TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Basanta Lamichhane 177775IVSB

Security Considerations For Implementation Of Blockchain In IoT Infrastructure

Bachelor's Thesis

Supervisor:	Tauseef Ahmed Ph.D in Electronics and Telecommunication

Tallinn 2021

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Basanta Lamichhane 177775IVSB

Turvalisuse kaalutlused plokiahela rakendamisel Iot Infrastruktuurides

Bakalaureusetöö

Juhendaja: Tauseef Ahmed
Ph.D Elektroonika ja Telekommunikatsiooi Alal

Tallinn 2021

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Basanta Lamichhane

30.04.202

Abstract

IoT can power automation and speed up several daily life applications across multitudes of industries like factory digitization, product flow monitoring, inventory management, packet optimization, logistics etc. IoT devices, by nature are low on computational power and designed for as few specific objectives as possible, this makes them inherently vulnerable to breaches in data with various kinds of cyber-attacks. The existing security measures are mostly backed by a central infrastructure and face a severe scaling and decentralization problem.

Blockchain combined with IoT can aid several fields like Supply Chain Management, Logistics, Pharmaceuticals and Insurance by providing an immutable ledger through which machine to machine data transactions can be facilitated thus by cutting intermediary steps for arranging untampered data. This can drastically improve the security in existing IoT systems.

Implementation of blockchain, however, comes with its own caveats. The power efficiency, storage dilemma and several other problems should be addressed and a side by side study with multivariate analysis should be done to figure out the optimum implementation of blockchain in the IoT sphere.

SECURITY CONSIDERATIONS FOR IMPLEMENTATION OF BLOCKCHAIN IN IoT INFRASTRUCTURE

Lõputöö on kirjutatud Inglise keeles ning sisaldab teksti 44 leheküljel, 8 peatükki, 9 joonist.

List of abbreviations and terms

LPWAN	low-power wide-area network (LPWAN)
DOE	Department of Engineering
QoS	Quality of Service
SPF	Single Point of Failure
P2P	Peer-to-peer
DAG	Directed Acyclic Graphs
IoT	Internet of Things
M2M	Machine to Machine
CIA	Confidentiality, Integrity and Availability
CAGR	Compound Annual Growth Rate
OSI	Open Systems Interconnections
DDoS	Distributed Denial of Service
PKI	Public Key Infrastructure
PoW	Proof of Work

Table of Contents

List of Figures

List of Tables

1 Introduction

Internet of Things (IoT) systems comprise devices that generate, process, and exchange huge amounts of business oriented, mission-critical or social information that are critical as well as privacy-sensitive and hence are appealing targets of various cyber attacks [1].

Being low energy and lightweight, these devices must devote most of their available energy and computation to executing core application functionality, leaving less room for security and privacy within them [2].

Traditional security methods tend to be expensive for IoT in terms of energy consumption and processing overhead. Moreover, many of the state-of-the-art security frameworks are highly centralized and are thus not necessarily well-suited for IoT due to the difficulty of scale, many-to-one nature of the traffic, and single point of failure [3].

In this paper we will focus on the challenges faced by IoT system in terms of following traditional cybersecurity measures:

- Confidentiality (C): making sure that the data packets are not intercepted and examined; also, making sure that the host is not corrupted to the point that a hacker can appropriate data, credentials, information, or configuration parameters (keeping the data safe from being divulged by/to unauthorized agents).
- Integrity (I): making sure that the packets received (or stored) have not been altered in an unauthorized manner (making sure the data is not modified by unauthorized agents).
- Availability (A): making sure that devices are not prevented from functioning properly and/or performing their function; or, making sure they are not made to operate in an improper or compromised manner. For example, the devices might become infected with viruses, worms, or degraded via other debilitating intrusions and/or exploited through weaknesses in the OS, software utilities, packaged microcode or applications. The term “no repudiation” has also been used in the context of availability. Availability also means the device is readily available to serve as a point of data exchange in often elaborate models.

Internet of Things

In modern use, The Internet of things (IoT) is an arrangement of interrelated computing devices along with mechanical and digital machines equipped with unique identifiers (UIDs) with the ability to move information over a system without expecting human-to-human or human-to-computer collaboration [4].

The term IoT was invented in 1999 to promote then popular Radio Frequency Identification (RFID) technologies. The exploration of the IoT world began to accelerate after the saturation of the Internet. Some more prominent examples of IoT devices around us comprise of:

- Wearable devices/fitness trackers (e.g., Jawbone Up, Fitbit, Pebble)
- Home Automation (Examples: Nest, 4Control, Lifx)
- Industrial asset monitoring (GE, AGT Intl.)
- Smart energy meters etc.

As the Internet fosters more collaboration and globalization, the IoT market is expected to grow as the current IT gadgets should be integrated to the IoT. The growth of traditional IT systems is at a modest two percent every year but the mass popularity of phones, tablets and personal computers leave a huge number of devices to be integrated [5].

A study by Norton, one of the biggest computer security service providers, predicts that there will be 21 billion IoT devices by 2025.

