoT ecosystem, but since its first launch IOTA has received a lot of criticism as the operation of the network appears to be problematic.

5.2.6 Weeve

Weeve aims to become a global network of IoT devices that would be able to autonomously buy and sell their data streams. It will make use of cutting edge cryptography, open source hardware and it will be secured by blockchain technology, Weeves ultimate target is to form the base for the Economy of Things. The Weeve platform will be able to unlock the power of any individuals IoT data by simply joining weeves data trading marketplace and securely monetize their data. Weeve was founded in early 2017 (70).

The Weeve team is trying to develop a platform that will be based on blockchain technology in order solve the problem of transmitting IoT data with enhanced security and privacy and they make use of a Trusted Execution Environment to successfully achieve that. One of the most intriguing features of the Weeve platform is that it integrates a recently developed TEE-MQTTS protocol that offers fast and extremely scalable processing. Thus enabling the blockchain based Weeve platform to successfully process the vast quantity of data that are produced by IoT devices (71).

The Economy of Things is a term that according to the Weeve team is consisted by the terms Internet of Things + Blockchain Technology + Weeve. EoT means that IoT devices will not only exchange data but will also conclude financial transactions autonomously.

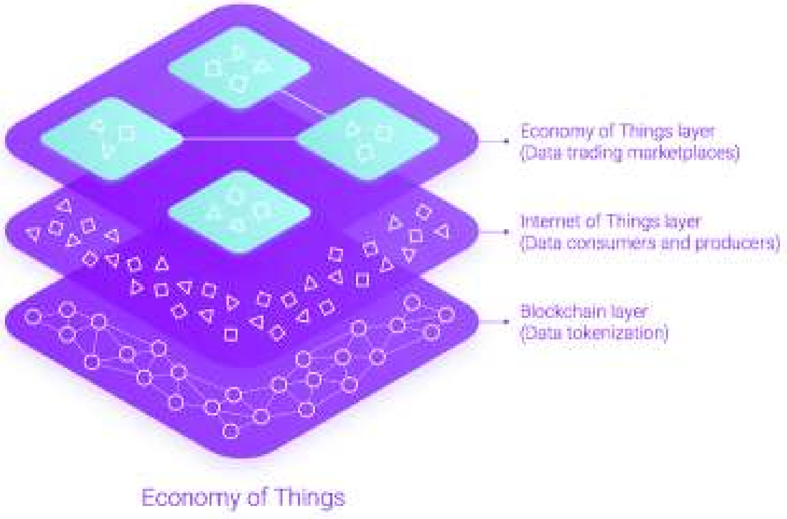


Figure 14: Economy of Things (72).

Currently, data marketplaces are mainly centralized and owned by tech giants such as Facebook and Google. A decentralized data marketplace, would enable users to take advantage or make profit of their devices data. But such marketplaces will have to confront with data authenticity and quality assurance, and this is highly expected as anyone could have access and sell his data in such an open marketplace. The solution suggested by the Weeve team will be "blockchain-agnostic" and will enable marketplace operators to choose the blockchain technology that best fit their needs, permission-based or permission less. Their starting point blockchain ledger is Ethereum, but we they also consider to issue support for Hyperledger, IOTA.etc. To sum up, Weeve is complimentary to Ethereum or any other blockchain.

More specific features and innovations of the Weeve (70).

MQTTS: a high-throughput, low-latency, transportation protocol developed by Weeve especially for securing IoT data.

weeveOS (alpha): TEE-OS (Trusted Execution Environment Operating System) that supports secure boot, encrypted storage, and built-in wallet. WeeveOS is probably the pioneer operating system that was developed specifically for IoT.

Testimony: The Weeve Platform also harnesses testified smart contracts. A testimony is a novel concept developed by Weeve to cryptographically prove (kinda ZK-SNARK[12]) the truthfulness and integrity of the data. This is a stepping stone to assess the quality and value of the data. For example, when the marketplace policy requires testified data, the gateway will drop data offers not satisfying the marketplace policy. In the same vein, it will drop the data from making it tradable, if the testimony is incorrect, as this implies the data was tampered with and its quality cannot be assured.

Blockchain technology: An unchangeable distributed ledger of financial transaction records that can also be used after properly tuned to record anything that has a potential value.

Cryptoeconomics: Cryptoeconomics is a term that comes from the joint use of cryptography (secure exchange of information) and financial motivations so as to create environments with specific attributes. They use this fresh popularized discipline to provide the instruments for building a secure, distributed and solid network.

[12] https://en.wikipedia.org/wiki/Non-interactive_zero-knowledge_proof

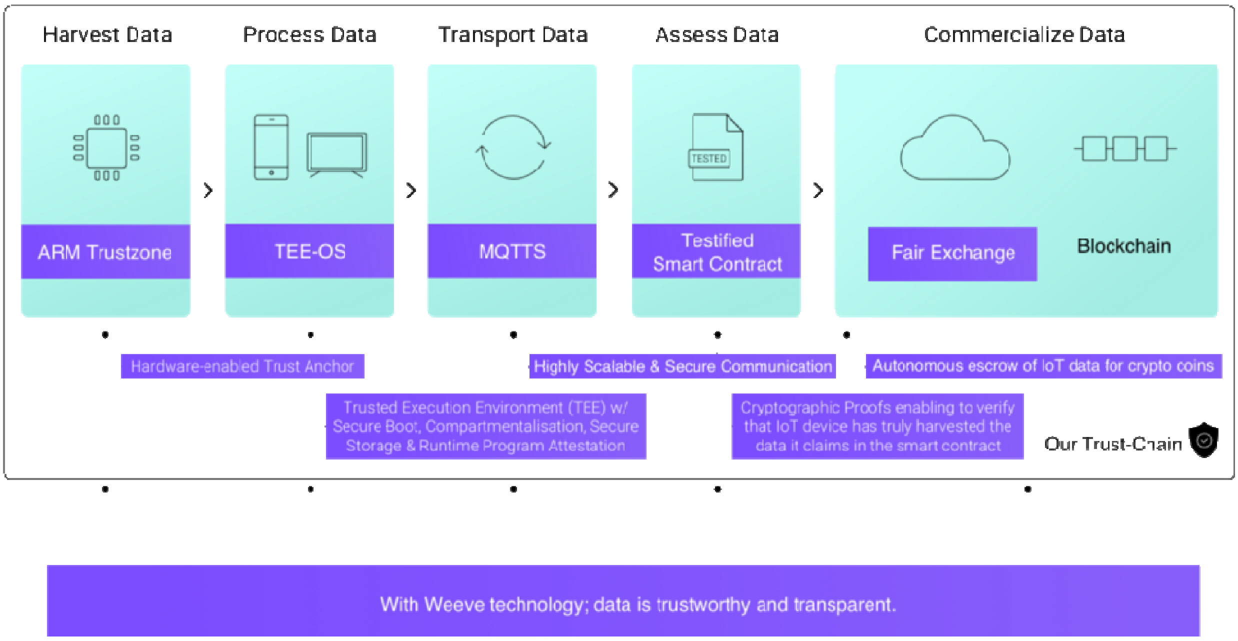

Harvest Data
Process Data
Transport Data
Assess Data
Commercialize Data
ARM Trustzone
TEE-OS
MQTTS
TESTED
Testified Smart Contract
Fair Exchange
Blockchain
Hardware-enabled Trust Anchor
Highly Scalable & Secure Communication
Autonomous escrow of IoT data for crypto coins
Trusted Execution Environment (TEE) w/ Secure Boot, Compartmentalisation, Secure Storage & Runtime Program Attestation
Cryptographic Proofs enabling to verify that IoT device has truly harvested the data it claims in the smart contract
Our Trust-Chain
With Weeve technology; data is trustworthy and transparent.

Figure 15: Weeve technology stack (70).

In order to run the weeveOS you must use hardware supporting the ARM Trustzone security extension that is supported by a lot of major hardware manufacturer like NXP and Infineon. But, there is also available a VM to virtualize the ARM chipset on any PC.

5.2.7 Contractnet

It is a public, permissionless, turing complete blockchain that was developed particularly for IoT's smart contracts, as it suitable for devices that have less build in memory. Such IoT devices will share information promptly and directly with the ContractNet blockchain or other intermediate entities such as oracles, in order to transmit and receive data with the use of blockchain enabled smart contracts. (73).

