NyronChain™ Technical Whitepaper

"Integrating blockchain with the new IOT world"

Version 1.2 | 12/02/2018

COPYRIGHT © 2018 NyronChain Foundation Inc. All Rights Reserved

Legal disclaimer

NOTHING IN THIS TECHNICAL WHITEPAPER CONSTITUTES LEGAL, FINANCIAL, BUSINESS OR TAX ADVICE AND YOU SHOULD CONSULT YOUR OWN LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISER BEFORE ENGAGING IN ANY ACTIVITY IN CONNECTION HEREWITH. NEITHER NYRONCHAIN FOUNDATION LTD. (THE FOUNDATION), ANY OF THE PROJECT TEAM MEMBERS WHO HAVE WORKED ON THE NYRONCHAIN PLATFORM (AS DEFINED HEREIN) OR PROJECT TO DEVELOP THE NYRONCHAIN PLATFORM IN ANY WAY WHATSOEVER (THE NYRONCHAIN TEAM) NOR ANY SERVICE PROVIDER SHALL BE LIABLE FOR ANY KIND OF DIRECT OR INDIRECT DAMAGE OR LOSS WHATSOEVER WHICH YOU MAY SUFFER IN CONNECTION WITH ACCESSING THIS TECHNICAL WHITEPAPER, THE BUSINESS WHITEPAPER, THE WEBSITE AT HTTPS://WWW.NYRONCHAIN.ORG/ OR ANY OTHER MATERIALS PUBLISHED BY THE FOUNDATION.

All contributions will be applied towards the Foundation's objects, including without limitation promoting the research, design and development of, and advocacy for a scalable, extensible, cost efficient, protocol-agnostic and easy-to-use platform for building a new IoT generation, which would overcome many of the existing technological barriers faced by existing platforms and which is designed to be a self-evolving ecosystem. This Technical Whitepaper is intended for general informational purposes only and does not constitute a prospectus, an offer document, an offer of securities, a solicitation for investment, or any offer to sell any product, item or asset (whether digital or otherwise). The information herein below may not be exhaustive and does not imply any elements of a contractual relationship. There is no assurance as to the accuracy or completeness of such information and no representation, warranty or undertaking is or purported to be provided as to the accuracy or completeness of such information. Where this Technical Whitepaper includes information that has been obtained from third party sources, the Foundation and/or the NyronChain team have not independently verified the accuracy or completion of such information. This Technical Whitepaper does not constitute any offer by the Foundation or the NyronChain team to sell any NYR (as defined herein) nor shall it or any part of it nor the fact of its presentation form the basis of, or be relied upon in connection with, any contract or investment decision. Nothing contained in this Technical Whitepaper is or may be relied upon as a promise, representation or undertaking as to the future performance of the NyronChain Platform. The agreement between the Foundation (or its affiliate) and you, in relation to any sale and purchase of NYR is to be governed by only the separate terms and conditions of such agreement. By accessing this Technical Whitepaper or any part thereof, you represent and warrant to the Foundation, its affiliates and the NyronChain team as follows: (a) you acknowledge, understand and agree that NYR may have no value, there is no guarantee or representation of value or liquidity for NYR, and NYR is not for speculative investment; (b) none of the Foundation, its affiliates, and/or the NyronChain team members shall be responsible for or liable for the value of NYR, the transferability and/or liquidity of NYR and/or the availability of any market for NYR through third parties or otherwise; (c) in any decision to purchase any NYR, you have not relied on any statement set out in this Technical Whitepaper; (d) you will and shall at your own expense ensure compliance with all laws, regulatory requirements and restrictions applicable to you (as the case may be); and (e) you acknowledge, understand and agree that you are not eligible to purchase any NYR if you are a citizen, national, resident (tax or otherwise), domiciliary and/or green card holder of a geographic area or country (i) where it is likely that the sale of NYR would be construed as the sale of a security (howsoever named) or investment product and/or (ii) in which access to or participation in the NYR token sale or the NyronChain Platform is prohibited by applicable law, decree, regulation, treaty, or administrative act, and/or (including without limitation The United States of America, The People's Republic of China, New Zealand, and the Republic of Korea). The Foundation and the NyronChain team do not and do not purport to make, and hereby disclaims, all representations, warranties or undertaking to any entity or person. Prospective purchasers of NYR should carefully consider and evaluate all risks and uncertainties (including financial and legal risks and uncertainties) associated with the NYR token sale, the Foundation and the NyronChain team. The information set out in this Technical Whitepaper is for community discussion only and is not legally binding.

All statements contained in this Technical Whitepaper, statements made in press releases or in any place accessible by the public and oral statements that may be made by the Foundation and/or the NyronChain team may constitute forward-looking statements (including statements regarding intent, belief or current expectations with respect to market conditions, business strategy and plans, financial condition, specific provisions and risk management practices). You are cautioned not to place undue reliance on these forward-looking statements given that these statements involve known and unknown risks, uncertainties and other factors that may cause the actual future results to be materially different from that described by such forward-looking statements. These forward-looking statements are applicable only as of the date of this Technical Whitepaper and the Foundation and the NyronChain team expressly disclaims any responsibility (whether express or implied) to release any revisions to these forward-looking statements to reflect events after such date. This Technical Whitepaper may be translated into a language other than English and in the event of conflict or ambiguity between the English language version and translated versions of this Technical Whitepaper, the English language version shall prevail. You acknowledge that you have read and understood the English language version of this Technical Whitepaper. No part of this Technical Whitepaper is to be copied, reproduced, distributed or disseminated in any way without the prior written consent of the Foundation

Table of Contents

Abstract

NyronChain is a platform and an ecosystem for the new Internet of Things (IoT) world. The platform goes beyond providing the necessary foundational components for using internet to power complex business rules. It connects your existing system to blockchain networks, enabling you to automate business processes using the data and identities associated with existing systems.

With yearly shipments of more than 10 billion microcontrollers that all can exchange information locally or through the Internet, a huge variety of so called “intelligent devices” are enabled. All these devices can be accessed over the Internet and this evolution is commonly referred to as Internet of Things (IoT). IoT typically requires a local low power wireless connection along with the Internet connection. For most such applications and solutions, a gateway is required to connect sensor nodes to the Internet via a local infrastructure or using a cellular connection. Gateways are important components of the IoT vision. These gateways can be used to connect Bluetooth low energy devices to the Internet and can also be used as "repeaters" to extend the system range. This whitepaper describes how Bluetooth low energy technology works and how it can be used to connect devices to Internet-based services and applications. A significant feature in Bluetooth low energy compared to other IoT wireless technologies is the support for smartphones and tablets. The whitepaper thus also describes how a smartphone or tablet can be used in IoT.

Introduction

1.1 Motivation

The fast development of the Internet and associated technologies, namely regarding the possibility of connection to physical (smart) objects, has opened new perspectives and opportunities for developments that can have a deep impact on the society. Internet of Things (IoT) will include services, networks, and any connectable devices, anyone who intends to use IoT, at any time, in anyplace. These features provide connectivity at a much larger scale than the Internet as we know it today. With the number of objects with capability of connection to the Internet growing exponentially, a new generation of Internet, the IoT, is being established. In this IoT context, objects will be able to be connected and accessible anytime and anywhere, creating new possibilities for applications, taking full advantage of the access to those objects. A wide range of application domains, including smart grid, transportation, health care, smart cities, safety, among others can benefit from these new perspectives and better support the needs of our society. This leads to the so called “Vision of IoT”.

1.2 Introduction to our technology

Bluetooth low energy was introduced back in 2011 as the hallmark feature of Bluetooth v4.0. Bluetooth low energy is ideal for applications requiring episodic or periodic transfer of small amounts of data. Therefore, Bluetooth low energy is especially well suited for sensors, actuators and other small devices that require extremely low power consumption.

Bluetooth low energy features:

- Works well with high numbers of communication nodes with limited latency requirements
- Very low power consumption
- Robustness equal to Classic Bluetooth
- Short wake-up and connection times
- Good smartphone and tablet support

In general terms, a beacon is a small, battery-powered, wireless device that uses Bluetooth low energy technology (Bluetooth Smart) to advertise its presence and services. It does this by repeatedly broadcasting or advertising a beacon identifier to compatible smartphones or tablets within its proximity. The smartphone or tablet can then use the beacon’s information to determine its location and services, and act accordingly. Beacons enable proximity-based customized experiences for users. Beacons are generally used for proximity-aware applications. By monitoring beacons, a device can detect when it has entered or exited a area, and then use that information to create interactive experiences based on what’s nearby.

The global Bluetooth beacon market size is expected to reach USD 58.7 billion by 2025, according to a new report by Grand View Research, Inc. The introduction of next-generation software-based and virtual beacons are expected to boost the market demand. The key factor driving the industry growth is the increased number of applications powered by beacons and Bluetooth Low Energy (BLE) tags. Beacons are witnessing growing penetration across asset tracking and machine/equipment status observation in high volume verticals. At the same time, the markets for both existing and new applications are maturing, leading to larger roll-outs.

Growing integration of beacons in cameras, LED lightings, point of sale (POS) devices, digital signage, and vending machines is expected to propel the industry growth over the forecast period. Apart from retail applications, beacons are also projected to become a common commodity in industrial applications. Industries are increasingly shifting toward the incorporation of Bluetooth-powered solutions from conventional proximity solutions including Wi-Fi and RFID. Assets based on Wi-Fi, RFID, and people flow tracking systems have currently captured a significant revenue share in the healthcare and intra-logistics sectors. The relatively lower price point of Bluetooth-based solutions is playing a pivotal role in their large-scale adoption in various domains such as indoor navigation, worker security, elderly care, and affordable asset tracking.