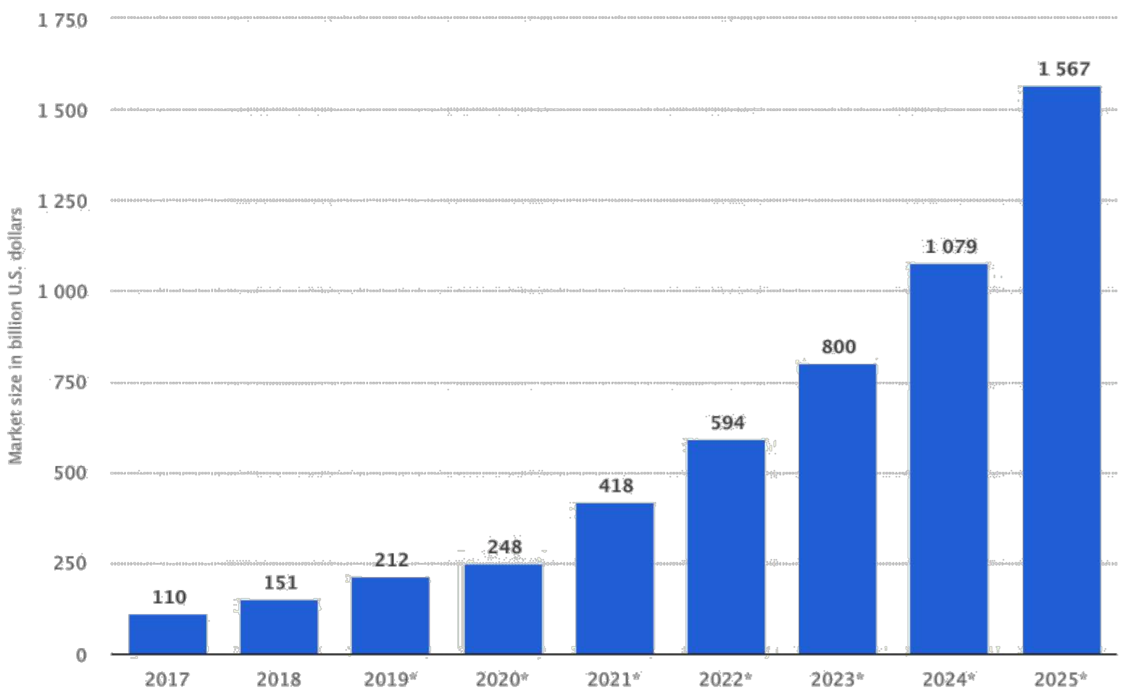


Figure 1 Forecast end-user spending on IoT solutions worldwide from 2017 to 2025 [6]

The growing demand will be accompanied by growing expenditure and investments in the IoT sector which is expected to exceed 1 trillion by 2024.

Consumers will just be one demographic of people that will leverage the power of IoT systems. Urban communities and organizations will progressively receive savvy innovations to set aside investments in time and cash.

That implies urban areas will have the option to robotize, remotely oversee, and gather information through things like CCTV systems, bike rentals, taxis and many more.

The paralleled developments in Artificial Intelligence and Machine Learning means IoT will rise up to be a thing of vital importance in smart homes, thermostats, lighting systems, and even beverage and cocktail makers. This will mean a lot of aggregation of data of consumers habits and patterns of usage [7].

The adoption of IoT will be fueled by the launch of 5G technologies. 5G is a major upgrade in the telecommunication technology over the existing 4G networks. The implementation of 5G would open up new and exciting innovation avenues for IoT devices [8].

Blockchain

Blockchain can be defined as a time-stamped series of non tamperable data that is managed by a cluster of computers not owned by any single entity. Each singular unit of this record is called a block. The series of these blocks are bound to each other using cryptographic principles forming a chain of records referred to as blockchain [9].

Blockchain was made popular by the inception and popularity of Bitcoin, the largest digital peer to peer currency. Blockchain is the underlying ledger that powers bitcoin but the use of blockchain is not limited to only that. In addition to acting as a distributed ledger, several other utilities of blockchain include notarization, supply chain record keeping, smart contract etc [10].

The potential uses of blockchain technology go beyond Bitcoin. Blockchain technology has the following properties:

- Cecentralized Control: A decentralized scheme in which no central authority dictates the rules.
- Data Transparency and Auditability: A full copy of every transaction ever executed in the system is stored in the blockchain and is public to all the peers.
- Distributed Information: Every network node keeps a copy of the blockchain to avoid having a centralized authority privately keep all that information.
- Decentralized Consensus: The transactions are validated by all the nodes of a network instead of a central entity. This breaks with the paradigm of centralized consensus.
- Security The blockchain is tamper-proof and cannot be manipulated by malicious actors. Those are few of the major strengths of blockchain technology. The secure, decentralized and autonomous capabilities of the blockchain make it an ideal component to become a fundamental element of IoT solutions.

Similar to IoT the adoption of blockchain is also on the rise. Worldwide spending in blockchain technology amounted to 2.7 billion USD in 2019, an increase of over 80% from 2019.