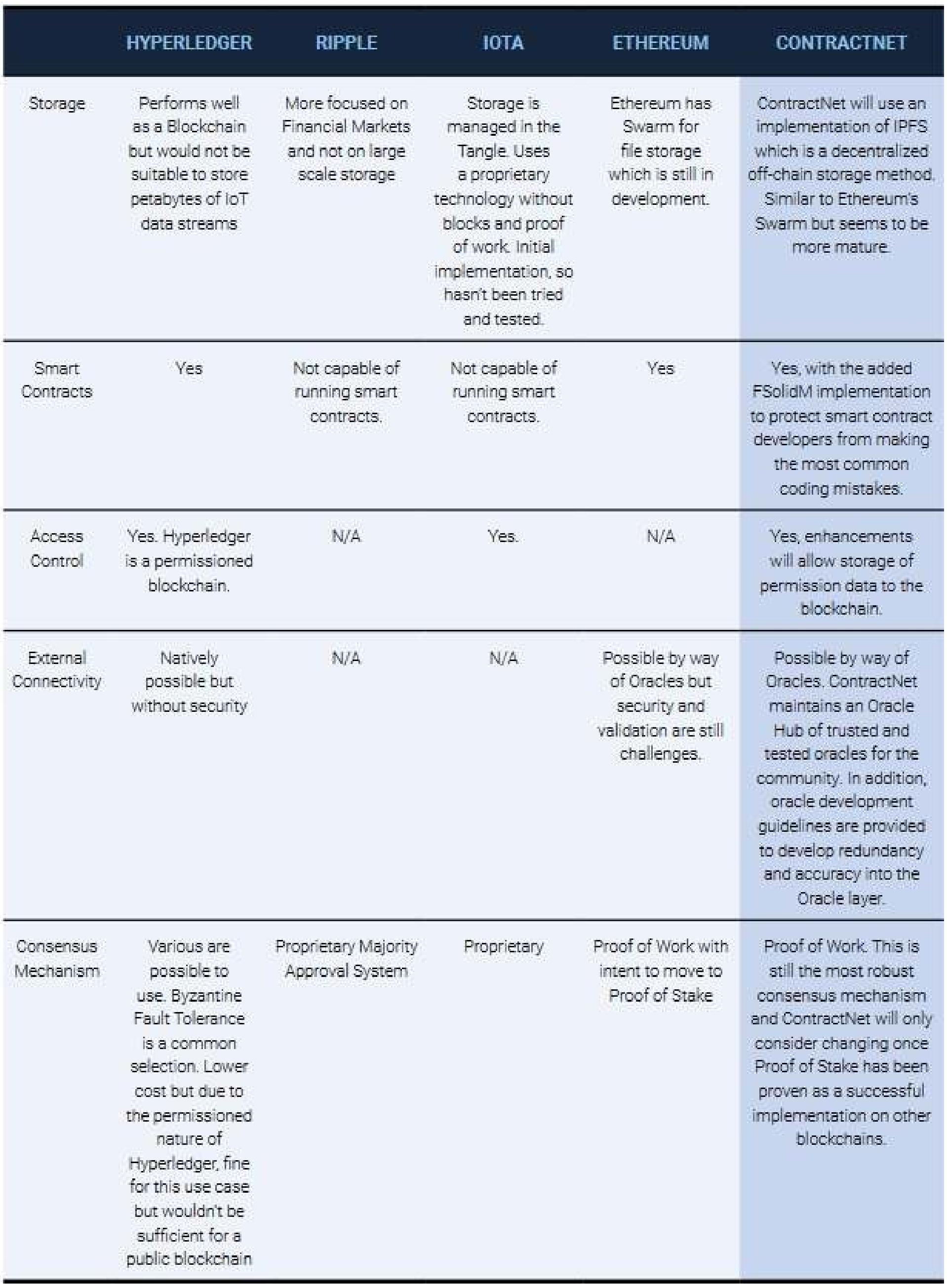
ContractNet was originally built as a fork from Ubiq and Ethereum. This fork provided the foundations for the platform. ContractNet's blockchain is built for one specific purpose: the storage and sharing of IoT data.

It differentiates itself from the competition through the creation of a hybrid system that combines the trust and immutability of blockchain with the practical nature of an off-chain storage later.

This hybrid system is managed through a "virtual chain" and specifically designed oracles. The end result is a solution that could be 1,000 to 8,000 times cheaper than traditional blockchain technology. They claim that it is significantly more efficient to store data on ContractNet's off-chain storage solution instead of on the blockchain.

ContractNet also differentiates itself from other IoT blockchains by introducing technology that avoids the pitfalls of coding errors in smart contracts, helping to protect smart contracts from malicious attacks as well as problems with confidentiality and integrity of data.

Finally, it plans to share all IP and data through a strictly controlled system, including access control permissions on the blockchain. (74).



	HYPERLEDGER	RIPPLE	IOTA	ETHEREUM	CONTRACTNET
Storage	Performs well as a Blockchain but would not be suitable to store petabytes of IoT data streams	More focused on Financial Markets and not on large scale storage	Storage is managed in the Tangle. Uses a proprietary technology without blocks and proof of work. Initial implementation, so hasn't been tried and tested.	Ethereum has Swarm for file storage which is still in development.	ContractNet will use an implementation of IPFS which is a decentralized off-chain storage method. Similar to Ethereum's Swarm but seems to be more mature.
Smart Contracts	Yes	Not capable of running smart contracts.	Not capable of running smart contracts.	Yes	Yes, with the added FSolidM implementation to protect smart contract developers from making the most common coding mistakes.
Access Control	Yes. Hyperledger is a permissioned blockchain.	N/A	Yes.	N/A	Yes, enhancements will allow storage of permission data to the blockchain.
External Connectivity	Natively possible but without security	N/A	N/A	Possible by way of Oracles but security and validation are still challenges.	Possible by way of Oracles. ContractNet maintains an Oracle Hub of trusted and tested oracles for the community. In addition, oracle development guidelines are provided to develop redundancy and accuracy into the Oracle layer.
Consensus Mechanism	Various are possible to use. Byzantine Fault Tolerance is a common selection. Lower cost but due to the permissioned nature of Hyperledger, fine for this use case but wouldn't be sufficient for a public blockchain	Proprietary Majority Approval System	Proprietary	Proof of Work with intent to move to Proof of Stake	Proof of Work. This is still the most robust consensus mechanism and ContractNet will only consider changing once Proof of Stake has been proven as a successful implementation on other blockchains.

Figure 16: Comparison of Contractnet with other blockchains
Source: https://contractnet.com/light_paper_contractnet.pdf

5.2.8 Waltonchain

Waltonchain is a blockchain project that started out in December 2016. This platform aimed to combine the technological capabilities of RFID and blockchain and form a system that can monitor supply chains. Like other blockchain projects that we mentioned earlier it was build to decentralize the entire supply chain, being able to keep records of a products' history, as well as store this information on its internal network.

"Two of the most important components of Waltonchain are the RFID reader chips and RFID reader tags. The tags can be thought of as radio frequency devices that serve as physical carriers of information such as the electronic product code (EPC). This code can be attached to traceable items such as medicines, electronic goods, and clothing and then circulated all across the globe. The reader chip or the UHF recognizer is then used to harness the coded data from the tags. Technically speaking, the reader not only extracts vital supply chain info but also amplifies the incoming signals via the use of technologies such as LNA[13] and ADC[14]" (75).

The RFID readers are considered as nodes into the network and the tags are attached to the products that are circulated within the supply chain. All produced data, i.e. dispatch details and delivery info is recorded on the Waltonchain blockchain via the RFID system.

Smaller data sets that contain i.e. an items geo-position or temperature are stored in what they name "child chains" which over time are accumulated and allowed to merge with the master chain. And this design is that boosts the overall speed of data distribution as well encryption levels.

One more significant feature of the platform is the Walton Genesis Block— which works as a central service module that allows a host of performing functions such as WTC (WaltonCoins) token management, internal monetary regulation, sub chain management, smart contract execution, etc (75).

WaltonChain can track and verify the various conditions and locations that the tagged products had been through and all the information are available to the consumer. In addition the tags have been manufactured with the ability to generate randomized public and private keys to increase IoT security applications and counter forgery or tampering issues.

[13] Low Noise Amplifier
[14] Analog to Digital converter

Given that all transactions are executed using the internal WTC token, in order for a transaction to be written on the master chain it must first fulfill all the pre-set smart contracts criteria.

The Waltonchain parent chain will be a distributed public ledger, and transactions that were performed in the interval of 60 seconds are written into a block that is associated (linked) with the last block that was added to the chain. The consensus mechanism that is used in the parent chain is Proof of Stake & Trust (PoST) which is an evolvement of the classic Proof of Stake mechanism. This new consensus mechanism offers two improvements. Firstly, by using together the Waltonchain blockchain and RFID it can exploit the commercial credit link capability to enhance the honest functioning of the involved nodes by using the evaluation mechanism to achieve further training and promotion of their behavior. Secondly, it offers a more sophisticated mechanism for choosing the most appropriate and decent nodes as coinage nodes, thus increasing the total security of the blockchain environment. The child chains are free to select among PoS, PoST or any suitable consensus algorithm to meet the needs of different application scenarios (76).

According to the developing team of Waltonchain they aim to create a cross-industry data connection through the innovative parent chainchild chain structure, enterprises in various industries can customize the child chains to their specific needs and ultimately creating a “parent chainchild chain-application-chip” reliable connection ecosystem. ”Waltonchain launched the SMN Recruitment Program, where SMNs will help build the global child chain ecosystem and form a multi-chain cross-industry network. The cross-chain technology architecture can connect data and information of the parent chain and child chains to form a vast cross-industry blockchain ecosystem” (77). At the time six large industrial child chains are build and Korean Sensor Technology [NIDS] is their strategic partner. They have also prepared a layout for smart cities. And in the near feature they aim to enter smart agriculture, smart healthcare etc.

The ultimate goal of the Waltonchain project is to set the base for what they name as the Value Internet of Things (VIoT) by integrating the physical world with the blockchain.