A relatively new concept, Bluetooth beacons can help apps running on mobile devices to determine their precise location. The technology they are based upon is inexpensive to mass-produce, with the BLE chip costing less than a dollar. In many cases, beacons can provide a smartphone with location information with greater precision than that offered by alternative technologies, such as GPS, Wi-Fi and cell tower triangulation. Importantly, beacons also work well indoors, enabling them to be used in a wide variety of applications, such as triggering information / offers upon entering a retail store, surfacing tickets at entry to a transit station and initiating a transaction at a retail point of sale. In some use cases, the app may need to use a cellular or WIFI connection to display relevant content, while in other cases the app can simply pull up the content from a local cache.

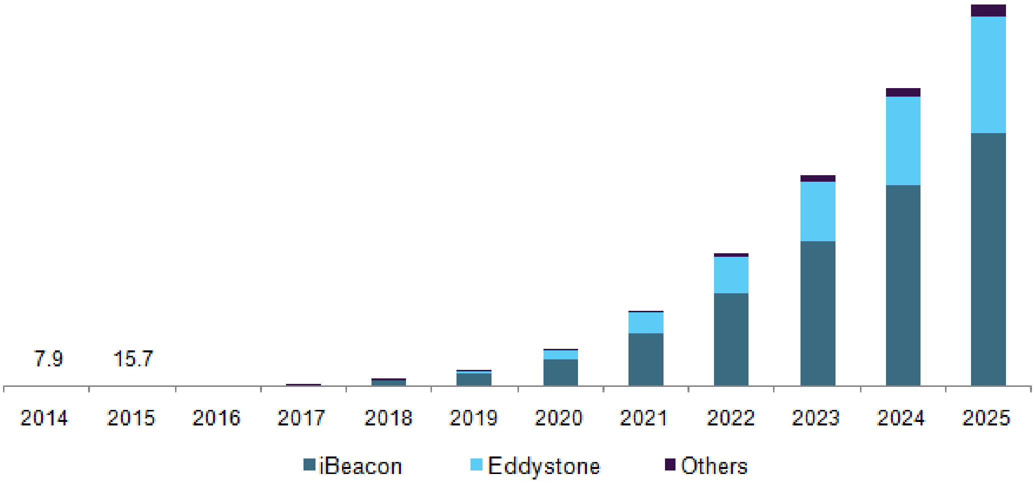
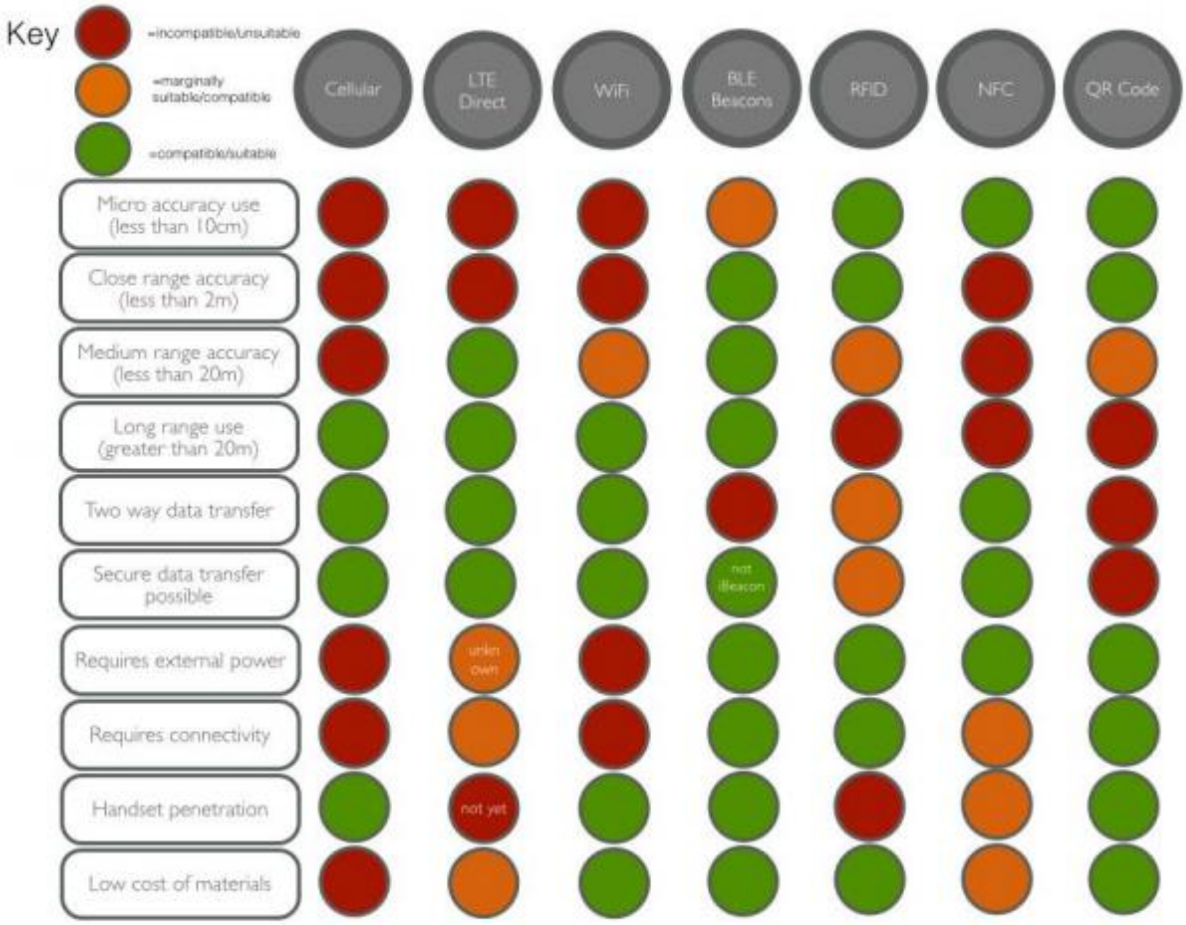


Fig. 1 – Expected growth of the most known BLE technology-based beacons brands

1.3 Other solutions

There are numerous technologies, such as Wi-Fi and RFID, in the market today that can perform some, all or more of the tasks that beacons can perform. They each have specific strengths and weaknesses. Table below gives a very high-level overview of some of these technologies and how they compare with beacons.



Key
🟥 =incompatible/unsuitable
🟧 =marginally suitable/compatible
🟩 =compatible/suitable

	Cellular	LTE Direct	WiFi	BLE Beacons	RFID	NFC	QR Code
Micro accuracy use (less than 10cm)	🟥	🟥	🟥	🟧	🟩	🟩	🟩
Close range accuracy (less than 2m)	🟥	🟥	🟥	🟩	🟩	🟥	🟩
Medium range accuracy (less than 20m)	🟥	🟩	🟧	🟩	🟧	🟥	🟧
Long range use (greater than 20m)	🟩	🟩	🟩	🟩	🟥	🟥	🟥
Two way data transfer	🟩	🟩	🟩	🟥	🟧	🟩	🟥
Secure data transfer possible	🟩	🟩	🟩	🟩 not iBeacon	🟧	🟩	🟥
Requires external power	🟥	🟧 unknown	🟥	🟩	🟩	🟩	🟩
Requires connectivity	🟥	🟧	🟥	🟩	🟩	🟧	🟩
Handset penetration	🟩	🟥 not yet	🟩	🟩	🟥	🟧	🟩
Low cost of materials	🟥	🟧	🟩	🟩	🟩	🟧	🟩

Fig. 2 – Comparison of available IoT technology

1.4 Use Cases

There are several different generic interactions that can be enabled by beacons working in conjunction with mobile apps.

Deliver relevant content

A beacon may trigger an app to deliver information to an individual based upon their location. Typically, content falls into one of the following categories:

- An offer: This may take the form of information or an actionable coupon (for example a barcode or NFC tap).
- Loyalty: Surfacing a loyalty card which may be used to collect points at the point of sale (PoS) or as the result of a visit.
- Ticket: A ticket for entrance to a transit station or some form of event/entertainment, typically rendered as a QR code or NFC tap.
- Downloadable/streamable content: Content such as video, audio, document or app.
- Information/guidance: Text or graphical guidance aimed at assisting an individual or informing them of something relevant to their time/location.

Facilitate payment

Beacons can play a role in either initiating a payment action or forming part of the location verification. A beacon may alert an app that a consumer has entered a store where payment can be made using the app. The app may then take two possible actions (or both):

- Issue the consumer with a one-time or location-specific payment token to be used at the PoS.
- Inform the PoS that a particular customer is on the premises and can pay using their app (and issue the PoS with a token). This may or may not require the app to interact with the PoS.

Or the beacon may simply be used to inform the consumer that they can pay with a payment mechanism, with no location specific payment interaction.

Enable check-in

A check-in is any action that an app performs as a result of being aware of beacon proximity, but does not necessarily require the consumer to directly interact or be informed. For example, a check-in may reward a consumer for visiting a particular location, without the individual having to interact with an app. A beacon could also trigger a social location check-in by an app, such as Foursquare (with the approval of the consumer). Note, the app does not necessarily need to alert a consumer when they come into range of a beacon. A retailer's app might simply record when a customer enters a store, how often they visit, which stores they visit, how long they stay and even their path through the store. However, consumers should be made aware of any such tracking and gain an explicit benefit from sharing their location in this way

Track an Item (Supply management)

Beacons are not always stationary items with a designated specific longitude and latitude. Beacons can also be attached to mobile items, where location is a measure of proximity to a 'tagged' item. For example, a suitcase may have a beacon attached, enabling the luggage owner to know when they are in range of their suitcase, or importantly, when their luggage goes out of range.