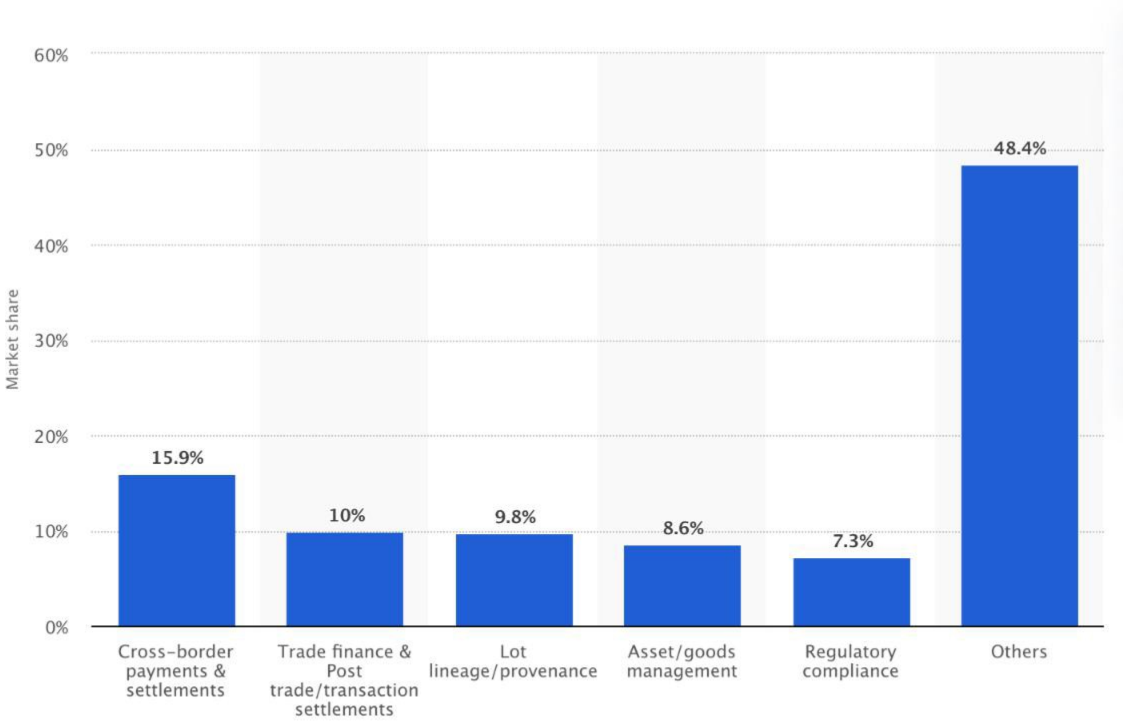


Figure 2 Blockchain Technology Market Share forecast in 2019 [11]

1.1 Problem Statement

Existing IoT based infrastructure run into severe problems with a necessity for centralized system for management of CIA and a single point of failure. Decentralization, automation and minimum human errors are critical for IoT infrastructures to flourish and thus speed up the adoption in daily lives.

However, by nature, IoT devices have less computational resources to allow many of the existing CIA measures and facilitate decentralization. Taking a decentralized approach to IoT networking and adopting a standardized peer-to-peer communication model would aid plethora of transactions between devices thereby resulting a significant drop in the costs associated with installations and maintenance of a large centralized data center or a set of large decentralized data and balance the storage needs for billions of IoT devices across the network. This will not only distribute the workload across various nodes spanning across many geographical areas but will also remove the single point of failures.

Blockchain can prove to be a one fit solution for all these problems. By nature, its decentralized ledger model means myriads of devices across the world can make use of a single record to make decisions and since it is tamperproof, the authenticity shall not be doubted.

Though these two emerging technologies appear to be a natural mix, there are several problems that can hinder [12]. For example, there have not been studies that compare the technologies side by side on the basis of different variables like speed, accuracy, costs etc.

Though blockchain may appear to be an apparent solution to security woes of IoT devices, the integration may come with its own baggage. Blockchain solutions are known not to scale very well [13] and also not all the sensitive internal information should be in the public ledger. These problems need to be addressed before a widespread adoption of integration of both technologies.

1.2 Goals of Thesis

The goals of this thesis are:

- Study and document current implementations of CIA triad in modern IoT systems.
- Study and document how effective these systems are.
- Study and document the limitations, bottlenecks and failures regarding current systems that is limiting mass adoption.
- Studying and documenting how blockchain can be seamlessly integrated to provide security to IoT devices.
- Studying and documenting the benefits and limitations of such integration.
- Proposing solutions to underlying problem with blockchain implementation.

1.3 Structure of Thesis

The thesis starts with a brief introduction to each of the IoT and blockchain technology. It then proceeds to discuss more about the importance of blockchain as a secured system and laying out the security requirements for IoT and blockchain. It then goes on to describe the methodology and analyze existing technologies. It then discusses the benefits of blockchain integration and point out the challenges. Finally, conclusions have been made on how can blockchain or parts of this technology can be used to solve scalability and privacy issues that is hindering the adoption.

2 Background

2.1 Blockchain as a secured system

The blockchain is a distributed database that does not need a central authority and eliminates the need for 3rd party verification. A blockchain contains a set of blocks, and every block contains a hash of the previous block, creating a chain of blocks from the genesis block to the current block.

A genesis block is the first block in a blockchain [13]. The genesis block is almost always hardcoded into the software. It is a special case in that it does not reference a previous block. For any block on the blockchain, there is only one path to the genesis block.

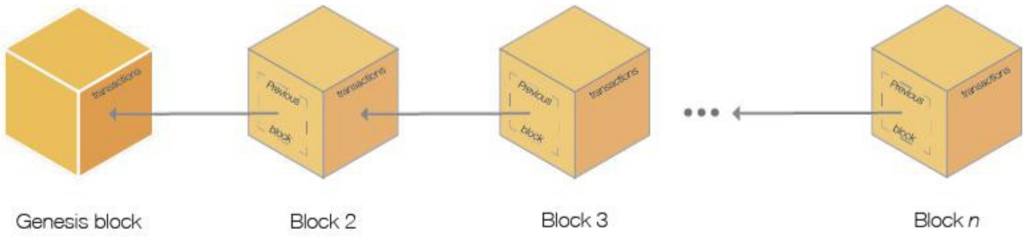


Figure 3 Formations of blocks in a blockchain

Blocks have a set of transactions. A transaction is a transfer of values between different entities that are broadcast to the network and collected into the blocks. All transactions are visible in the blockchain. The transactions are mined into a block by the so-called pool miners or solo miners [14]. The pool miners technique is a mining approach where multiple devices called miners contribute to the generation of a block. Pool miners or solo miners are entities that add transaction records into the blockchain. That process is called mining.