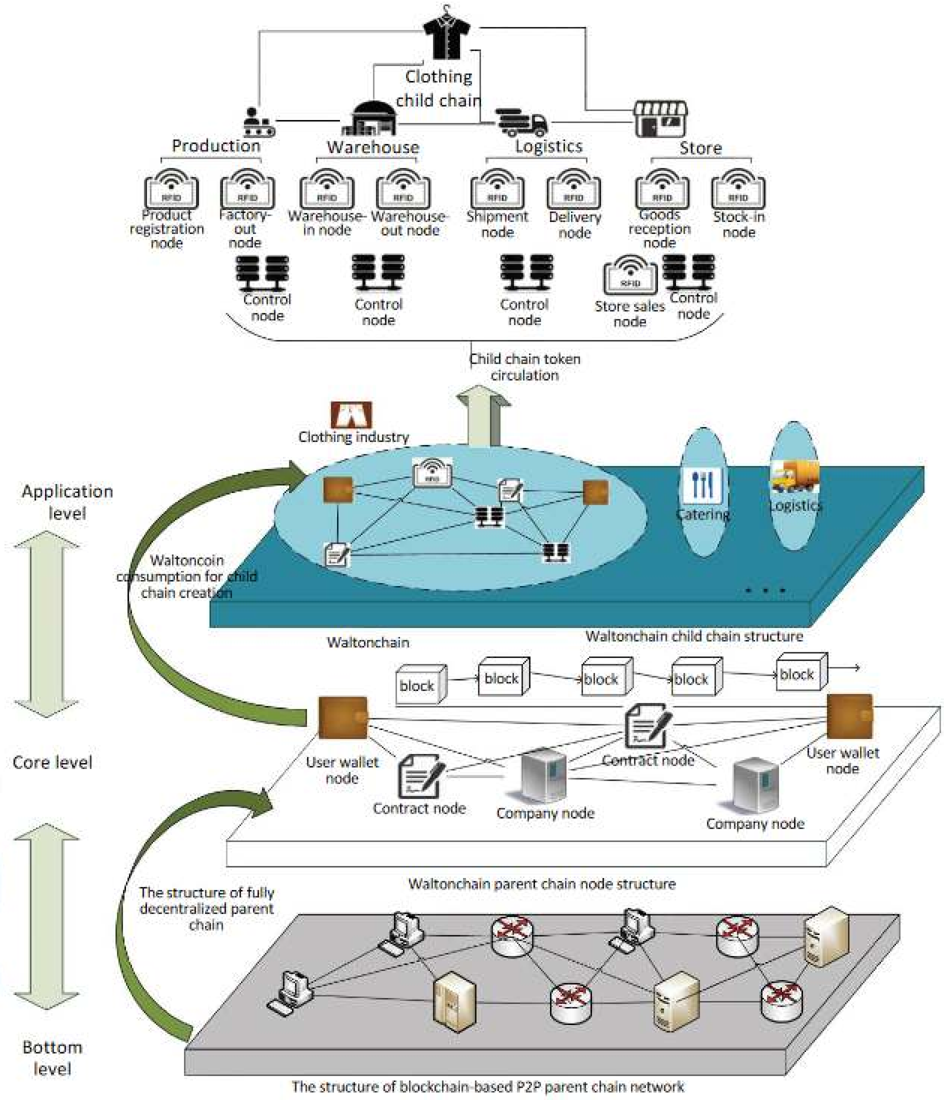


Figure 17: The detailed structure of Waltonchain
Source: Waltonchain Whiteparer

5.2.9 SDChain

SDChain or SixDomainChain is a public and decentralized blockchain ecosystem that wants to set the world wide standards of IoT Six-Domain Model and also the key architecture principles regarding the implementation of decentralized blockchains. By taking into account all the technical specifications of IoT as well as the evolvement requirements of the developing environment, SDChain implements most of the characteristics of the current blockchains such as smart contracts that also support cross-chain transactions, circulation of digital assets, Peer to Peer communication, identity management, encryption and consensus algorithms, identity management, credit management, DApps and market consensus-based inducements. With such features they mean to ensure beneficial, rapid and sustainable development of SDChain business ecosystem to achieve mutual benefits among digital assets, blockchain and industrial IoT through efficient circulation and value transformation of digital asset credits, within a global framework of ISO/IEC standards (78).

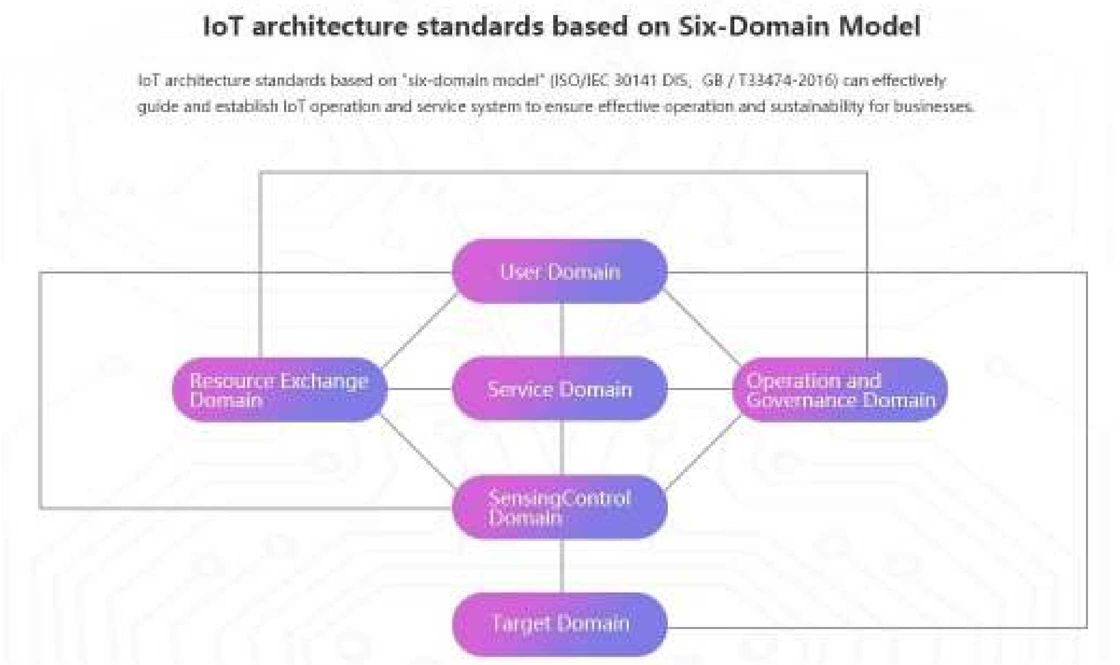

IoT architecture standards based on Six-Domain Model
IoT architecture standards based on "six-domain model" (ISO/IEC 30141 DIS, GB / T33474-2016) can effectively guide and establish IoT operation and service system to ensure effective operation and sustainability for businesses.
User Domain
Resource Exchange Domain
Service Domain
Operation and Governance Domain
SensingControl Domain
Target Domain

Figure 18 : IoT architecture standards based on Six-Domain Model

They believe that the blockchain should be the underlying decentralized eco-operation platform, which will ensure the development of an IoT credit system and value system. Below we see the proposed model for a converged architecture of IoT and blockchain.

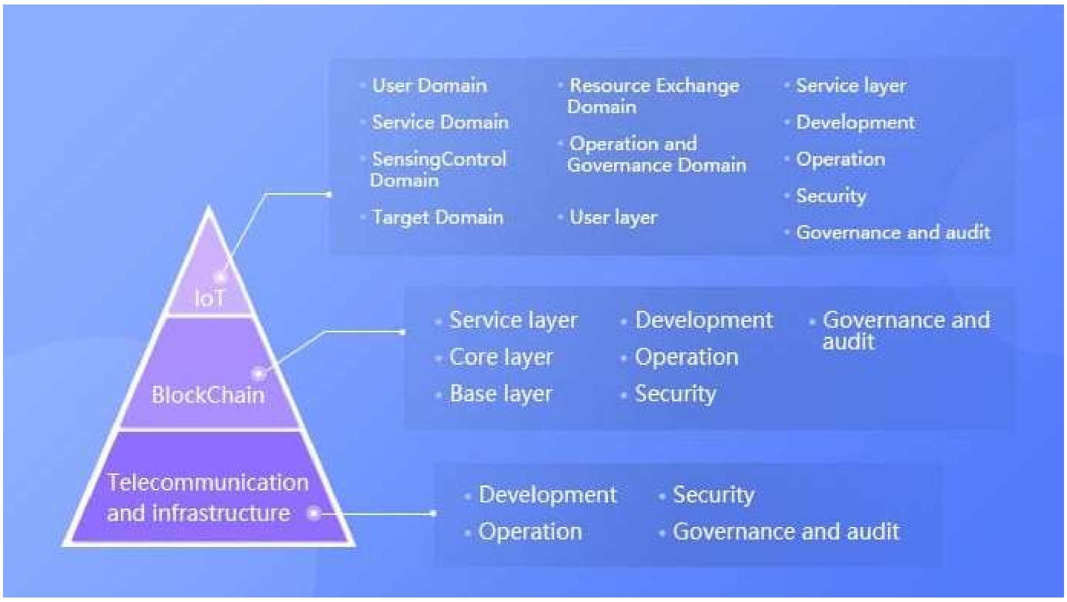


Figure 19: Converged architecture of IoT and blockchain.

The transaction performance of the blockchain is improved by reducing communication, computation and storage load of the consensus nodes through specifying associated physical configurations and size of users and consensus nodes with sharding mechanism and high-speed network connection.

Regarding encryption SDChain mainly adopts SHA256 in hash function as its basic algorithm. SDChain develops its own SDSchnorr[15] algorithm based on Schnorr, but designed to be flexible SDChain can integrate with a variety of encryption algorithms.

The consensus mechanism used taking under consideration the complexity of IoT, the diversity of communication protocols and the high security and performance requirements of the underlying blockchain, SDChain innovatively proposes the SDFT (Six Domain Fault Tolerant) algorithm, incorporating the highly-consistent RAFT[16] and the strongly-concurrent PBFT algorithms, while ensuring security, high performance and trust in a scalable manner (78).

In SDChain the private key of the smart contracts is discarded upon creation and no one can send out the digital asset except through the consensus mechanism. Smart contracts of SDChain require mandatory, highly real-time and fully automatic triggering. The triggering data is also protected by the blockchain, to ensure accuracy, security, reliability and tamper-resistance.