The role of beacons in retail

More than two thirds of American consumers say that a timely, relevant notification that offers value will influence their shopping decision there and then. Beacons can help deliver these notifications, prompting spontaneous purchasing decisions, while facilitating engagement through mobile loyalty programs. Removing the need to carry a plastic loyalty card, retailers' mobile apps can also enhance the shopping experience with gamification, and surprise and delight techniques. Beacons can perform the simple job of reminding the consumer to use the retail app at the right point in time.

Public Service

Location-oriented alerts can help local councils, tourist boards and public services surface content at the right time and place, such as historic facts on a city tour or information on nearby attractions or facilities, interactive learning, resource management, asset tracking and RTLS.

Healthcare

Beacons, combined with apps, can be used to check patients into hospital departments or surgeries and provide internal directions or relevant information. Beacons can also be used by healthcare insurers and associated partners, such as a network of gyms. For example, a health insurer could encourage customers to stay fit by rewarding them for gym visits. In Appendix 2 of this paper, we have outlined some of the potential use cases in healthcare.

Financial services

Banks can use beacons to engage consumers when they are making purchases. For example, triggered by a beacon, a banking app could remind a consumer that they can use their bank card in a retail setting, and perhaps offer them an incentive. Banks could also offer consumers (who have opted in) specific financial services in third party locations. For example, if a banking app detects that a consumer has spent a long time in a jeweler, it is perhaps time to offer them home contents insurance, or at least remind them to add the item they just bought to their existing policy. Banks could also use beacons on their own premises to improve customer service and to engage customers in a wider set of products and services.

Outdoor Media

Brokers of outdoor advertising could use cloud platforms and content management systems to offer an advertiser short term access to beacons at outdoor media sites to coincide with advertising campaigns. If a consumer has downloaded an app that monitors for an advertising broker's beacons, they could receive a notification enabling them to buy the product or service on the advertising hoarding they are looking at.

Smart Cities / Home automation

Environmentalists are hoping for better efficiency and less waste. Everyday people would love futuristic and easier ways to get around and use their city. Politicians and businesses alike are looking for ways to save funds and make new possibilities available.

Several cities have the beginnings of a smart system in place, and many more are looking into their options. Of course, the bulk of these solutions have not yet been finessed or even created.

Some of the most popular smart city IoT solutions include:

- smart lights
- smart grids
- automated traffic lights and parking
- data-driven transportation
- sensor-equipped… *everything*

Standardization between devices will paramount to making this happen. Not every device will speak the exact same language, but there will be a need to send that data from one place to another constantly. Because of Bluetooth's incredible penetration rates, high efficiency and the increased capabilities of Bluetooth 5, it is the standard that will connect the millions of Things in our future smart cities.

1.5 Integrating blockchain with NyronChain beacons

In an environment such as a smart home or factory, various devices equipped with sensors, which are closely interconnected using a private blockchain, can be configured to operate more safely and reliably in accordance with each other's conditions. A public blockchain is configured to perform not only user authentication but also mutual authentication between devices.

The use of private blockchains is only practical if they can interact with a public blockchain which is already operating. In this regard, we provide NyronChain, a platform and cryptocurrency-enabled public blockchain that can be effectively used with multiple private blockchains. In other words, with our blockchain-by-use, transactions are possible beyond the P2P settlement of the public blockchain. In a controlled private blockchain network, we implement NyronChain for mutual contracts and transactions between IoT devices, thereby enabling more accessible, reliable, and secure consumption and M2M transaction processes.

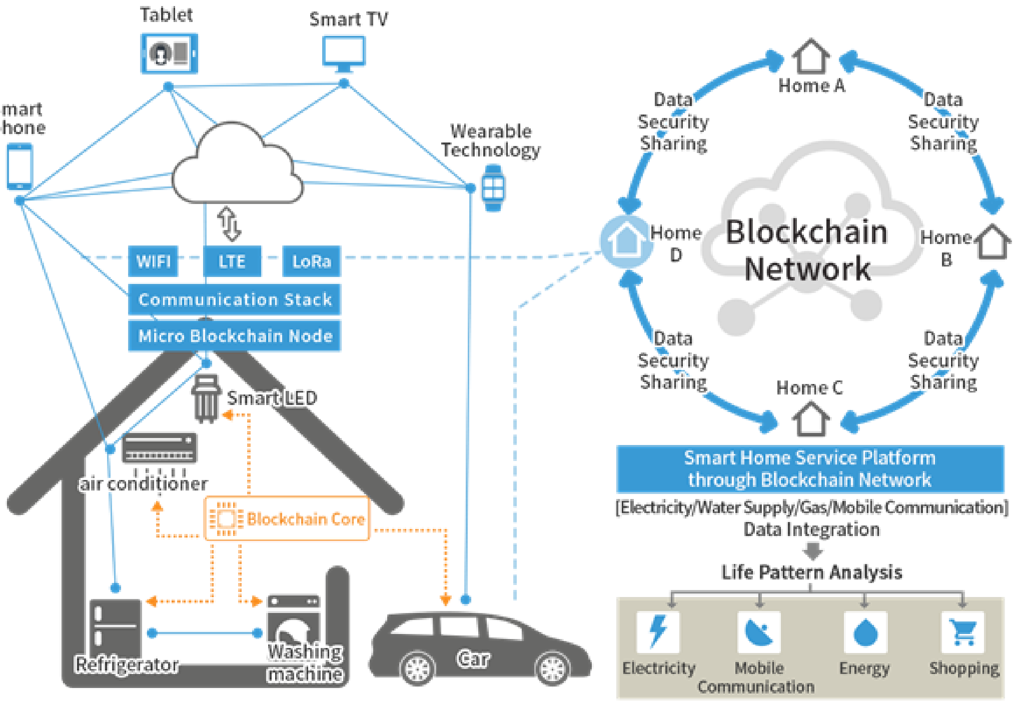


Fig. 3 – Example of a blockchain enabling IoT usage

1.6 IoT components

Although there are many different existing and emerging IoT architecture patterns, they all share one set of components in common – the concepts of physical device, edge and platform. The following subsections describe these concepts in detail and set the common terminology used throughout this White Paper.

Physical device

In today's IoT system architectures, the "things" encompassed in the Internet of Things go by many names, including cyber-physical device, device, end-point, entity and human entity. All these things share a common attribute regardless of the domain in which they reside, namely their individual identity as a physical device. These physical devices may contain some level of computing power, either embedded in the device or directly attached in the form of their actuators or controllers. The physical devices may also be connected directly to other physical devices, edge platforms, gateways and to one or more IoT systems.

Edge

In today's IoT system architectures, the concept of the "edge" refers to the aspect that comprises the operational domain of the overall IoT system. The edge typically consists of sensors, controllers, actuators, tag and tag readers, communication components, gateways and the physical devices themselves. The edge is where operational components connect, communicate and interact with each other, with the platform and in some cases directly with components in other edges. The edge can be as small as a single physical device with a direct connect to a platform, or as large as a manufacturing plant comprising all manufacturing equipment with a comprehensive communications functional component and edge computing platform, or anything in between. Within the edge, there may or may not be a platform to support processing. The edge communication component can consist of an independent local area network or networks where the components connect using one or more protocols and zero (direct connect to gateway) or more routers to connect to an edge gateway/hub/bus, which in turn connects to larger networks or cloud-based solutions that include the platform. The local network can use hub and spoke, mesh, WIFI, cellular or other topology for internal connections and connection to the gateway/hub. Edge processing addresses requirements and/ or limitations of the edge components or system functionality. These requirements and limitations include device connectivity as devices, such as those in industrial settings, may only have local connectivity capabilities. Other requirements comprise appropriate handling of devices with offline operation, i.e. since certain devices may not be connected online 24x7, these devices collect data while offline and upload the data when connected. In addition, there may be a need or a desire for edge analytics, edge transaction processing or another edge functionality as an extension of, or independently of, the IoT platform. As not all data should or needs to be transferred to the platform for storage, the edge provides local storage capabilities. To reduce the volumes of data to be transferred to the platform, an edge processing is often required that enables dynamic filtering or sampling or aggregating device data.

Platform

In today's IoT system architectures, the concept of an IoT platform is typically expressed as referring to the central hub of domains that collectively constitute the physical realization of the functional view of an architecture encompassing one or more aggregated edge environments. The IoT platform is an integrated physical/virtual entity system employing various applications and components to provide fully interoperable IoT services and management of those services. This includes, but is not limited to, networks, IoT environments, IoT devices (sensors, controllers, actuators, tags and tag readers, gateways) and the attached physical devices, IoT operations and management, and external connectivity with suppliers, markets and temporary stakeholders of the IoT system. The typical IoT platform either contains, or interacts with the following domains:

- **Control -** Comprises functions executed by the controlling mechanisms to enable the IoT devices to include sensing, actuation, communication, asset management and execution. In an industrial environment, control systems are typically located in proximity to the IoT device connected to the physical device. In a consumer environment, the control systems could be proximity located or remotely located. In a public environment, the control systems will typically include a combination of proximity or remote.
- **Operations** – Typically on the IoT platform and optimizing operations across multiple control domains, it includes prognostics, optimization, monitoring and diagnostics, provisioning and deployment, and management.
- **Information -** Typically on the IoT platform but also emerging as part of the edge, it comprises core IoT analytics and data and is responsible for gathering, transforming, persisting and modelling the data to support optimized decision making, system-wide operations and improvement of system models.
- **Application -** Typically on the IoT platform but can also contain components that are part of the business domain. Typically consists of the application program interface, user interface and logic and rules and is responsible for implementing logic that realizes functionalities for the IoT system itself
- **Business domain -** Typically on a platform separate from those of the core IoT functions defined in the operations, information, application and to some extent control domains, it integrates the IoT functionalities with back end applications such as CRM, ERP, billing and payments.