Mining is intentionally designed to be resource-intensive and difficult. Individual blocks must contain a proof of work (PoW) to be considered valid in the blockchain. The PoW is verified by other miners each time they receive a block [15].

The primary purpose of mining is to allow the nodes in a system to reach a secure, tamper-resistant consensus. Mining is also the mechanism used to introduce new cryptocurrency (e.g. Bitcoins) into the system. The miners are paid a transaction fee as well as a determined amount of newly created coins when they validate a block. This method serves the purpose of disseminating new coins in a decentralized manner as well as providing security to the system.

The system automatically adapts to the total mining power of the network keeping it constant to a specific amount of time (e.g. 10 minutes in Bitcoin). The difficulty target of the PoW is also adjusted after every certain number of blocks (e.g. 2016 blocks in Bitcoin) based on the network performance. A transaction takes time to reach all the nodes in the network, and the delay ensures that all the transactions are verified by all the nodes in the network, to prevent the so-called double spending problem [16].

Double spending is the result of using some cryptocurrency more than once at the same time. Consensus is a fundamental problem in distributed systems that requires two or more agents to mutually agree on a given value needed for computational purposes. Some of these agents may be unreliable, and therefore the consensus process needs to be reliant. Blockchains can use various consensus algorithms. Some of them include proof of work (PoW), proof of stake (PoS), proof of storage [17], proof of burn [18], or proof of capacity among others [19].

Some of the well-known benefits of using the blockchain technology are:

- The blockchain allows the verification of data without the intervention of a third party.
- Since the data can be only appended on the blockchain, a record once kept can never be removed.
- The chain of events is recorded in sequential order. In this manner, hence all the blocks in a blockchain are time stamped.
- The information structure in a blockchain is attached as it were. In this way, the information cannot be changed or erased.
- The source of any record can be followed along the chain to its place of starting point aka genesis block.
- The ledger can be distributed across a vast array of nodes and it would remain identical.

2.1.1 Why use blockchain for IoT systems

It is to be noted that not all IoT systems require a blockchain implementation. The flowchart below describes specific cases on which a blockchain should be used [20].

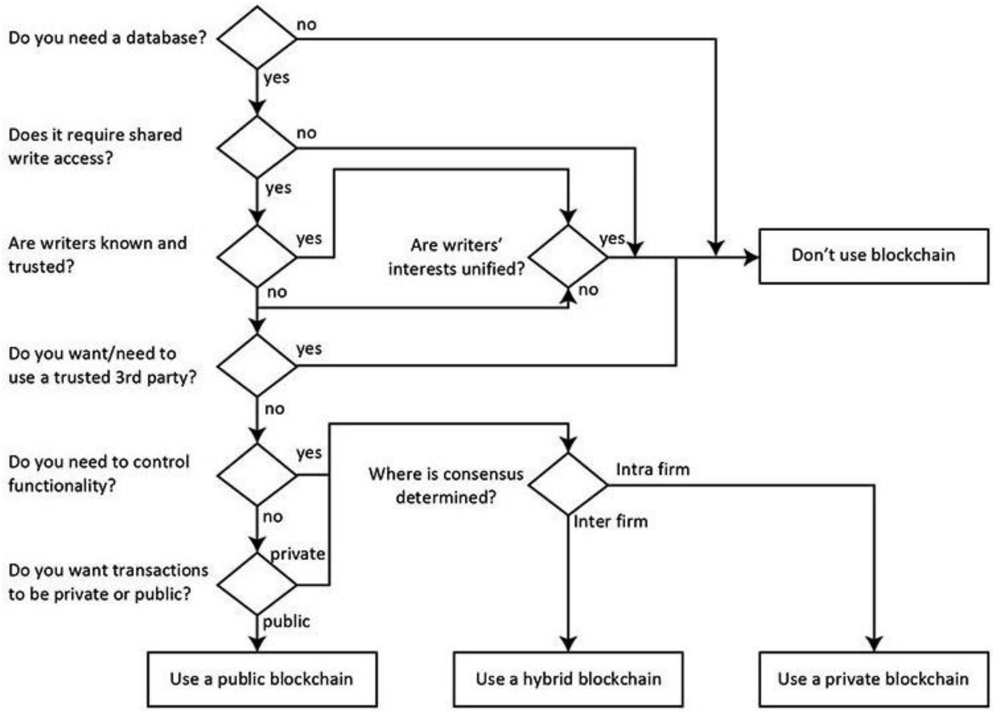

Do you need a database?
no
yes
Does it require shared write access?
no
yes
Are writers known and trusted?
yes
no
Are writers' interests unified?
yes
no
Don't use blockchain
Do you want/need to use a trusted 3rd party?
yes
no
Do you need to control functionality?
yes
no
Where is consensus determined?
Intra firm
Inter firm
Do you want transactions to be private or public?
private
public
Use a public blockchain
Use a hybrid blockchain
Use a private blockchain

Figure 4 When to use blockchain

Only on systems where a trusted third party is required, a blockchain implementation is necessary. Just integrating blockchain in any system cannot be a one stop security solution. It may in turn add more resources, processes and computational intermediaries in already complicated systems.

3 Methodologies

This paper is an output of mostly analytical research. A thorough qualitative research was conducted with exploration as a main agenda. The expected results from the series of explorations of blogs, websites and research papers from the journals was a better understanding of underlying reasons, case studies, and comparisons of existing technologies and future models.