5.2.10 QuarkChain

QuarkChain is using the PoW consensus mechanism as they believe that it has proved its worth after being used for so many years, but though at first this seems to be unrealistic they propose other innovations to take advantage of the probably most secure consensus mechanism.

To solve the scalability issues, they introduced a re-shardable 2 layer blockchain design where the first layer consists of elastic sharding blockchains (shards) and the second layer is a root blockchain that confirms the blocks from the shards. In their test net the number of transactions per second has already reached 14755+ tps (79). Transactions between shards can take place at all times, and be validated within a few minutes. The number of validated cross-shard transactions per second will increase alongside the

[15] https://en.wikipedia.org/wiki/Schnorr_signature

[16] Raft is a consensus algorithm that uses log replication,

increase of the number of shards. QuarkChain Network adopts the use of PoW to achieve consensus in the root chain, and root-chain first proof of work for the shards.

Regarding decentralization QuarkChain implemented horizontal scalability. When TPS (transaction/second) goes high a super-full node may become too expensive so they allow many honest nodes to form a cluster and operate like a super-full node. This way a node could operate without the need of buying high cost hardware and weak miners will be discouraged to join mining pools as they will be able to mine using their low demanding electricity hardware.

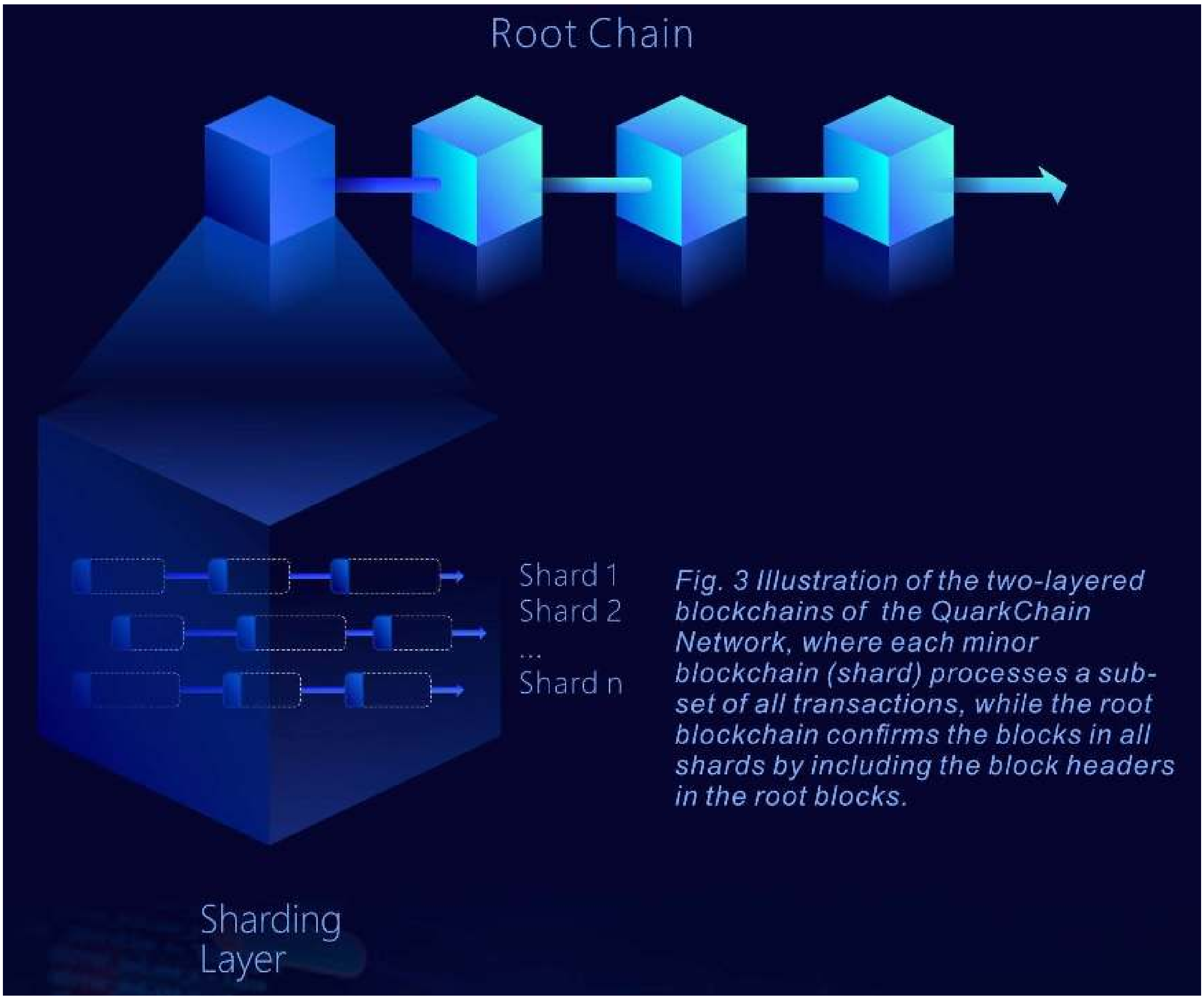

Root Chain
Shard 1
Shard 2
...
Shard n
Fig. 3 Illustration of the two-layered blockchains of the QuarkChain Network, where each minor blockchain (shard) processes a sub-set of all transactions, while the root blockchain confirms the blocks in all shards by including the block headers in the root blocks.
Sharding Layer

Figure 20: QuarkChain system architecture
Source: https://quarkchain.io/QUARK%20CHAIN%20Public%20Version%200.3.5.pdf

In order to encourage miners to participate in such clusters, QuarkChain has developed a game theoretic groundwork to give motivations, within which hash powers are evenly distributed to all participating shards to incite greater effort by everyone. At least 50% of the global hash power is used by the root chain to counter the possibility of a double spending attack (80).

QuarkChain Network will support many different dApps, including ones that require increased throughput ratios such at dedicated IoT dApps, advertisement, Artificial Intelligence, P2P economy, games, Big Data etc. It also supports Turing-complete smart contracts that may be used without any constrain within the QuarkChain Network and these contracts are written in Solidity.

QuarkChain is able to support cross-shard transactions (tx) at any scale, meaning that every user can execute such transactions whenever he wants at his own will. This is made possible by the implementation of the 2-layer scheme that is based on the root chain. After the process is initialized by the tx-input shard, the tx-output shard has to first receive the required validation signal by the root chain to acknowledge the transaction fully. This is essential due to the fact that the tx-input shard and the tx-output shard do not have the same ledger so they must be reassured by the root chain that the transaction process that they were involved in was valid (80).

5.2.11 Atonomi

Atonomi is supposed to offer a new security protocol and the required infrastructure that will allow to the billions of IoT devices to interact and exchange information and value in a trusted environment (81).

Atonomis main novelty is that it integrates into the blockchains unchangeable ledger both the identity and the reputation of devices. In order to achieve that they build ecosystems were the users will be motivated to preserve decentralized consensus regarding the transactions that take place within Atonomis Network. Their use case scenarios, building on the Atonomi Security Protocol include, Healtcare, Smart Home, Smart Cities and Industrial IoT.

One of the major problems of IoT's security is the difficulty to validate the reputation and the identities of IoT devices, and they aim to resolve these issues by tokenizing the two previously mentioned attributes of such devices on their Network by leveraging Ethereum and at the same time to make use of the token as the tool to guide the ecosystems population growth. Important participants that will keep up the operation of the network, like manufacturers of OEM devices, wholesalers, home or industry users will be granted with Atonomi tokens for being a part of the Atonomi network.

Atonomi Token empowers a decentralized, unchanged secure framework and forms a structure that leads to the continuous rising of commitment in the Atonomi Network, it is also exploited by the security protocol to allow for device reputation management activation, registration and economic transactions. The attributes of reputation and trust offer increased security levels that allow increased interoperability for IoT devices. They say that the existence of digital tokens is the factor that enables automated D2D transactions for the IoT enabled devices, as otherwise in the absence of such a token for exchanging values the devices should have embedded capabilities for processing credit cards and that would demand higher computing power on resource-constrained devices.