The IoT platform itself can be in the cloud, located on premise or involve a combination of the two. It can comprise a single server, multiple servers or a combination of physical and virtual servers. Regardless of its physical location or architecture, the domains that comprise the IoT platform – operations, information, application and perhaps even aspects of business and control – contain multiple data and control flows with one another, with the back-end applications of the business domain and with the physical systems/ control domain that resides in the edge. Additional services of the IoT platform can include resource interchanges to enable access to resources outside of the IoT system, network services, cloud integration services and many other services as defined by the individual platform provider.

Appendix 1: NyronChain Blockchain

1.1 Blockchain Based New Secure Multi-Layer Network Model for IoT

The centric network model can support cross-regional networking of devices and utilize the services provided by the central server to greatly enhance and leverage the performance of the devices themselves. It can also obtain a large amount of data from a variety of heterogeneous devices to form the basis of Big-data services. Correspondingly, the central model has a high-performance requirement for the cloud platform, a large demand for network bandwidth, and a potentially centralized risk. The decentralized network model has the flexibility to set up a network where equipment is transparent and resilient and is capable to support real-time services. Based on blockchain techniques, it can also improve the degree of trust between devices. Its shortcomings lie in the equipment performance requirements are high and is not conducive to large-scale network formation. In addition, the control ability of administrators and the overall performance of the network is weaker than those in the centric network model. The new network model based on multi-layer distributed accounting can be regarded as an organic combination of the two methods, which not only effectively utilizes the performance and capabilities of the cloud server, but also significantly improves the overall security and reliability of the IoT with taking advantages of blockchain techniques. The most critical point is that the network model allows the existing center-based networks' iterative upgrade, which makes large-scale applications and deployments possible. This article mainly discusses the model from the security point of view and to elaborate the mechanism to achieve secure IoT.

The network model divides the whole IoT into two parts: the edge layers and the high-level layers.

Edge Layers

Edge layers provide entities of localized Internet of things and interfaces to high-level layers. In general, the edge layer is consistent with the current centralized network model: the cloud server manages device data and processes requests. In terms of security, the device is authenticated by the cloud server through the device's universal unique identity (UUID) and the corresponding seamless hash algorithm. Powerful devices can choose to support nonsymmetric encryption algorithm for data transmission. However, the edge layer is still different from the current common cloud service system of IoT:

- The number of devices of a single edge layer is less thus its network efficiency is higher. According to the current application situation, one of the main factors limiting the ability of central networking is network bandwidth limitation. IoT equipment often needs heartbeat signals to keep contact with cloud. When many devices are networked, high concurrent access to the server often occurs. At this time, even if the cloud server's computing power is sufficient to handle high concurrent requests, the Internet's bandwidth limits and network instability and even service providers' constraints tend to cause delays, congestion and even loss of response and other issues in IoT practical applications. As a comparison, according to the bandwidth, an edge layer can limit the number of devices to a certain extent to avoid this application problem. Correspondingly, since the flexibility of cloud services, cloud servers' performance in the edge layer can be appropriately reduced by redeployment, thus avoiding waste of resources.

- The devices in edge layers tend to be geographically or regionally concentrated. In theory, the edge layer is only a logical concept, and should not limit the region of devices. In fact, since the edge layer is like a local area network, the regionalization of the devices can be more conducive to the actual management and optimal allocation of cloud resources. All in all, the edge layer is a small centric IoT managed by a designated cloud platform or private data center with a certain type of security regulations

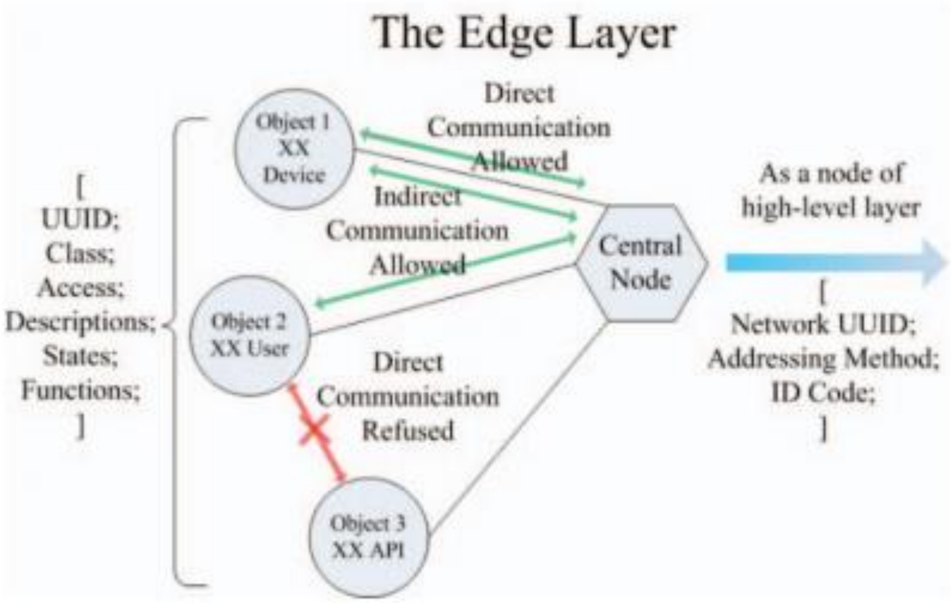


Fig. 4 – The Edge Layer

High-level Layers

High-level layers are the part that connects the edge layer and implements the wide area networking capabilities of the IoT. In fact, the edge layer can be defined internally by the central node. From the view of whole network structure, it only needs to provide a data access interface to the high-level layer to indicate its identity. In other words, the edge layer is equivalent to a node that belongs to the higher layer which it connects to. The logic also applies to the connections between high-level layers. Thus, the complete network model will have the following structure: treating the edge layer as Layer 0, the superior high-level layer as Layer 1, then Layer 2, Layer 3, and so on. Unlike the edge layer, in the high-level layer, the network is decentralized. All nodes in the same layer run in a distributed way. For example, based on the Byzantine Fault Tolerance (BFT)[7] algorithm to maintain a block chain of distributed records, all the nodes belongs to one certain layer are easy to achieve self-management and a certain degree of fault tolerance. The advantage of the multi-layer network model is listed as below:

- To enhance the application efficiency of the blockchain technology and reduce the difficulty of its deployment. At present, the main problem of blockchain technology is that the recording block has high requirements for node capability, and the response speed of the distributed consensus algorithm is low when the number of nodes is large. When deployed in a multi-layer network model, each node in the high-level layers is physically at least one data center and certainly with enough computing ability. What's more, we can also limit the number of nodes per layer to 23- 26 order to reduce the time and space costs required for blockchain records.
- The entire IoT has a strong ability to self-adjust and resist risks. can be adjusted and anti-risk ability. At this time the block chain is deployed in each high-level layer, which means that even if single high-level layer is destroyed, other layers can also provide blockchain records.

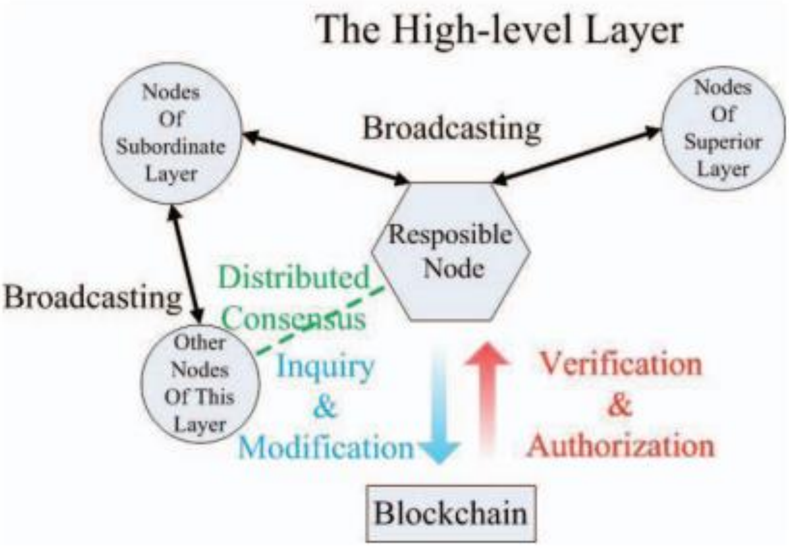


Fig. 5 -The High-level Layer

The specific concepts in this model will be described below.

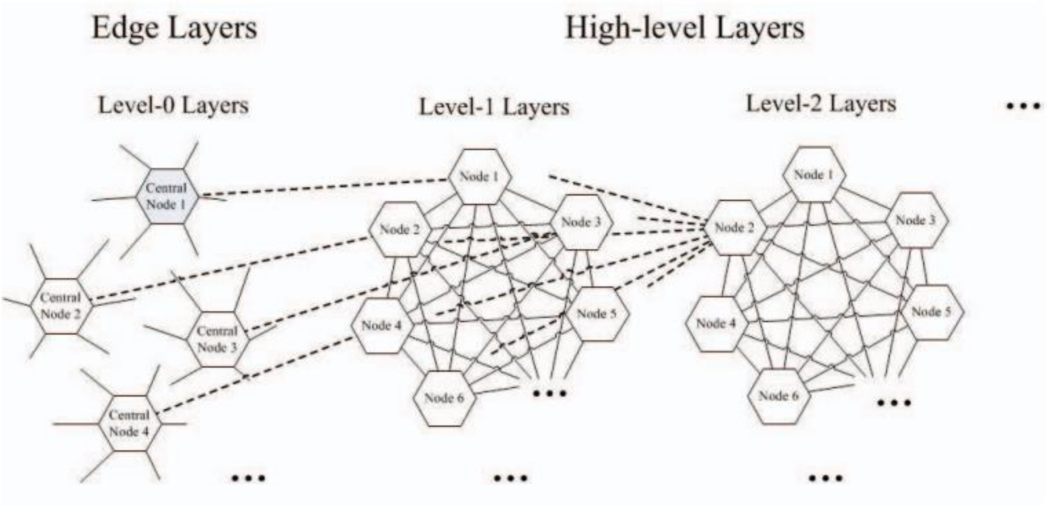


Fig. 6 – Overview of the proposed network model

1.2 ControlChain - Central Enabler for Access Control Authorizations in the IoT

A complete access control solution involves three components: authentication, authorization and auditing. The authentication identifies the correct identity of the subject. The authorization verifies if the subject has the rights to do some operation on the object. Finally, the auditing (or accountability) allow the posterior analysis of the realized activities in the system. These components have important roles in securing the system, however the authorization component requires a special attention because it is responsible for enforcing the access rules.