The research aims to provide insights into the problem or helps to develop ideas or hypotheses for further potential qualitative research. Following steps were followed for developing a methodology framework for this paper:

- Investing existing technologies that facilitate better security measures.
- Navigating the limitations of the existing technologies.
- Finding areas in which blockchain can be integrated or substituted.
- Drawing out conclusions that can improve the security of IoT systems while eliminating the scalability and privacy issues.

4 Existing Technologies and Limitations

The gradual advancement of innovative IoT solutions, with growing prevalence of embedded intelligent systems in broad spectrum of use cases such as health, surveillance, production dictate the need for reliable security.

The challenges associated with reliable security in IoT are driven most by the fact that IoT systems are almost invariably distributed over a wide geography, even in the uncontrollable open environments. Additionally, end-to-end standards for architecture, networking or security have not been fully developed, stabilized, adopted or implemented across the industry [21].

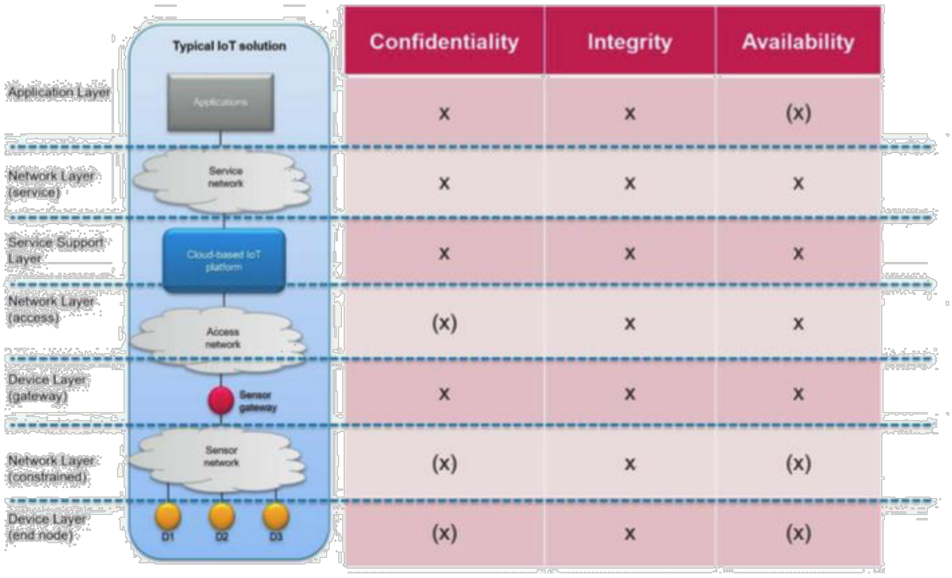
The Wireless Sensor Networks (WSNs) and Machine-to-Machine (M2M) or Cyber Physical Systems (CPS) have now evolved as integral components for the broader term IoT. Consequently, the security problems related to WSN, M2M, or CPS continue to arise in the context of IoT with the IP protocol being the main standard for connectivity [22].

The entire deployment architecture therefore needs to be secured from attacks which may hinder the services provided by IoT as well as may pose threat to privacy, integrity or confidentiality of data.

Since the IoT paradigm represents a collection of interconnected networks, and heterogeneous devices, it inherits the conventional security issues related to the computer networks. The constrained resources pose further challenges to IoT security since the small devices or things containing sensors have limited power and memory [23]. Consequently, the security solutions need to be adapted to the constrained architectures.

4.1 Layers of IoT system in terms of CIA triad

The InfocomMedia Development Authority of Singapore (IMDA) has a brief overlay of CIA triad in IoT systems [24].



	Confidentiality	Integrity	Availability
Application Layer	x	x	(x)
Network Layer (service)	x	x	x
Service Support Layer	x	x	x
Network Layer (access)	(x)	x	x
Device Layer (gateway)	x	x	x
Network Layer (constrained)	(x)	x	(x)
Device Layer (end node)	(x)	x	(x)

Figure 5 Proposed layers of IoT model [26]

There are several models for IoT systems, in one of them, operations of IoT devices can also be modelled into a layered system consisting in the layers as shown in the table above.

For device layer (gateway), “Confidentiality”, “Integrity” and “Availability” are recommended because of the assumption that gateway is not constrained. In fact, gateway should also act as a security gateway for remote access to the local sensor network and its devices. It is important for the gateway to establish a secure connection for communication between cloud platforms and the devices. In addition, the gateway can also act as an agent for the cloud platform to monitor and track the security status of the connected devices.

For network layer (access), “Integrity” and “Availability” are typically provided for public network service providers, while “Confidentiality” is an add-on function.

For service support layer, “Confidentiality”, “Integrity” and “Availability” are recommended because the cloud platform hosts data from multiple sensor networks and users, where some are probably sensitive.

For network layer (service), “Confidentiality”, “Integrity” and “Availability” are recommended because potentially user and processed data are exchanged over public networks or the internet.

For application layer, “Confidentiality” is recommended to safeguard sensitive data in storage and “Integrity” is required to safeguard commands invoked from applications.

Even in theory, a centralized security model will be very difficult to manage and scale and also vulnerable to all sorts of attacks. This is especially risky in the IoT ecosystem as some of the IoT devices can be too important to fail, especially if they are sensors that carry valuable information. A DDoS attack on medical industry IoT devices can prove to be fatal [25]and so will a similar attack in the supply chain for the food industry [26].

4.2 Initial Considerations

4.2.1 Security Requirements for IoT

For a secure IoT deployment, various mechanisms and parameters need to be reckoned with as described below.

Data privacy, confidentiality and integrity as IoT data travels through multiple hops in a network, a proper encryption mechanism is required to ensure the confidentiality of data. Due to a diverse integration of services, devices and network, the data stored on a device is vulnerable to privacy violation by compromising nodes existing in an IoT network. The IoT devices susceptible to attacks may cause an attacker to impact the data integrity by modifying the stored data for malicious purposes [27].