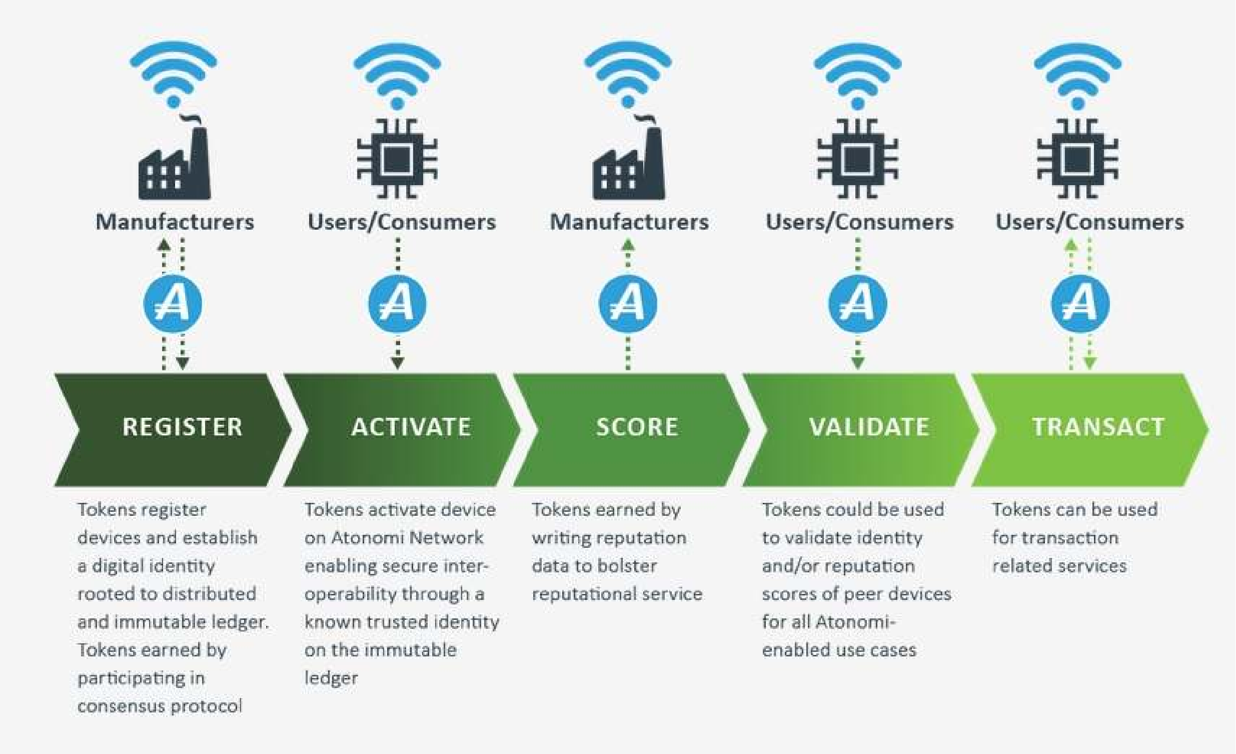

Manufacturers
Users/Consumers
Manufacturers
Users/Consumers
Users/Consumers
REGISTER
ACTIVATE
SCORE
VALIDATE
TRANSACT
Tokens register devices and establish a digital identity rooted to distributed and immutable ledger. Tokens earned by participating in consensus protocol
Tokens activate device on Atonomi Network enabling secure inter-operability through a known trusted identity on the immutable ledger
Tokens earned by writing reputation data to bolster reputational service
Tokens could be used to validate identity and/or reputation scores of peer devices for all Atonomi-enabled use cases
Tokens can be used for transaction related services

Figure 21: Tokenized IoT Security Ecosystem (Atonomi)

Atonomi leverages established technology of its parent company, Seattle-based CENTRI Technology, who is a leader in providing IoT data security solutions, with partnerships with Arm, Flex and STMicroelectronics.

Atonomi enables secure transactions between IoT devices through their blockchain-based Identity Registry Network (IRN), which establishes root-of-trust using encrypted whitelist data from participating OEMs/ODMs providing unique device identity and cryptographic key for each device to be validated onto Atonomi Network. Atonomi uses the Ethereum blockchain as part of their decentralized solution.

New manufactures in the Atonomi Network are screened by existing members of the network and then provided with a unique manufacturer identifier used when registering devices submitted on the network. This screening process is used to continuously calculate the reputation of each manufacturer. Trusted manufacturers submit their list of devices, including unique device ID and cryptographic public key, to the Atonomi whitelist which is written to the Ethereum blockchain, and referenced later during device activation. Selected manufacturers of the Atonomi Network will run a limited number of Identity Registry servers. After being registered, the device may be activated and added in the network and work without any issues as it will be already known and trusted by the Atonomi Network.

When the identity of a device is settled, its reputation has to be governed so as to allow secure and proper interoperability. The reputation of devices is expressed by their exclusive behavioral signature that represents various degrees of service quality measurements and security. The Atonomi Network enables registered devices to validate a device's reputation stored on the blockchain to establish trust before exchanging data or engaging in commerce (82).

5.2.12 XAIN

XAIN is a research project that focuses on the enhancement of the blockchain through supportive training and a new two-fold mechanism for achieving consensus that they name Practical Proof of Kernel, that will have much less energy consumption needs and will promote network democratization (less powerful devices such as ECU[17] could be used) (83) .

In 2017, XAIN was the winner of the 1st Porsche Innovation Contest and formed a partnership with them, to develop the XAIN's Blockchain-powered hybrid vehicle client. Some of the features of the final product would be, traffic information, lock/unlock of the car or the trunk remotely from another location and increased security for the vehicle software.

[17] Engine or Electronic Control Unit (https://en.wikipedia.org/wiki/Engine_control_unit)

So, to address all the previously discusses difficulties of integration, the fundamental characteristics of the eXpandable AI Network – XAIN, are

- Three types of clients
- Practical Proof of Kernel Work
- The use of an Ethereum Virtual Machine module to enable the use of Solidity based smart contracts.

The three client types are distinguished in a) **Logging-Only:** they hold the whole Merkle tree (4.3.2) of the Blockchain as well as the full transactions history b) **Initiators:** like Ethereums light clients that have to look at a near Logging-Only client for actual data, but are able to insert newly conducted transactions in the blockchain network c) **Processors:** these are hybrid nodes that apart from mining transactions they also save the newest stack of transactions, currently they only store merely block headers for older transactions as over time the available storage is decreased.

Practical Proof of Kernel Work is a consensus mechanism that was developed by XAIN, all blocks are enhanced with a seed called Q. The seed is generated randomly and it is recalculated for every new block as a deterministic digital signature of the previous blocks seed, and it is signed by the next blocks leader. Afterwards the seed is utilized by a method named Cryptographic Sortition—encountered at the Algorand[18] research— that chooses a random set of nodes among every node that is eligible to mine and has a particular anticipated size, in a way that only the chosen nodes have the required knowledge that they had been selected thus giving no fertile ground for an attacker to manipulate these nodes and alter their mining behavior as no one else can have a clue about which are the selected nodes and an attacker can only target random nodes of the network. The above described procedure renders the network to be resilient to such attacks even if the case that the anticipated size of the committee is limited even to just 20 members. Additionally this procedure is also enhanced by using a white list and other access control mechanisms achieving scale invariance with energy-efficient mining.

[18] www.algorand.com: Decentralized digital currency and transactions platform.

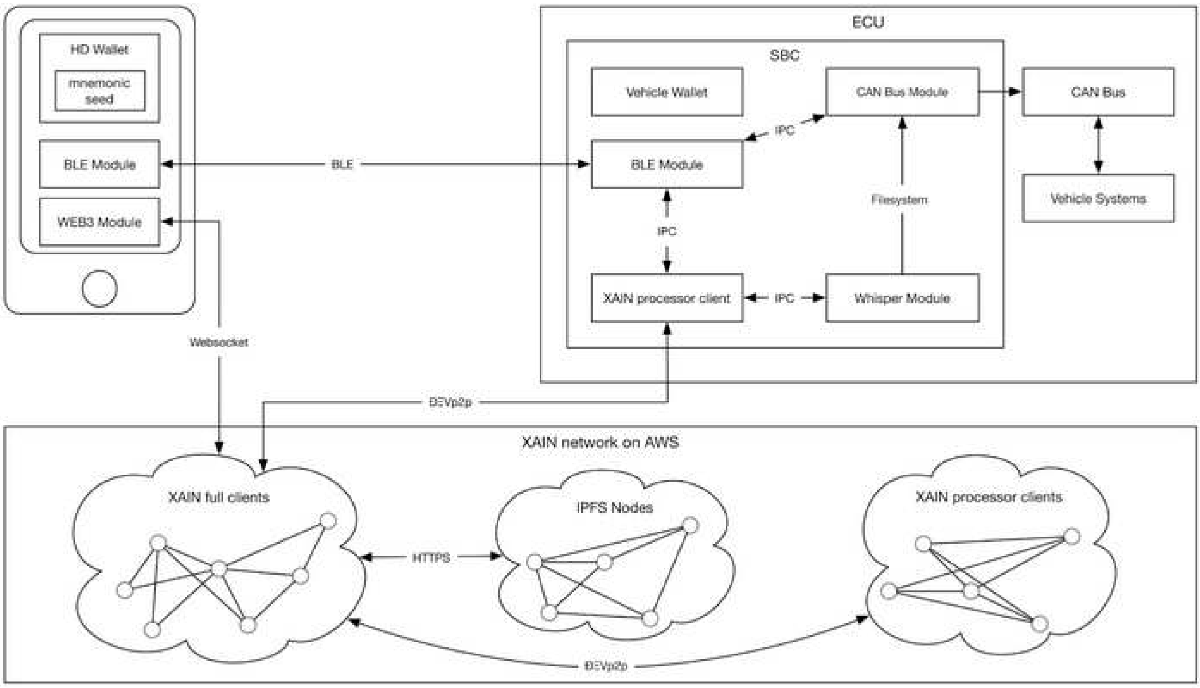


Figure 22: XAIN Vehicle Network System Architecture
Source: https://medium.com/@XAIN/part-1-technical-overview-of-the-porsche-xain-vehicle-network-f70bb117be16