The ControlChain is an architecture to provide access control in IoT. It was created with the following principles in mind: Decentralization. The expected grow of the IoT requires a decentralized solution. Resilience. Make an architecture with no single points of failure and resilience to data corruption. Off-line working. The dominant IoT communication media type, i.e. wireless, is known to be instable and could lead to intermittent connections, so the continuous operation in a disconnected environment is necessary. Low processor usage for authorizations. In the IoT, some devices will be restricted in the power processing capacity. Therefore, the ControlChain is a decentralized, resilient, allow off-line work and has low processor usage profile on the authorization process. The Figure 1 presents an overview of the ControlChain. Although nothing prevents all the information to be in one unique Blockchain, for organization and to facilitate the explanation, we divided the database of the ControlChain in 4 different Blockchains: Context Blockchain, Relationships Blockchain, Rules Blockchain and Accountability Blockchain. It is important to note that, based on the Blockchain principles, once an information is published on one of these Blockchain it is part of the information history and cannot be erased, however, we allow the update of the Blockchain contents with the creation of new registers. Next, we explain how these 4 Blockchains works.

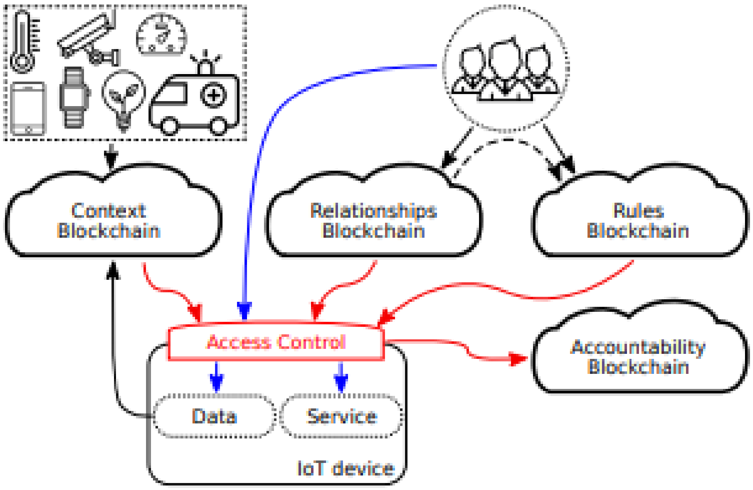


Fig. 7 – Architecture Overview

Relationships Blockchain:

The Relationships Blockchain is responsible for the storage of the public credentials and relationships of all entities in the system. In fact, there is no differentiation between users, devices or groups in our proposal. Each entity has an owner that has complete control over it in the system. A relationship is a unilateral reference to another entity with an optional set of attributes to it. The relationships of the entities are important in our architecture because it could be used in the authorization decisions. There are two possible types of relationship references: Blockchain-dependent and external. The Blockchain dependent reference is a link created with identifications tied to Blockchain registers (for example, chronological number of the block and line number of the register inside the block). The external reference is a link based on Blockchain external identification (for example, a public key). It is a dynamic reference that always is interpreted as a pointer to the most recent update of an entity in the Blockchain, if it exists there. Note that it also allows the reference to entities outside the Blockchain. The choose of best type of reference is use case dependent. The Figure 8 shows two examples (numbered as 1 and 2) of Relationships Blockchain. In this figure, each square is a block, the leftmost square is the genesis block, contiguous line arrows are the default links between the blocks, dashed line arrows are relationships, dotted line arrows are relationships that are dependent of the relationship references type chosen and the hatch represents the block owner. It's important to remainder that one block could have more than one entity and not necessarily the blocks are labeled with their type or function inside the use case, like the user, device or group in the figure. However, to simplify these examples, we represent only one entity per block and label the blocks.

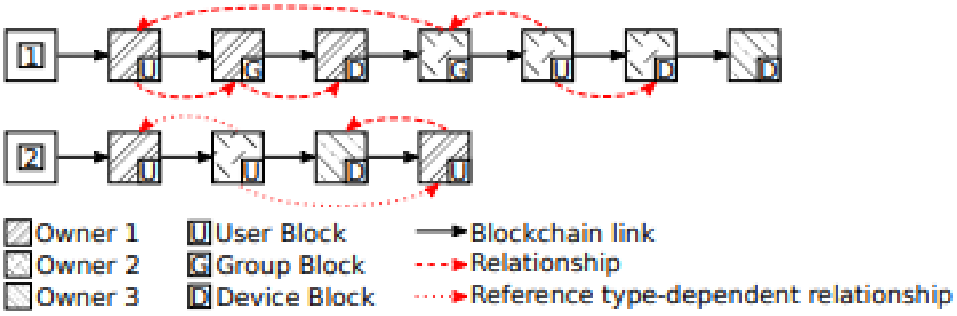


Fig. 8 – Relationship overview

In the first example, the left part shows the relationship between a user, a group and a device (all owned by the Owner 1): the user references the group and the group references the device. In the middle of the example, there is an Owner 2 user with a group (for example, with the attribute "friends") that links to the Owner 1 user. Finally, could exist entities without references or been referenced like the last entity of the Blockchain. As can be seen, the type of relationship adopted in this example is the external one because there are entities referencing other after-appended entities. The second part of the Figure 8 presents an example of a behavior that depend on the chosen reference type. In this example, the Owner 1 user was created on the second block with no relationship and was referenced by the Owner 2 user in the third block. After, the Owner 1 user was updated to reference the Owner 3 device. With the Blockchain-dependent reference type, the Owner 2 user stays referencing the first version of the Owner 1 user, i.e. the one without references. With the external reference type, the Owner 2 user relationship is automatically pointing to the updated Owner 1 user, i.e. the one with the reference to the Owner 3 device.

Context Blockchain:

The Context Blockchain store contextual information obtained from sensors, processed data and manual inputs. This contextual information can be used in the authorization decision. For example, suppose there is an access rule with the following statement: "8k resolution videos can only be accessed when the router reports that the network traffic is low". In this situation, the access control will find the report of the router in the Context Blockchain and check its state before allowing the access.

Accountability Blockchain:

The Accountability Blockchain register information about permissions or denies of access to object. The information required to registered is described in the Rules Blockchain. This information could be used for accountability and auditing of accesses, and for checking the sanity of the system. Furthermore, the information stored in this Blockchain could also be used like the contextual ones.

Rules Blockchain:

The Rules Blockchain keep the authorization rules defined by owners to their objects or by objects to themselves. The big challenge faced by this Blockchain is making it generic enough to be compatible with the big variety of access control models and mechanisms used in the IoT. Each one capable of fulfill different IoT scenarios requirements. Without loss of generalization, we identified 3 types of access control mechanisms (based on ACL, Capability and Attribute) that with some minor additions could lead to the compatibility with a lot of models. These minor additions are the append of context conditions, obligations and a list of information to be registered on the Accountability Blockchain. The context conditions are Boolean expressions that are build using context identifiers of the Context Blockchain. The obligations determine routines (for example, accept an agreement) that the subject must accomplish to get the access authorization. Finally, the third addition describe the access information that should be recorded on the Accountability Blockchain by the access control. We call these mechanisms-based blocks as ACL rule block (allows a list of subjects for each object), capability rule block (allows a list of objects for each subject) and attribute rule block (allow a list of subjects' and objects' attributes).

The process to transform access control models to more generic mechanisms is illustrated in Figure 9. We propose the utilization of a Decoder. This Decoder receives the access control model and rules and translate them to mechanisms supported in our architecture. In some cases, the users need to provide additional information. For example, suppose a rule says that only subjects with the role "manager" can have access to the management system. This role be an attribute of the entity subject, however, at least one entity should be pointed as the official attribute provider for the evaluation of the rule.

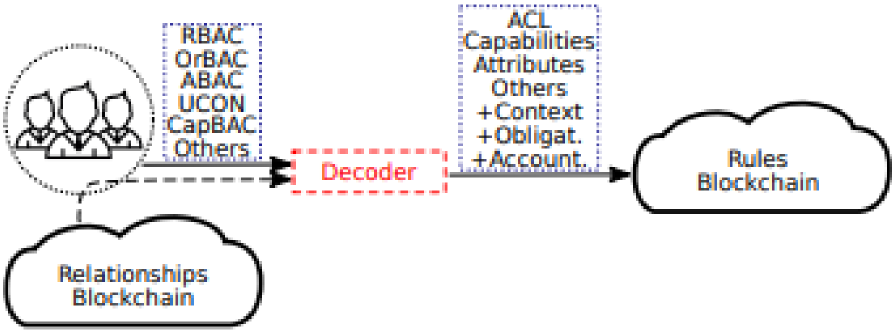


Fig. 9 - Transformation of access control models to the mechanisms

1.3 Viability with limited resources devices

One important factor about an access control architecture for the IoT is it viability in scenarios with limited resource devices. In this section, we discuss how the main technology used in the ControlChain (the Blockchain) and the evaluation of rules can be compatible with these scenarios.