Authentication, authorization and accounting to secure communication in IoT, the authentication is required between two parties communicating with each other. For privileged access to services, the devices must be authenticated. The diversity of authentication mechanisms for IoT exists mainly due to the diverse heterogeneous underlying architectures and environments which support IoT devices [28].

These environments pose a challenge for defining standard global protocol for authentication in IoT. Similarly, the authorization mechanisms ensure that the access to systems or information is provided to the authorized ones. A proper implementation of authorization and authentication results in a trustworthy environment which ensures a secure environment for communication. Moreover, the accounting for resource usage, along with auditing and reporting provide a reliable mechanism for securing network management [29].

Availability of services: The attacks on IoT devices may hinder the provision of services through the conventional denial-of-service attacks. Various strategies including the sinkhole attacks [30], jamming adversaries or the replay attacks exploit IoT components [31]at different layers to deteriorate the quality-of-service(QoS) being provided to IoT users.

Energy efficiency: The IoT devices are typically resource-constrained and are characterized with low power and less storage. The attacks on IoT architectures may result in an increase in energy consumption by flooding the network and exhausting IoT resources through redundant or forged service requests.

Single Point of failure: A continuous growth of heterogeneous networks for the IoT based infrastructure may expose a large number of single-points-of-failure which may in turn deteriorate the services envisioned through IoT. It necessitates the development of a tamper-proof environment for a large number of IoT devices as well as to provide alternative mechanisms for implementation of a fault-tolerant network.

Most existing IoT systems are characterized by Machine-to-Machine(M2M) interaction [32] and maintaining trust between participating machines is still a big challenge in the IOT ecosystem. Thus, existing confidentiality, integrity and authenticity gaps can be fulfilled using blockchain.

In blockchain, data is encrypted using cryptographic algorithms as well as the hashing techniques. Thus, the application of blockchain in an IoT ecosystem can offer better security services.

4.3 Blockchain for IoT Security

In the present context, almost all top cryptocurrencies with exception of Ripple are utilizing public blockchain for recording financial transactions [33], where transactions are encoded and kept by all the participants or nodes across the network. Thus, all transactions are transparent, and any modifications can be easily detected or traced. Blockchain technology has been foreseen by industry and research community as a disruptive technology that is poised to play a major role in managing, controlling, and most importantly securing IoT devices in terms of CIA.

The approach is to set up a private blockchain having scope limited within an institution or some institutional or corporate entity. The private P2P network having locally limited scope instead of global scope implies discovery, transaction querying, invoking, synchronization and consensus – require less aggregate bandwidth and far-end assurance of reliable delivery across large network [34].

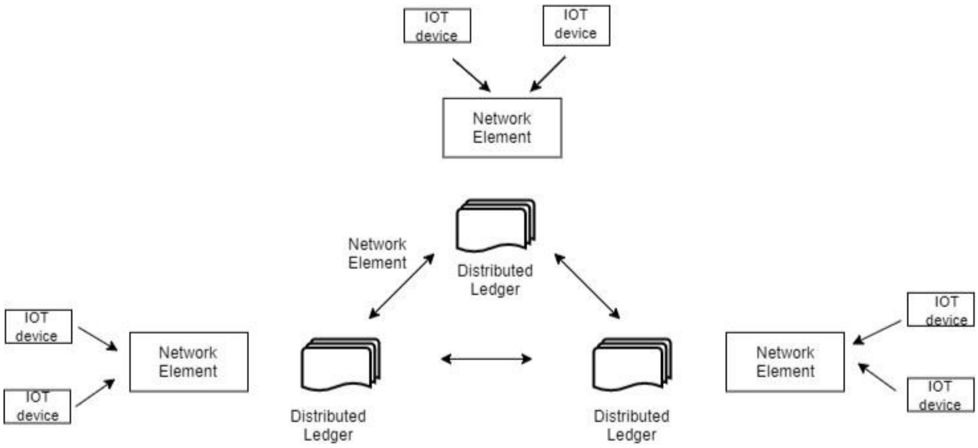


Figure 6 Integrating blockchain in IoT solutions

Also, the number of transactions and/or blocks to be processed and stored may be smaller. The potential limitations of implementing such roles in generic IoT nodes to create distributed ledgers due to limited computing and storage capacity of IoT devices is perhaps evident and the blockchain capabilities may thus have to be implemented in selected Network Elements (NEs) in the network.

One would not expect that a low-end IoT node, such as remote sensor or actuator would vouch for integrity of the entire ecosystem data; thus, only some select NEs may be expected to take on that more onerous role.

The source (here being a “miner”) creates a transaction block containing data and creates the first block. Other NEs will append the next block in the blockchain, as the information travels through the network to its ultimate (intended) destination, typically some analytics engine in the cloud for analysis, trending, and likely also storage. Here storage also enjoys the integrity protection of the blockchain. For example, these transactions could be claims, photos, and so on.

Gateway-level: Here the individual pendent users create data that is not immediately protected for integrity; however, once the data reaches the gateway, it is incorporated into the blockchain along with data from other users. One motivation for this approach is that the individual end nodes may lack the computational capabilities to create hashes of (possibly large) blocks of data.

Site-level: Here the individual users at a given site (for example sensors or robots on a factory floor) create data that is not immediately protected for integrity at the device level; however, once the data reaches the local concentration node (for example a layer 2 switch, a Wi-Fi access point, a router, a firewall, and so on), it is incorporated into the blockchain along with data from other site users. Again, one motivation for this approach is that the individual end nodes may lack the computational capabilities to create hashes of (possibly large) blocks of data, but the site-based NE would have the computational power.