5.2.14 Comparison chart of the discussed integration approaches of IoT and the Blockchain technology

Projects	Network	Use of	Consensus	Token	Smart Contracts	Special Features
Filament	Private or Public	Bitcoin	PoW & TEE	Bitcoin, Jason Web Token, data, etc	Yes	• Use in current devices • Blocklet USB Device • Software Blocklet Chip • Trusted Execution Environment • Microtransactions in Private side chains
IoT Watson	Permissioned	Hyperledger	PBFT	N/A	Yes (chaincode)	• Private blockchain for users • Natural Language Processing • Public or confidential transactions
Slock.it	Public	Ethereum	verification of single result (Merkle-Proof)	Ether, ERC20 or other	Yes	• Incentivized remote node network INCUBED (IN3) • Multichain support
Streamr	Public	Ethereum	PoW	DataCoin	Yes	• Use of Blockchain only for the static/slowly changing aspects of the network.
INT	Public	N/A	Double chain consensus dBFT/dPoS	ERC20	Yes	• Multichain • Thearchy chain • Ordinary chains
IoTeX	Public	N/A	RDPos (VRF & PoS)	IOTX ERC20 compatible	Yes	• Multichain • Rootchain Subchains • Subchain as a Service
IOTA	Public	N/A	Proprietary PoW simple	mIOTA	Yes TOQEN (smart contracts)	• Directed Acyclic Graph (DAG) • Tangle • Offline transactions
Weeve	Public or Private	Ethereum	PoW	WEE (Ether)	Yes	• Trusted Execution Environment OS • MQTTS protocol • Blockchain agnostic
Contractnet	Permissioned	N/A	POW	CNET	Yes	• Hybrid Chain • Virtual Chains Oracles • IPFS (Decentralized off-chain storage)
Waltonchain	Public	N/A	POST	WTC	Yes	• Child/parent chain • RFID reader chips/tags
SDChain	Public	N/A	SDFT (RAFT & PBFT)	SDA	Yes	• Six Domain Fault Tolerant
QuarkChain	Public	N/A	POW & rfPOW (for shards)	QKC	Yes	• Reshardable 2-layer blockchain
Atonomi	Public	Ethereum	POW	ATMI	Yes	• Tokenize the Identity and reputation of devices
XAIN	Permissioned	N/A	PPoKW	XAIN	Yes	• Three type of clients • Hybrid nodes • Cryptographic Sortition

Table 7: Summary table of the discussed integration approaches of IoT and Blockchain Technology

5.3 Proposals

The attention draught on this topic is vast and many independent researchers and groups are trying to find the best solution on how to take advantage of the blockchain technology to secure IoT ecosystems. Many proposals have already been published and their issuers will try to materialize them in the forthcoming years. Below I will present some of the most interesting proposals, focusing on the attributes that differentiates them.

The authors of (16) proposed a blockchain-based architecture for IoT, they name it Lightweight Scalable BC (LSB) and it implements a consensus algorithm that is IoT friendly and eliminates the demand for figuring out a cryptographic puzzle before being able to add new blocks into the Blockchain. LSB integrates a trust method that works in a distributed manner and it works like this. All nodes are organized in clusters and every cluster vote for a Cluster Head (CH), these CHs are committed to properly run the Blockchain and they are called Overlay Block Managers (OBMs). Moreover, the CHs handle every transaction either incoming or outgoing that was produced by or involves any of their cluster members. As the most important functions for the operation of the blockchain are executed by the CHs, the LSB is not susceptible to the continuous presence of the IoT devices, meaning that if one or more devices go off line it won't be affected. LSB does not broadcast every new event (transactions, blocks) to the entire network, as they limit the number of nodes that manages the Blockchain. Also, the user data is not saved in the Blockchain but instead they store a hash of the data in the public Blockchain.

The authors of (37) proposed a distributed cloud architecture that relys on the blockchain and offers secure, cheap and customized access to the parts of the IoT network that have higher computing demands. They transfer computing resources closer to the limits of the network by implying a distributed secure SDN (software defined network) controller network architecture that is based on the blockchain, which results in securely minimizing delays among IoT devices that are at the edge of the network as well as the computational needs in the core of the network. They propose "Proof of Service" as their consensus protocol which is a 2-hop blockchain teqnique (84) which combines the mechanisms of PoS and PoW.

The authors of (85) proposed the Blockchain Connected Gateway in order to postpone the need for immediate modification or replacement of legacy IoT devices. The Blockchain gateway is an intermediate between users and IoT devices, meaning that the users don't have to access their IoT devices directly but they do it through the defined BC gateway, increasing security and privacy. Appropriately programmed, the BC gateway may deter the device from having access to private user information and allow such access only if the user accept its privacy policies. Also, they propose a digital signature mechanism for securely managing privacy preferences and authentication purposes, which relies on the tenacity of ECDLP (Elliptic-Curve Cryptography) as well as the durability that bilinear pairing offer.

The authors of (86) propose hybrid blockchain architecture for IoT, named Hybrid-IoT were subgroups of IoT devices become peers on PoW sub-blockchains, connected with a BFT inter-connector framework as the BFT consensus protocols offer high throughput rates with a low number of peers. PoW blockchains offer distributed consensus among many IoT devices and they are interconnected by a BFT inter-connector framework such as Polkadot [19]and Cosmos[20] in order to achieve interoperability among sub-blockchains and guarantee inter-blockchain transactions. In case a transaction between two distinct blockchains occurs, it is retrieved by the BFT inter-connector framework that checks that the transaction is correct and authentic; after a positive response, the BFT inter-connector framework transfers the transaction to the target sub-blockchain's transaction pools that hold unprocessed transactions; last, the transaction is processed and included in a newly generated block in the respective sub-blockchain, upon PoW consensus.

The authors of (87) proposed blockchain-based architecture for IoT security called the IoTchain. It is divided in three tiers namely: authentication layer, blockchain layer, and application layer. Authentication layer contains the certification center and the detection center that provide certification and security. In the application layer they use regional nodes that have significant computing power and storage capacities in order to manage the devices of a region. The consensus mechanism they prefer to use between regional nodes is the PBFT (Practical Byzantine Fault Tolerant) but they may use any other lightweight consensus algorithm. The Blockchain layer accepts transactional information from the application layer, and provides the possibility to either store them on the blockchain directly or via the merkle tree.

The authors of (88) suggest they key enabling technologies that will enable a Fog-IoT architecture to materialize. Regarding security they suggest the use of (a) Blockchain and smart contracts; (b) multi-layer identities and naming other than IP; (c) Artificial Intelligence (AI) and machine learning (ML) technologies; (d) lightweight IoT security, and deception based active cyber defense technology. Regarding scalability they suggest (a) again Blockchain and smart contracts; (b) integration of Network Function Virtualization

[19] Polkadot.network
[20] Cosmos.network

(NFV) and Software Defined Networking (SDN); (c) orchestration, resource allocation, and onloading/offloading technologies; (d) global infrastructures such as GENI[21] and Planetlab[22] for large-scale Fog-IoT experimentation; (e) AI and ML technologies. They suggest that with NFV in the Fog-IoT architecture, the Fog nodes essentially form an edge cloud computing platform with virtualization and sharing capability and each IoT application is delivered and deployed as an independent "slice" over the same physical Fog infrastructure. Also, they suggest that the Fog nodes need to orchestrate the deployment, manage resource allocations, and coordinate the collaborations between the Fog Servers and the resource-poor IoT devices by Onloading/Offloading.

The authors of (89) suggest SpeedyChain: a framework for decoupling data from blockchain for smart cities. Having in mind the lack of privacy and the vulnerability of data, that any centralized approach would result into regarding data transfers between in example thousands of cars, they propose SpeedyChain, a permissioned blockchain-based framework for ensuring resilient, decentralized and immutable management of smart city data. Vehicle to Infrastructure communication is kept secure and private by employing periodically changeable keys. They also, introduce an expiration time of a block, to avoid oversized blocks. Based on the approach presented by Lunardi (90), they suggest a lightweight permissioned blockchain that creates blocks on demand and each device produces information and appends data blocks to its own block. In order to overcome the resource intensive consensus algorithms they undertake the designated gateway nodes suggested again by Lunardi (90) .

The authors of (91) proposed an IoT system that is based on the Blockchain that will offer Homomorphic Computation and secure Storage. They suggest a threshold secure multi-party computing (TSMPC) protocol, were servers could execute homorphic computations on specific common parts (shares) and afterwards produce appropriate answers, while they will not be able to retrieve any information out of the processed data. They name their system BeeKeeper which offers the benefits of the immutable ledger, meaning that data can't get altered, erased or lost and also that all data that were verified publicly is trustworthy. Another characteristic is that the TSMPC protocol does more verification than the nodes, and all nodes could be appointed as a leader server if it comes to an agreement with it. BeeKeeper consists of record and light nodes, were every record

[21] www.geni.net
[22] www.planet-lab.org

node is interconnected to each other through a trustworthy P2P network and each light node is linked to a specific sum of record nodes. The record nodes preserve the functioning of the blockchain through a consensus scheme based on PBFT and store the whole list of the blockchain. On the contrary light nodes store just the block headers. The TSMPC protocol that they suggest and is responsible for securing the shares of the Beekeper is an extension of the SSS (Shamir's secret sharing) (92).

The authors of (93) proposed a hypergraph-based blockchain model. Differently from the first implied architecture of the blockchain technology that demands from every node of the network to be coordinated with the others and maintain the same data, they reduce the amount of nodes that keep the same synchronized network's data mirrors to the extent that the regular operation of the blockchain could be guaranteed. They implement hypergraph theory in order to divide the whole network to a lot of hyperedges that save portions of the generated transactions data thus reducing the storage burdens. By doing that additional risks regarding security arise, but they believe that will be able to scale them down by thoroughly tuning network parameters, specifically for IoT ecosystems. Storage structure of every node consists of two portions: the blockchain head and subBlockchains. The structure of the blockchain head includes a linear independence matrix, a vector and a Blockchain-list. The linear independence matrix consists of N linearly independent vectors forming a N-order integer matrix, and each vector is mapped to a hyperedge. The total amount of the network's hyperedges is illustrated by the N. Meaning that every distinct hyperedge of the BC network is linked with a distinct N-dimensional vector. That vector may be considered as the hyperedges identification. The blockchain-list includes various blockchain indexes and each one of them indicates a subchain. The actual amount of the subchains is equal with the node's degree. Subchains are something similar to a blockchain but they also have a head that contains an N-dimensional vector as a feature of the hyperedge. Every subchain saves concurrent transaction data independently in the hyperedge, and the hyperedges feature vector is identical to the one that is stored in the subchain head. This is why all nodes that are part of one hyperedge are obliged to be linked to the same subchain. The linear independence matrix is used to ease the changes that will come up after the network's evolvement, as it is hard to create new identification for new hyperedges simultaneously, but on the other hand with the use of a linear independence matrix one can easily create a linear independence vector.