Growing of the Blockchain:

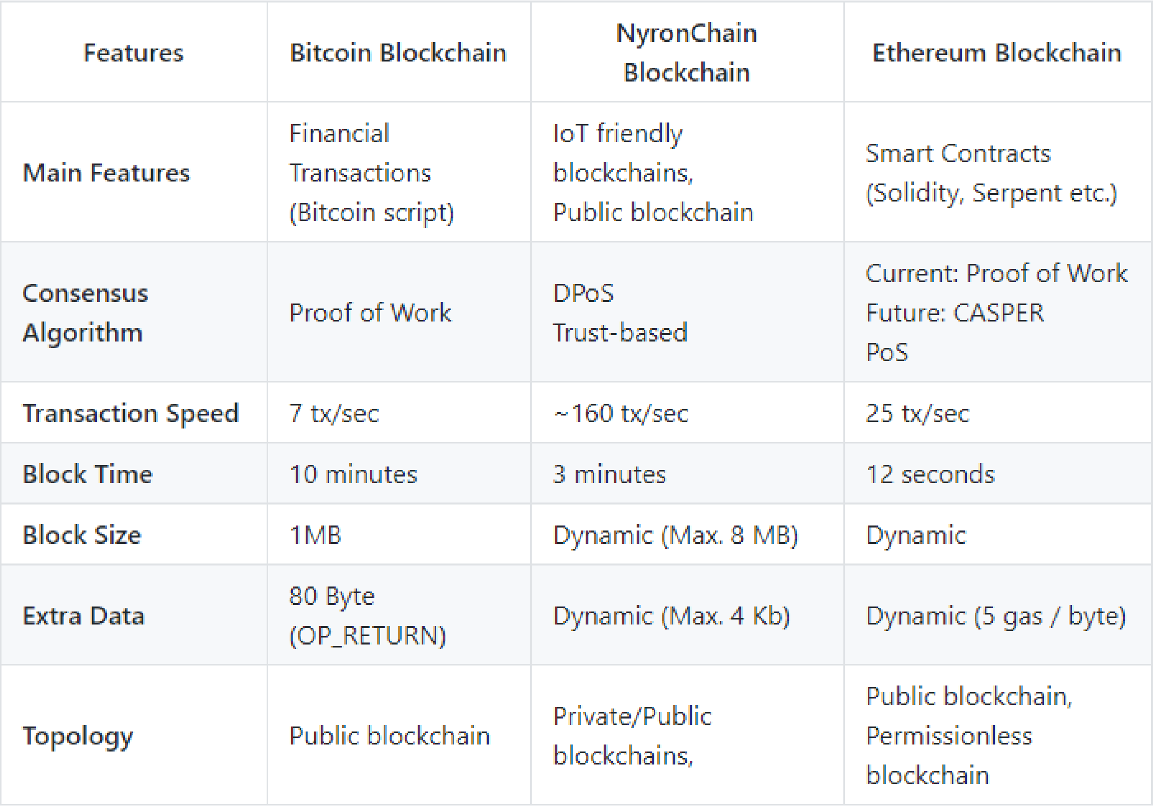
The size of an entire Blockchain could be a problem to devices with low storage space. However, devices doesn't need to store the full Blockchain. For example, the storage could be performed with some replication factor. Beside this, more limited devices could also filter all the non-important information and store only the ones it judges to be important. For example, a device could store only rules related to it and both, contexts and relationships, related to these stored rules.

Speed of new registers:

With the arise of many new registers in a short period of time, devices with less resources could not be capable of keep up with the updates. However, the number of registers in a block could be limited and the speed of new blocks can be adjusted by, for example, changing the difficult of the proof-of-work imposed to miners. Beside this, different Blockchains could be used for different systems. Finally, the restricted devices could also find support in other devices, like those with the same owner in the Relationships Blockchain.

The Blockchain has interesting features desired for a wide range of domain applications. One example of these domains is the access control. Although other works already use it in this domain, they only explored a little of the great potential of the Blockchain. In this work, we proposed an architecture for access control based on the Blockchain. Our architecture is fully decentralized (requiring no third-party), scalable, user transparent, user friendly, fault tolerant and compatible with a wide range of access control models employed in the IoT. Furthermore, our architecture also includes a secure way of creating relationships, assigning attributes for them and using them in the access control

1.4 Overview of our blockchain



Features	Bitcoin Blockchain	NyronChain Blockchain	Ethereum Blockchain
Main Features	Financial Transactions (Bitcoin script)	IoT friendly blockchains, Public blockchain	Smart Contracts (Solidity, Serpent etc.)
Consensus Algorithm	Proof of Work	DPoS Trust-based	Current: Proof of Work Future: CASPER PoS
Transaction Speed	7 tx/sec	~160 tx/sec	25 tx/sec
Block Time	10 minutes	3 minutes	12 seconds
Block Size	1MB	Dynamic (Max. 8 MB)	Dynamic
Extra Data	80 Byte (OP_RETURN)	Dynamic (Max. 4 Kb)	Dynamic (5 gas / byte)
Topology	Public blockchain	Private/Public blockchains,	Public blockchain, Permissionless blockchain

Delegated Proof-of-Stake

Invented by Daniel Larimer, Delegated Proof-of-Stake (DPoS) is an alternative consensus mechanism that requires coin holders to vote for “delegates”, who are then responsible for validating transactions and maintaining the blockchain. DPoS is an alternative to the more commonly known, Proof-of-Stake (PoS) model which requires miners to put up a stake in a cryptocurrency in-order for them to be able to validate transactions.

The process of Delegated Proof-of-Stake is quite a bit different from more traditional consensus mechanisms. In DPoS, stakeholders elect what are known as witnesses. Witnesses are responsible and rewarded for generating blocks which are then added to the blockchain. Stakeholders can vote for as many witnesses as they wish, so long as, at least 50% of the stakeholders believe sufficient decentralization has been achieved through the number of elected witnesses. The voting for witnesses is a continuous process, therefore, witnesses have an incentive to carry out their function to the highest standard or they risk losing their position.

In addition, there are also what are known as delegates. Delegates are elected in a similar manner to witnesses, however, delegates are responsible for maintaining the network and can even propose changes to the network. Changes such as: Block sizes, the amount that witnesses should be paid and transaction fees. Once these changes have been submitted, it is then up to the stakeholders to decide whether the proposed changes should be implemented.

Appendix 2: NyronChain Beacons technology

The modulation rate of the Bluetooth Low Energy radio is set by the specification at a constant 1Mbps (one mega bit per second). This, of course, is the theoretical upper limit. In practice, you can expect between 5-10 KB per second, depending on the limitations of the devices used. As far as range goes, BLE is focused on very short-range communication. It's possible to create and configure a BLE device that can reliably transmit data 30 meters or more line-of-sight, but a typical operating range is probably closer to 2 to 5 meters. Of course, the higher the range the more battery consumption, so take care when trying to tweak your device for higher range.

3.1 Building blocks of the BLE

BLE is organized in 3 major building blocks: Application, Host and Controller. Application block is, as the name says, the user application which interfaces with the Bluetooth protocol stack. The Host covers the upper layers of the Bluetooth protocol stack. And the Controller covers the lower layers. The Host can communicate with the BLE module with an addition of something we call HCI - the Host Controller Interface. The purpose of HCI is, obviously, to interface the Controller with the Host, and this interface makes it possible to interface a wide range of Hosts with the controller. In our case, the MCU runs the Application, and talks to a Connectivity Device, the Connectivity Device is made out the Host and Controller. For this purpose, we use SPI to communicate, but different interfaces can also be used.

3.2 Network Topology

BLE devices can have two different roles, either as Central Devices or Peripheral Devices. Central devices are usually mobile phones or PC's which have a higher CPU processing power. While peripheral devices are usually some sensors or low power devices, which connect to the central device. A BLE device can send two types of data: Advertising Packets, and Scan Response Data. Advertising Packets are necessary and are constantly being transmitted from a peripheral device in order to be seen by other devices. When other devices receive this data, they can request additional data from the peripheral device which then sends the Scan Response Data. A BLE device can talk to nearby devices in one of two ways: Broadcasting and Connections. Broadcasting is the act of sending data out to all the listening devices. When talking about Broadcasting, we define two roles: Broadcaster and Observer. The Broadcaster sends non-connectable advertising packets periodically to anyone who is willing to accept them. While the Observer repeatedly scans the area in order to receive the packets. Then, when the Observer receives the Advertising packet, it can request the Scan Response Data. It is important to note that Broadcasting is the only way a device can transmit data to more than one peer at a time.