Device level: Here each individual device has the capability, as well as the imposed requirement, to build blockchains of data to be immediately protected.

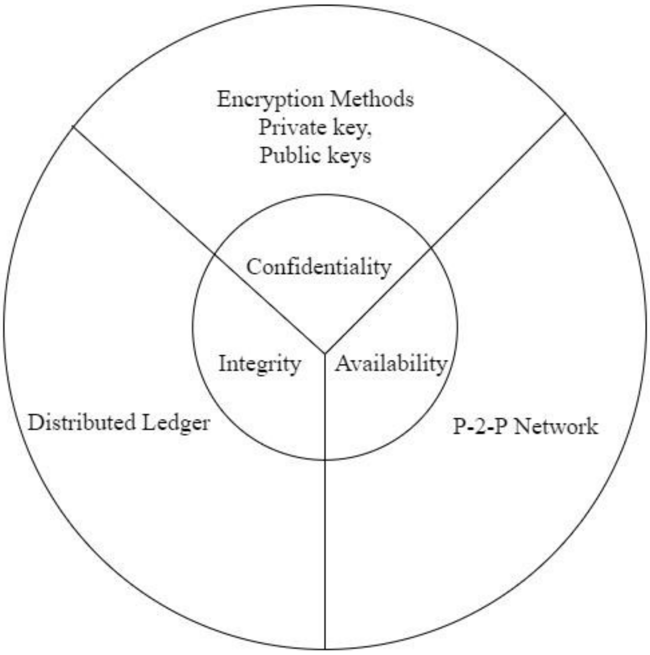


Figure 7 How blockchain fits into CIA triad

Thus, realized architecture ensures the confidentiality measure as the network is private and each node is uniquely characterized by its private key and public keys. Furthermore, the private blockchain means that the access to distributed ledger is only within an institution or business entity.

Since the network is peer-to-peer and no single party reserves the total right to modify or remove information contained in the distributed ledger. Even if an intruder changes the state of a block or blocks in his node the acceptance of its authenticity is discarded once the consensus among other nodes in the network is done thus any transaction in any node once created is immutable the integrity of the chain is maintained.

Application of the blockchain in any IoT ecosystem will further enhance the availability and reliability by completely eliminating any Single Point of Failure (SPF).

Blockchains can also be used at the lower layer of the communications model to provide integrity for information transfer over a chained number of links, converging from the edge towards a centralized analytics engine or a cloud-based server.

Beyond security per se there are many other applications of blockchains in the IoT environment; these include, but are not limited, to the following:

- Manage device configuration, store sensor data, and enable micropayments support e-business on the IoT (UBI is one example)

- Create decentralized, shared economy applications that allow people to monetize their things to create wealth; beyond Airbnb and Uber there are many other opportunities to share in the digital economy, for example sharing applications, e.g., peer-to-peer automatic payment mechanisms, foreign exchange platforms, and digital rights management

- Supply-chain provenance

4.4 Implementation of existing technology and limitations

There are several techniques used for CIA in IoT sphere. A majority of them are machine to machine encryption and thus cannot scale to a decentralized model, however these access control-based models can be expanded and worked upon.

4.4.1 IBAC (Identity Based Access Control):

IBAC is a legacy technique still used for small IoT systems used in today’s IoT implementations. This framework allows access control to different units based on identity.

4.4.2 RBAC (Role Based Access Control):

Role-based access control is widely used in today's IoT implementations. This framework allows users to define roles, assign entities, allow/limit resource usage all being overseen by a central infrastructure.

4.4.3 ABAC (Attribute Based Access Control):

ABAC differs with RBAC in a sense that instead of users having specific roles, an attribute may refer to either of a user or to a particular resource or to the surrounding environment.

An "attribute" in this case can be defined as a particular property, role or permission associated to a part of a system. [35]

4.5 Limitations of existing techniques and need for blockchain

- Often RBAC can lead to a role explosion, i.e. if one employee requires access to ten applications or services with two roles per application, the number of roles being managed for this single employee is twenty. As these number scale across organizations spanning across different geographical planes, these records can amount to thousands, this is not only hard to manage but prone to all kinds of database errors.
- With RBAC, it is impossible to use contextual information e.g. time, user location, device type etc.
- RBAC ignores resource meta-data e.g. medical record owner.
- There is a lot of room for human error, very often, administrators are found fumbling up with creating, reading, updating and deleting the records and database is flooded with dozens if not hundreds of roles and permissions
- Access reviews are painful, error-prone and lengthy.
- RBAC based systems are unable of performing dynamic segregation of duty, one of the features needed for decentralized systems [36].

ABAC though an improvement upon RBAC, much more dynamic flexible and context based, still is centralized and prone to single point of failure and very hard to implement in M2M systems [37].

Blockchain can easily step in as a solution for CIA of these system and aid decentralization. Blockchain eliminates the need for CRUD in the database, facilitate real time communication, limit the use of access lists to smaller networks and make the data flow more transparent. Results

4.6 Advantages of Using Blockchain for IoT CIA Infrastructure

Standalone, both IoT and blockchain have emerged as industry disruptive technologies. There is so much more room for the combination of these two. Blockchain, by nature requires decentralized computing devices(nodes) for reaching consensus this can be definitely supported IoT devices.

On the other hand, IoT devices require a solid CIA framework to function readily and reliably, these features can be provided by blockchain, a handful of notable features are transparency, privacy, immutability.