6. Conclusion

The integration of Blockchain technology with the Internet of Thing is one of the hottest topics in technology nowadays and this is why many startup companies and individual researchers are competing to discover and deliver the most appropriate solution so as to take advantage of the benefits provided by the Blockchain in the vast, vulnerable and chaotic nature of the IoT ecosystem.

The number of connected devices increases as every device that may improve its functionality and enhance its services is being connected to the internet. Moreover, current and future trends in IoT ecosystems will require significant increase in edge computing services as the infiltration of IoT devices in our routine (cars, locks) will require instantaneous interactions among communicating devices, as latency will be unacceptable.

The benefits that Blockchain technology can bring to IoT are numerous such as, security through decentralized interaction and data exchange, the use of hashing algorithms to create an unchangeable record of transactions and the encryption of the information with the use of public and private keys. Also, the use of smart contracts, self-executing code that could be embedded on each IoT chip, may completely change the current transaction system as we know it.

However, as discussed in section 4.2 the barriers that must be overcome are numerous such as scalability, latency, throughput, sustainability and adoption issues. Regarding the latter, a huge step forward has been taken by semiconductor giants Intel and ARM as they recently made a strategic partnership to use common standards developed by Intel for securely managing such networks.

In *table 7*, we get a good idea about where the industry is heading to solve these issues, we see that six of the proposed projects base their functioning on existing trustworthy Blockchains networks. Eight use variants of PoW as a consensus mechanism, two use PBFT variants, three PoS variants and two use TEE. Regarding network access nine are based on public networks, three on permissioned and two on public/private. All projects support the use of smart contracts and only one doesn't have a native token.

Considering all the above, we see that already working products are based on existing blockchain networks and are using Trusted Execution Environments (TEE) to deal with security, throughput and latency issues. Current research initiatives are leaning towards the use of multichain schemes, less demanding consensus algorithms, edge/fog/mist computing plus other sharding techniques to deal with the above mentioned issues. Also many researchers propose the use of Software Defined Networks (SDN) to further enhance shardability and responsiveness.

But in order for this to be possible we still have a lot of ground to cover and as said by Mario Milicevic (communication systems engineer at MaxLinear) the blockchain technology is wildly understudied, in an IEEE database of 40 million research papers, only 480 contain the term "blockchain, and among them very few are about real – world blockchain networks that have been deployed.

Also, regarding security it is important to mention that if a centralized authority manages the network in case of an emergency, it has the ability to pull the plug, but that is not possible if in example rogue nodes take over majority in a blockchain network. Moreover, some question the fact that the blockchain networks should be considered truly as trustless environments as always you have to trust your software and hardware developers, meaning that either could place security backdoors in the device software or in the environment software and consequently take over the network manipulating transactions.

As of legal and compliance issues, another matter that should be taken under thorough consideration as described by Martha Bennett (Forrester analyst) “regarding responsibility issues in case of actions that are taken by devices, based on a rule that is automatically executed by a blockchain-based application, triggered by another blockchain-based application (you see the complexity)”.

As was mentioned earlier the integration problems are numerous and by some are believed as unsolvable, but the tremendous attention draught to this project may lead to innovation miracles and even if this effort does not give the expected results it may lead to other solutions that could solve the problem in other ways.

Bibliography

1. [Online] [Cited:] https://en.wikipedia.org/wiki/Internet_of_things.
2. www.postscapes.com. [Online] https://www.postscapes.com/internet-of-things-protocols/.
3. THE FOUR INTERNET OF THINGS CONNECTIVITY MODELS EXPLAINED. [Online] http://www.inetservicescloud.com/the-four-internet-of-things-connectivity-models-explained/.
4. **Xiaolin Jia, Quanyuan Feng, Taihua Fan, Quanshui Lei,.** RFID technology and its applications in Internet of Things (IoT). 2012. 2nd International Conference on Consumer Electron- ics, Communications and Networks (CECNet), IEEE DOI: 10.1109/CECNet.2012.6201508.
5. **N. Dharini, Ranjith Balakrishnan and A. Pravin Renold.** 'Distributed Detection of Flooding and Gray Hole Attacks in Wireless Sensor Network". 2015. International Conference on Smart Technologies and Management for Computing, Com- munication, Controls, Ene.
6. **Sarangi, Pallavi Sethi and Smruti R.** Internet of Things: Architectures, Protocols, and Applications. [Online] Department of Computer Science, IIT Delhi, New Delhi, India, 2017. https://doi.org/10.1155/2017/9324035.
7. **E. Vasilomanolakis, J. Daubert, M. Luthra.** On the Security and Privacy of IoT Architectures and Systems. [Online] 2015. https://www.researchgate.net/publication/282075370_On_the_Security_and_Privacy_of_ Internet_of_things_ Architectures_and_Systems.
8. IoT applications spanning across industries. [Online] https://www.ibm.com/blogs/internet-of-things/iot-applications-industries/.
9. **Das, Manik Lal.** *Privacy and Security Challenges in Internet of Things.* s.l. : Distributed Computing and, 2015.
10. **Bhattacharya, Sumit.** The Top Ten IoT Vulnerabilities. [Online] http://resources.infosecinstitute.com/the-top-ten-iot-vulnerabilities/#gref.
11. Top IoT Vulnerabilities. [Online] 2014. https://www.owasp.org/index.php/Top_IoT_Vulnerabilities.
12. **Kayleen Manwaring.** Beware the 'Internet of Things': Expert warns connected devices run risk of spying and hacking - and 40% of people now have them in their homes. [Online] 2017. http://www.dailymail.co.uk/sciencetech/article-4590176/From-spying-hacking-Expert-lists-dangers-IoT.html.
13. FBI Warns Public on Dangers of the Internet of Things. [Online] 2015. https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/fbi-warns-public-on-dangers-of-the-internet-of-things.
14. anking Is Only The Beginning: 36 Big Industries Blockchain Could Transform. [Online] 2018. https://www.cbinsights.com/research/industries-disrupted-blockchain/.
15. **Nakamoto, Satohi.** *"Bitcoin: A peer-to-peer electronic cash system,".* 2008.
16. **Ali Dorri, Salil S. Kanhere, Raja Jurdak, and Praveen Gauravaram.** *A Lightweight Scalable BlockChain for IoT.*
17. **Christidis, K.** *Blockchains and Smart Contracts for the IoT.* 2016. 10.1109/ACCESS.2016.2566339.
18. **Michael Crosby, Nachiappan, Pradhan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman.** *BlockChain Technology Beyond Bitcoin.* s.l. : Sutardja Center for Entrepreneurship & Technology Technical Report, 2015.
19. wikipedia. [Online] https://en.wikipedia.org/wiki/Sybil_attack.
20. **Tessone, Paolo Tasca and Claudio J.** *Taxonomy of Blockchain Technologies Principles of Identification and Classification.* 2018. https://ssrn.com/abstract=2977811.
21. **Bryk, Anna.** Blockchain: Cyber Security Pros and Cons. [Online] 2017. https://www.apriorit.com/dev-blog/462-blockchain-cybersecurity-pros-cons.

22. **Dickson, Ben.** [Online] 2016. https://techcrunch.com/2016/12/05/how-blockchain-can-help-fight-cyberattacks/.
23. **Liskov, M. Castro and B.** *Practical byzantine fault tolerance," in.* New Orleans, Louisiana, USA : (OSDI),, 1999.
24. **Witherspoon, Zane.** A Hitchhiker's Guide to Consensus Algorithms. [Online] https://hackernoon.com/a-hitchhikers-guide-to-consensus-algorithms-d81aae3eb0e3.
25. **Tien Tuan Anh Dinh, Rui Liu, Meihui Zhang, Gang Chen, Beng Chin Ooi and Ji Wang.** *Untangling Blockchain: A Data Processing View.* s.l. : ieee, 2017. 1041-4347.
26. **Castor, Amy.** A (Short) Guide to Blockchain Consensus Protocols. [Online] 2017. https://www.coindesk.com/short-guide-blockchain-consensus-protocols/.
27. **Lee, Sherman.** Explaining Directed Acylic Graph (DAG), The Real Blockchain 3.0. [Online] 2018. https://www.forbes.com/sites/shermanlee/2018/01/22/explaining-directed-acylic-graph-dag-the-real-blockchain-3-0/#55ef9bc2180b.
28. **E. Heilman, A. Kendler, A. Zohar, and S. Goldberg.** *Eclipse attacks on bitcoin's peer-to-peer network.* Washington, D.C. : (USENIX Security),, Washington, D.C.,.
29. PoS. [Online] https://en.wikipedia.org/wiki/Proof-of-stake.
30. **Rosic, Ameer.** [Online] https://blockgeeks.com/guides/blockchain-applications/.
31. Banking Is Only The Beginning: 36 Big Industries Blockchain Could Transform. [Online] https://www.cbinsights.com/research/industries-disrupted-blockchain/.
32. **Rosic, Ameer.** 5 Blockchain Applications That Are Shaping Your Future. [Online] https://www.huffingtonpost.com/ameer-rosic-/5-blockchain-applications_b_13279010.html.
33. **James, Febin John.** Popular Use Cases of Blockchain Technology You Need to Know. [Online] https://hackernoon.com/popular-use-cases-of-blockchain-technology-you-need-to-know-df4e1905d373.
34. **ianjun Sun, Jiaqi Yan and Kem Z. K. Zhang.** *Blockchain-based sharing services: What blockchain technology can contribute to smart cities.* s.l. : School of Information Management, Nanjing University,Nanjing, China, 2016.
35. **Banafa, Ahmed.** [Online] 2016. https://datafloq.com/read/securing-internet-of-things-iot-with-blockchain/2228.
36. **Williams, Sean.** 5 Big Advantages of Blockchain, and 1 Reason to Be Very Worried. [Online] https://www.fool.com/investing/2017/12/11/5-big-advantages-of-blockchain-and-1-reason-to-be.aspx.
37. **PRADIP KUMAR SHARMA, MU-YEN CHEN AND JONG HYUK PARK.** *A Software Defined Fog Node Based Distributed.* 2017. 10.1109/ACCESS.2017.2757955.
38. **Marco Conoscenti, Antonio Vetr`, Juan Carlos De Martin.** *Blockchain for the Internet of Things: a Systematic Literature Review.* s.l. : IEEE. 10.1109/AICCSA.2016.7945805.
39. **Papermaster, Mark.** Blockchain and Its Implementation Challenges. [Online] https://www.networkcomputing.com/network-security/blockchain-and-its-implementation-challenges/945374178.
40. Eris:Legal,. [Online] Eris Industries, 2016. https://erisindustries.com/components/erislegal/.
41. Quantum computing. [Online] https://en.wikipedia.org/wiki/Quantum_computing.
42. Elliptic. [Online] https://www.elliptic.co/.
43. **F. Zhang, E. Cecchetti, K. Croman, and E. Shi.** *Town crier: an authenticated data feed for smart contracts.* s.l. : IEEE, 2016.
44. Thin client. [Online] https://en.wikipedia.org/wiki/Thin_client.
45. **Harding, David A.** Thin Client. [Online] 2015. https://bitcoin.stackexchange.com/questions/32529/what-is-a-thin-client.
46. EIP 105 (Serenity): Binary sharding plus contract calling semantics #53. [Online] 2016. https://github.com/ethereum/EIPs/issues/53.