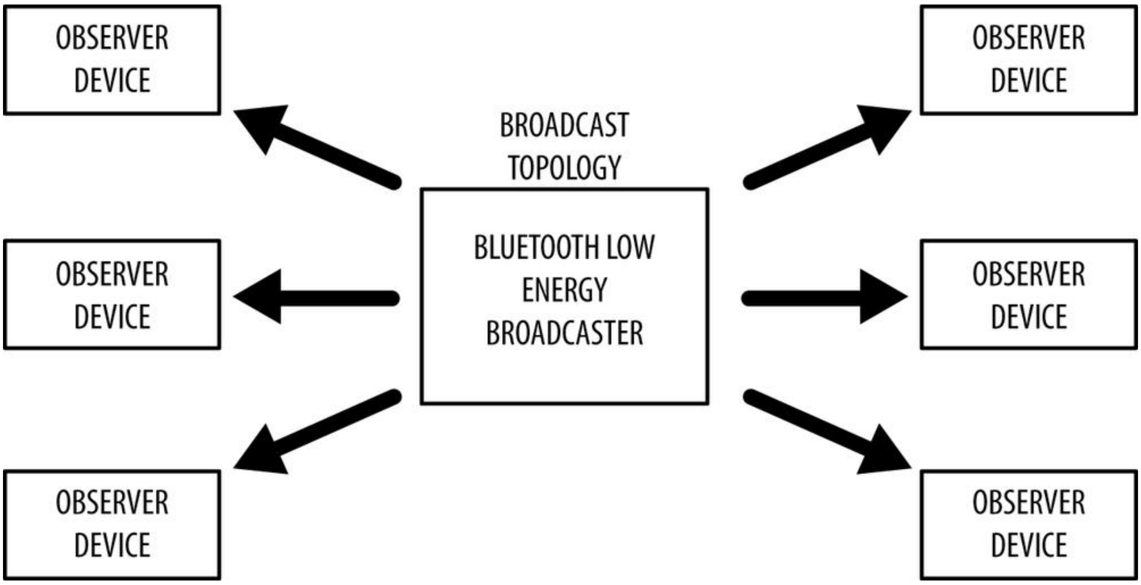


Fig. 10 – BLE Broadcasting Topology

A Connection is a permanent, periodical data exchange of packets between two devices. The master (central device) scans the frequencies for connectable advertising packets, and when suitable, initiates a connection. Once the connection is established, the central device manages the timing and initiates the periodical data exchanges. The slave (peripheral device) sends connectable advertising packets periodically and accepts incoming connections, once a connection is established the peripheral follows the central's timing and exchanges data regularly with it. When connected, the two devices usually define what is known as a connection event. A connection event is a periodical exchange of data at certain specific points in time. This is one of the key benefits for power saving - two devices can power up, exchange data, and then go to sleep until the next connection event.

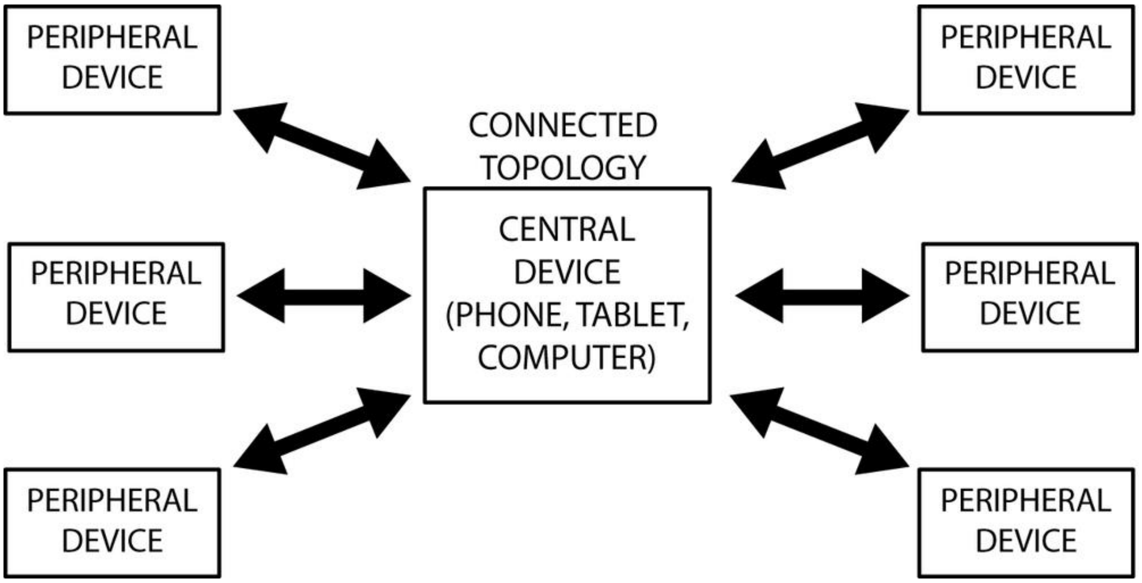


Fig.11 -BLE Connection Topology

3.3 NyronChain beacon: Different Layers and their Purposes

BLE, like many other wireless technologies, is organized in a number of layers. Each layer has its purpose and plays a significant role in making a BLE device function properly. All the layers and definitions can look quite overwhelming, but we will take it step by step and cover all the necessary fields required to develop a successful project with BLE.

Let's take a look again at the 3 building blocks of a BLE device: Application, Host and Controller:

The Application, is the highest layer and the one responsible for containing the logic, user interface, and data handling of everything related to the actual use-case that the application implements. The architecture of an application highly depends on the project developed with BLE.

The Host consists of the following layers:

- Generic Access Profile (GAP)
- Generic Attribute Profile (GATT)
- Logical Link Control and Adaptation Protocol (L2CAP)
- Attribute Protocol (ATT)
- Security Manager (SM)
- Host Controller Interface (HCI), Host side

The Controller includes the following layers:

- Host Controller Interface (HCI), Controller side
- Link Layer (LL)
- Physical Layer (PHY)

3.4 Physical Layer (PHY)

The Physical Layer contains the analog communications circuitry used for modulating and demodulating analog signals and transforming them into digital symbols. The BLE can communicate over 40 channels from 2.4000 GHz to 2.4835 GHz. 37 of these channels are used for connection data and the last three channels (37, 38, and 39) are used as advertising channels to set up connections and send broadcast data. BLE uses a technique called frequency hopping spread spectrum, in which the radio hops between channels on each connection event. The value of the hop is communicated when the connection is established, so it is different for every new established connection. This technique minimizes the effect of any radio interference.

3.5 Link Layer

The Link Layer is the part that directly interfaces with the physical layer, and it is usually implemented as a combination of custom hardware and software. The Link Layer defines following roles for it's devices, based on logical groups:

Advertiser - A device sending advertising packets, and Scanner - A device scanning for advertising packets.

Master - A device that initiates a connection and manages it later, and Slave - A device that accepts a connection request and follows the master's timing.

The Link Layer also takes care of the Bluetooth Device Address - a 48-bit number which uniquely identifies a device among peers. You can think of a BDA as something like the MAC address in IP.

The Link Layer is also in charge of establishing connections, it filters out advertising packets depending on the Bluetooth address or based on the data itself. And manages the connection interval - The time between the beginning of two consecutive connection events. The link layer can also configure Encryption, which is highly desirable in case of a lot of devices present in the same range.

3.6 Host Controller Interface (HCI)

As described before, HCI allows more powerful CPUs to control the BLE device over a serial interface, usually UART or USB.A typical example of this configuration includes most smartphones, tablets, and personal computers, where the host (and the application) runs in the main CPU, while the controller is located in a separate hardware chip connected via a UART or USB. Since we do not have this type of configuration, we will not be discussing the HCI any further.

3.7 Logical Link Control and Adaptation Protocol (L2CAP)

The L2CAP is in charge of two tasks:

- It takes multiple protocols from the upper layers and encapsulates them into the standard BLE packet format (and vice versa).
- Fragmentation and recombination: it takes large packets from the upper layers and breaks them up into chunks that fit into the 27 bytes maximum payload size of the BLE packets on the transmit side, and vice versa, it receives multiple packets that have been fragmented and recombines them into a single large packet that will then be sent to the upper

The L2CAP layer is in charge or routing two main protocols: The Attribute Protocol (ATT) and the Security Manager Protocol (SMP). The ATT forms the basis of data exchange in BLE applications, while the SMP provides a framework to generate and distribute security keys between peers. We will leave the SMP out of this tutorial since it is not crucial to our project for right now.

3.8 Attribute Protocol (ATT)

The Attribute Protocol (ATT) is a simple client/server protocol based on attributes presented by a device. A client requests data from a server, and the server then sends data to it's clients. It is important to remember that if there is a request still pending, no further requests can be sent until the response arrives. Each server contains data organized in the form of attributes, each of which is assigned a 16-bit attribute handle, a universally unique identifier (UUID), a set of permissions, and a value. The attribute handle is simply an identifier used to access an attribute value, while the UUID is used to specify the type and nature of the data in the value. The client sends the appropriate write or read requests, and the server responds according to them.

When a client wants to read or write attribute values from or to a server, it sends a read or write request to the server with the handle. The server then responds with the attribute value or an acknowledgement response. In the case of a read operation, the client has to parse the value and understand the data type based on the UUID of the attribute. On the other hand, during a write operation, the client is expected to provide data which corresponds with the attribute type and the server is free to reject the operation if that is not the case.

The set of operations which are executed over ATT are the following: Error Handling, Server Configuration, Find Information, Read Operations, Write Operations, Queued Writes, Server Initiated

3.9 Generic Attribute Profile (GATT)

The GATT is what comes on top of the ATT. It adds a data model and hierarchy, it defines how data is organized and exchanged in between different applications.

The data in GATT is organized in Services. Each Service contains one or more characteristics, and each characteristic is a union of user data along with metadata (descriptive information). Along with GAP, GATT makes up the main interface to a Bluetooth Low Energy protocol stack.

GATT Services are organized in something we called GATT Profiles, each profile can contain multiple services. Services are distinguished one from another using a 16-bit UUID. A full list of adopted services can be found on the Services page of the Bluetooth Developer Portal.

Characteristics also contain an UUID, and they usually represent a data end point. For example, if we are measuring temperature, the Characteristics part would contain some metadata (for example, if it's Fahrenheit or Celsius) and then the temperature value.

3.10 Generic Access Profile (GAP)

The GAP layer is in control of advertising and connections, it specifies how devices perform control procedures such as device discovery, connection, security establishment, etc.