47. **Loi Luu, Viswesh Narayanan, Chaodong Zheng, Chaodong Zheng, Seth Gilbert, Prateek Saxena.** *A Secure Sharding Protocol For Open Blockchains.* s.l. : National University of Singapore.
48. [Online] https://www.zilliqa.com/.
49. **deadalnix.** Introducing Merklix tree as an unordered Merkle tree on steroid. [Online] 2016. https://www.deadalnix.me/2016/09/24/introducing-merklix-tree-as-an-unordered-merkle-tree-on-steroid/.
50. **Ray, James.** On sharding blockchains. [Online] https://github.com/ethereum/wiki/wiki/Sharding-FAQ#on-sharding-blockchains.
51. **Cisco.** *Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are.* s.l. : Cisco.
52. **Ray, Brian.** The Role of Cloud Computing and Fog Computing in IoT. *Brian Ray.* [Online] 2017. https://www.iotforall.com/cloud-fog-computing-iot/.
53. **Rouse, Margaret.** fog computing (fog networking, fogging) . [Online] 2016. https://internetofthingsagenda.techtarget.com/definition/fog-computing-fogging.
54. **MSV, Janakiram.** Is Fog Computing The Next Big Thing In Internet of Things? [Online] 2016. https://www.forbes.com/sites/janakirammsv/2016/04/18/is-fog-computing-the-next-big-thing-in-internet-of-things/#47d5dd8e608d.
55. **Michaela Iorga, Larry Feldman, Robert Barton, Michael J Martin, Nedim Goren, Charif.** *Fog Computing Conceptual Model.* s.l. : NIST, 2018. https://doi.org/10.6028/NIST.SP.500.
56. **Thanasis Loukopoulos, Nikos Tziritas, Maria G. Koziri, Georgios I. Stamoulis, Samee Khan:.** *A Pareto-Efficient Algorithm for Data Stream Processing at Network Edges.* s.l. : CloudCom , 2018. 159-162.
57. **Thanasis Loukopoulos, Nikos Tziritas, Maria G. Koziri, George Stamoulis, Samee U. Khan, Cheng-Zhong Xu, Albert Y. Zomaya:.** *Data Stream Processing at Network Edges.* s.l. : IPDPS Workshops , 2018. 657-665.
58. filament.com. [Online] https://filament.com/products/.
59. **Filament.** *Foundation for the Next Economic Revolution, Distributed Exchange and the Internet of Things.*
60. [Online] https://www.ibm.com/watson/.
61. SLOCK.IT. *https://slock.it/landing.html.* [Online]
62. **Jentzsch, Christoph.** Slock.it IoT Layer. [Online] https://blog.slock.it/slock-it-iot-layer-f305601df963.
63. Streamr. [Online] https://www.streamr.com/faq#vision.
64. https://medium.com/int-chain. [Online] https://medium.com/int-chain/real-valuable-blockchain-int-chain-5ae92673b253.
65. [Online] https://medium.com/int-chain/int-chain-release-d580e6f5e68b.
66. intchain.io. [Online] https://intchain.io/whitepaper/INT-whitepaper-release-EN.pdf.
67. [Online] iotex. https://iotex.io/.
68. iota. [Online] https://www.iota.org/get-started/what-is-iota.
69. **TheCoinEconomy.** IOTA & the Tangle: The Future Backbone of the IoT. [Online] 2017. https://hackernoon.com/iota-the-tangle-the-future-backbone-of-the-iot-e7e417d5d86b.
70. **Weeve.** [Online] April 2018. https://medium.com/weeves-world/weeve-frequently-asked-questions-answered-6ba5fadb1980.
71. bitcoinist.com. [Online] Μαρτιος 2018. https://bitcoinist.com/how-nbt-and-weeve-are-solving-the-scaling-issue-of-ethereum/.
72. weeve. [Online] https://weeve.network/.
73. contractnet. [Online] https://contractnet.com/.
74. [Online] https://bitcoinexchangeguide.com/contractnet-cnet-ico/.

75. **Jagati, Shiraz.** cryptoslate.com. [Online] March 2018. https://cryptoslate.com/introduction-waltonchain-business-ecosystem-integrating-blockchain-iot/.
76. WaltonChain Whitepaper (V1.0.5). [Online] 05 24, 2018. https://www.waltonchain.org/templets/default/doc/Waltonchain-whitepaper_EN_20180525.pdf.
77. Waltonchain. [Online] July 2018. https://medium.com/@Waltonchain_EN/report-on-the-waltonchain-global-super-master-node-recruitment-program-launch-ceremony-c8836b976ebb.
78. sdchain. [Online] https://www.sdchain.io/.
79. One Block Away ICOs. *medium.com.* [Online] 2018. https://medium.com/@OneBlockAwayICO/quark-chain-one-to-rule-all-a-true-decentralized-blockchain-thoughtfully-designed-636c5ac02eac.
80. [Online] https://quarkchain.io/.
81. [Online] https://atonomi.io/.
82. **Vaughan Emery, David Fragale, Andrii Zamovsky, Peter Kinnaird.** *Atonomi. The secure ledger of things. Whitepaper.*
83. **XAIN.** XAIN. [Online] April 2018. https://medium.com/@XAIN/part-1-technical-overview-of-the-porsche-xain-vehicle-network-f70bb117be16.
84. **T. Duong, L. Fan, and H.S. Zhou.** 2-hop blockchain: Combining proof-of-work and proof-of-stake securely. *Cryptol. ePrint Arch.,Tech. Rep. 2016/716.* [Online] https://eprint.iacr.org/2016/716.pdf.
85. **Shi-Cho Cha, Jyun-Fu Chen , Chunhua Su , and Kuo-Hui Yeh.** *A Blockchain Connected Gateway for BLE-based Devices in the Internet of Things.* 2017. DOI 10.1109.
86. **Gokhan Sagirlar, Barbara Carminati , Elena Ferrari , John D. Sheehany , Emanuele Ragnoliy.** *Hybrid-IoT: Hybrid Blockchain Architecture for Internet of Things - PoW.* s.l. : University Of Insubria, Italy {gsagirlar, barbara.carminati, elena.ferrari}@uninsubria.it, 2018. arXiv:1804.03903v3 .
87. **Zijian Baoa, Wenbo Shi, Debiao He, Kim-Kwang Raymond Choo.** *IoTChain: A Three-Tier Blockchain-based IoT Security Architecture.* 2018. rXiv:1806.02008v2 .
88. **Jianli Pan, Yuanni Liu, Jianyu Wang, Austin Hester,.** *Key Enabling Technologies for Secure and Scalable Future Fog-IoT Architecture: A Survey.* 2018. arXiv:1806.06188v1 .
89. **Regio A. Michelin, Ali Dorri, Roben C. Lunardi, Marco Steger, Salil S. Kanhere, Raja Jurdak, Avelino F. Zorzo.** *SpeedyChain: A framework for decoupling data from blockchain for smart cities.* 2018. arXiv:1807.01980v1 .
90. **R. C. Lunardi, R. A. Michelin, C. V. Neu, and A. F. Zorzo,.** *access control on iot ledger-based architectur.* Taipei : s.n., 2018. IEEE/IFIP etwork Operations and Management Symposium (NOMS 2018).
91. **LIJING ZHOU, LICHENG WANG , YIRU SUN, AND PIN LV.** *BeeKeeper: A Blockchain-Based IoT System With Secure Storage and Homomorphic Computation.* 2018. 10.1109/ACCESS.2018.2847632.
92. **Shamir, A.** *How to share a secret.* Commun. ACM, vol. 22, no. 11,.
93. **Chao Qu ID, Ming Tao and Ruifen Yuan I.** *A Hypergraph-Based Blockchain Model and Application in Internet of Things-Enabled Smart Homes.* Dongguan 523808, China; : School of Computer Science and Network Security, Dongguan University of Technology, 2018.