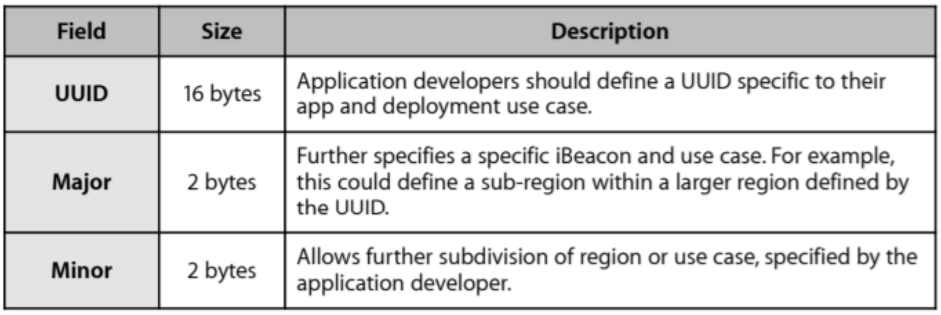
Its main focuses are:

- Roles and interaction between them
- Operational modes and transitions across those
- Operational procedures to achieve consistent and interoperable communication
- Security aspects, including security modes and procedures
- Additional data formats for no protocol data

As previously stated, a device can have the role of an Broadcaster or Observer, and of a Central or Peripheral device.

3.11 NyronChain Beacons UUID

Devices with NyronChain Beacon technology can be powered using coin cell batteries for a month or longer or operate for months at a time using larger batteries or can be powered externally for extended periods of time. BLE compatible devices can also be configured to generate NyronChain beacon advertisements, although this functionality is limited in scope. This would be appropriate for uses such as a Point of Sale or kiosk application, or for an application that wants to become an NyronChain beacon for a short time while someone is actively using the application.
An NyronChain Beacon advertisement provides the following information via Bluetooth Low Energy:



Field	Size	Description
UUID	16 bytes	Application developers should define a UUID specific to their app and deployment use case.
Major	2 bytes	Further specifies a specific iBeacon and use case. For example, this could define a sub-region within a larger region defined by the UUID.
Minor	2 bytes	Allows further subdivision of region or use case, specified by the application developer.

3.12 Current NyronChain beacons specs

Hardware:

- Size (5,4cm diameter)
- Coin cell battery included (CR2032), lasting up to 20 years
- Security (AES Encryption)

Software:

- Cloud-based CMS & API access
- IOS & Android SDK
- RTLS & Asset Tracking

Services:

- Beacon usage consultancy
- Phone & email sales support

Appendix 3: NyronChain IoT industry

Like the industrial revolutions such as steam power and electrification before it, the Internet of Things is fast becoming the new motive force driving the global economy. Uniting the physical world of objects and the virtual one of computing and analytics, it offers unrivalled opportunities for productivity gains, innovation, and new markets (see "What is the Internet of Things?").

Globally, nations are scrambling to seize the opportunities this new digital age promises, but for China, the task is particularly urgent. The economy has slowed significantly, productivity growth has dwindled, while competition at home and abroad has intensified. And many of the country's industries remain stuck in low-value segments, constrained by weak innovation capacity.

In response, China's government has launched the "Made in China 2025" initiative, modelled on Germany's "Industrie 4.0" scheme for improving that country's manufacturing competitiveness (see "Industrie 4.0"). The goal of "Made in China 2025" is to upgrade the nation's manufacturing capacity, with an eye toward boosting China's global position in manufacturing and production. It calls for greener, more intelligent and higher-quality manufacturing through the integration of production processes with the internet. Additionally, the government has introduced its "Internet Plus" strategy to integrate the country's mobile internet, cloud computing, big data and IoT initiatives to promote the extensive application of IT and smart technologies.

3.1 China IoT growth and projections

Our economic modelling shows how the IoT could provide significant benefits for China at the national level, but what about among industries? To understand its sector-specific economic potential in the country, Accenture teamed with Frontier Economics to estimate the cumulative GDP impact of the IoT for twelve key industries in the country.

Our analysis revealed that, based on China's current policy and investment trends, the IoT could add US$196 billion to the cumulative GDP in manufacturing industries alone over the next 15 years. While these gains may seem significant, the country could further boost its IoT impact considerably. By making targeted investments and supporting other similar initiatives to improve the country's capacity to absorb IoT technologies, the additional value generated by each industry would be substantial. For instance, in the case of manufacturing, the economic value from the IoT could jump from US$196 billion to US$736 billion—a 276 percent increase. For resources, the increase would be from US$48 billion to US$189 billion—almost three times higher than under current conditions. According to the analysis, manufacturing industries would account for the highest proportion of the IoT's economic benefits, followed by public services spending by the government, and the resource industries. These top three positions account for over 60 percent of the IoT's total cumulative GDP impact by 2030. In contrast, healthcare, education and transportation industries will likely make relatively small additions to the cumulative GDP from IoT due to their small sector sizes.

References

1. Antonopoulos, Andreas, Mastering Bitcoin: Programming the Open Blockchain, O'Reilly Media Inc. (California: 2017).
2. Arad Networks, "Why SPN Solutions?" http://www.aradnetworks.com/spn_why, (March 2017).
3. Banafa, Ahmed, "Internet of Things (IoT): Security, Privacy and Safety," Datafloq, https://datafloq.com/read/internet-of-things-iot-security-privacy-safety/948.
4. Beecham Research Limited, "IoT Security Threat Map," http://www.beechamresearch.com/download.aspx?id=43, (2015).
5. Belson, David [Ed.], "The State of the Internet / Q3 2015," Akami, https://www.akamai.com/us/en/multimedia/documents/report/q3-2015-soti-connectivity-fi nal.pdf, (December 2015).
6. Boldt, Bill, "Without Security, is the Internet of Things Just a Toy?" Pubnub, https://www.pubnub.com/blog/2015-01-30-without-security-internet-things-just-toy/, (January 2015).
7. Buterin, Vitalik, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform," https://github.com/ethereum/wiki/wiki/White-Paper, (2014).
8. Elasticsearch, "Heart of Elastic Stack," https://www.elastic.co/kr/products/elasticsearch, (2017).
9. EYL Partners, "Product Overview" http://www.eylpartners.com/index.php/product-overview/, (2017).
10. Greenspan, Dr. Gideon, "MultiChain Private Blockchain ? White Paper," Coin Sciences, http://www.multichain.com/download/MultiChain-White-Paper.pdf, (2014).
11. Intel Software, "Intel Realsense Camera SR300," https://software.intel.com/en-us/realsense/sr300, (June 2016).
12. La Marca, Daniela, "Gartner: hype in 2015 around the internet of things (iot) and wearables," Mediabuzz, http://www.mediabuzz.com.sg/asian-emarketing-latest-issue/210-asian-e-marketing/digital-marketing-trends-a-predictions-week-1/2504-gartner-hype-in-2015-around-the-intern et-of-things-iot-and-wearables, (Jan. 2015).
13. Modacom, "Smart IoT Gateway (Hub)," http://web.modacom.co.kr/ko/product/product_view.php?cate=IoT%20Products, (Feb. 2017).
14. Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System," https://bitcoin.org/bitcoin.pdf, (2008).
15. P&P Secure, "Domestic DB Security # 1 'P & S Secure,'" http://www.pnpsecure.com/NEWS--NOTICE/page-4, (Sept. 2017).
16. B. Anggorojati, P. Mahalle, N. Prasad, and R. Prasad, Secure Access Control and Authority Delegation Based on Capability and Context Awareness for Federated IoT. River Publishers, 5 2013, pp. 135–160.
17. S. Gusmeroli, S. Piccione, and D. Rotondi, "A capability-based security approach to manage access control in the internet of things," Mathematical and Computer Modelling, vol. 58, no. 56, pp. 1189 – 1205, 2013, the Measurement of Undesirable Outputs: Models Development and Empirical Analyses and Advances in mobile, ubiquitous and cognitive computing.
18. J. Bernal Bernabe, J. L. Hernandez Ramos, and A. F. Skarmeta Gomez, "Taciot: multidimensional trust-aware access control system for the internet of things," Soft Computing, vol. 20, no. 5, pp. 1763–1779, 2016.

19. R. Neisse, I. N. Fovino, G. Baldini, V. Stavroulaki, P. Vlacheas, and R. Giaffreda, “A model-based security toolkit for the internet of things,” in 2014 Ninth International Conference on Availability, Reliability and Security, Sept 2014, pp. 78–87.

20. D. Ferraiolo and R. Kuhn, “Role-based access control,” in In 15th NISTNCSC National Computer Security Conference, 1992, pp. 554–563.

21. A. A. E. Kalam, R. E. Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, A. Miege, C. Saurel, and G. Trouessin, “Organization based access control,” in Proceedings POLICY 2003. IEEE 4th International Workshop on Policies for Distributed Systems and Networks, June 2003, pp. 120–131.

22. V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, “Guide to attribute based access control (ABAC) definition and considerations,” National Institute of Standards and Technology (NIST), Tech. Rep., jan 2014.

23. J. Park and R. Sandhu, “The uconabc usage control model,” ACM Trans. Inf. Syst. Secur., vol. 7, no. 1, pp. 128–174, Feb. 2004.

24. B. Anggorojati, N. R. Prasad, and R. Prasad, “Secure capability-based access control in the m2m local cloud platform,” in 2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace Electronic Systems (VITAE), May 2014, pp. 1–5.

25. R. S. Sandhu and P. Samarati, “Access control: Principle and practice,” Comm. Mag., vol. 32, no. 9, pp. 40–48, Sep. 1994.

26. M. Swan, Blockchain: Blueprint for a New Economy. O’Reilly Media, 2015.

27. Z. Zheng, S. Xie, H.-N. Dai, and H. Wang. (2016) Blockchain challenges and opportunities

28. A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT. Cham: Springer International Publishing, 2017, pp. 523–533.

29. A. A. A. El-Aziz and A. Kannan, “A comprehensive presentation to xacml,” in Third International Conference on Computational Intelligence and Information Technology (CIIT 2013), Oct 2013, pp. 155–161.