Wireless Sensor Network (WSN) are often the backbone for IoT devices. Each individual node of the IoT ecosystem is vulnerable to different kinds of cyber-attacks and may serve as a single point of failure. And these devices being mostly leveraged on cloud environments constitutes a single centralized system with an obvious single point of failure [38].

A big amount of data is consistently generated and transmitted over the Internet for analytics and decision making using IoT devices. Data privacy and authentication and in a broader scope, all the three pillars of CIA triads, play a major role in ensuring the services and reliability of data in critical decision making. As there can be several malicious attempts and data injection to give a wrong record of the ongoing process.

Some of the several real-world benefits range from Supply chain to Pharmaceuticals, logistics and insurance [41].

4.6.1 Supply Chain:

A blockchain backed supply chain leverages the power of a shared distributed ledger which provides an indisputable record of all the data related to the shipping cycle. This includes the status, storage environment conditions and few more variables specific to this industry.

Verifiability of Product Source:

Both producers and consumers are able to track the life cycle of a product in the supply chain using IoT and blockchain. A real-life example can be the whole supply chain for Tuna Cans, from the day the fish was caught in the ocean, registered, sold and when the constituencies of the fish were changed to pack it in the form of a tuna can.

4.6.2 Smart Contracts for Cross Border Chains and Trade:

Cross border trades can be easily made online via smart contracts i.e. the contract is only executed when the prespecified terms and conditions have met. IoT devices can serve as a validator for the latter part ensuring the chain goes smoothly before the contract has been executed.

This means elimination of a lot of intermediaries and paperwork hassle and saving up on the labor costs as well as human error.

Blockchain and IoT together ensure safe cargo shipping, even in cross-border trades. The system acts like an online arrangement between all the parties involved in a trade. It can be said that the terms and conditions of the contract are written in computer codes, facilitating financial transactions among unknown parties without dispute [39].

Minimization of paperwork is another area where blockchain and IoT technologies can be beneficial. Transportation of a container from one place to another involves many intermediaries. As most of the companies are still using traditional methods of trade, the requirement of paperwork remains. Blockchain and IoT allows companies to save on labor cost and ensure data protection by removing paperwork throughout the ecosystem.

4.6.3 Blockchain and IoT for Pharmaceuticals

Pharmaceutical chains, just like other supply chains, must be devoid of any errors or miscalculations. During the shipment of pharmaceuticals, the temperature control within licensed ranges is a must have functionality.

If for some reasons, there is a temperature difference outside the specified range, there can be a sizable difference in the quality of the drugs being manufactured. Blockchain based IoT devices can serve a quick fix to this problem [40].

DOE Temperature Logger is one such implementation which can utilize Bluetooth to download data for all devices at the same time.

In a real-life example, when a shipment of intermediary products arrives at the warehouse, there can be a router or trigger at the door that will monitor all the sensors within a certain range, and then can automatically download all the relevant data. This eliminated the need of a human having to take the loggers off of every pallet, investigate and verify all the devices thus by overcomplicating the whole procedure [41].

4.6.4 To make insurance faster and reliable

It is no secret that IoT systems should be decentralized. There have been several studies that suggest that the usage of low-power wide-area network (LPWAN) technology, which is decentralized by nature, can allow people to set up their own networks and customize it to their needs.

This ensures the data has not been compromised and allows end users to operate without doubts.

4.6.5 Blockchain in Logistics

The logistics companies have already been implementing IoT devices for some years now. A common implementation as shown in the figure below depicts how modern vehicles contain a multitude of sensors for different purposes. This includes Geo Sensors, temperature, geo sensors etc.

The implementation of smart contracts can add another level of automation in these kinds of businesses. Between unauthenticated nodes, or the nodes that have not gone through the usual CIA cycle, the payments can be held at any stage of the logistic cycle.

The implementation of blockchain provides a PKI based secured transaction system for the participants. The universal ledger of proof also adds the global element to the whole process.

4.7 Challenges to Blockchain and IoT

Moving a centralized infrastructure to a decentralized model is definitely not easy and comes with its own caveats. The main drawbacks with implementing blockchain for IoT CIA can be summarized in the diagram below:

4.7.1 Storage

Data storage on blockchain comes with an extra step of having to store and mine the blocks. There should be incentives generated for the participating nodes for consensus generation, smart contracts can facilitate this transaction.

In a study done about the storage costs for blockchain concluded that blockchain may not be suited for all scenarios but there are many cases where benefits may outweigh the cost and further research was necessary to accurately determine the cost benefit trade- offs [42].

4.7.2 Processing Power and Time

Majority of the blockchains existing today are based on a concept of Proof of Work (PoW).

The authenticity of a record in the existing blockchains is usually done via something called a proof of work. Since IoT devices are restrained by low resource usage, implementing blockchain for CIA can be a daunting task because of energy requirements for the implementation of Proof of Work algorithm.

Thus, there can be several reservations for the application of current blockchain technology to the IoT universe. IoT applications inherently focus on energy-efficient computing and real-time decision making, this can be especially tedious for blockchain based IoT applications as the distributed ledgers require to solve energy and computation heavy mathematical problems for decentralization [42].

A variable that comes handy in these types of analyses is the block time, the time required to mine a block, (a set of records) and put it permanently in the blockchain. The usual time to mine a bitcoin block is around 10 minutes, Ethereum blockchain-- which most of the existing IoT devices are based in aims to bring that to about 12 seconds but this endangers several blocks being orphaned and is not yet ready for IoT ecosystems that require swift and real time decision making [43].

4.7.3 Scalability:

One of the major hurdles that is limiting the adoption of blockchain in the IoT sphere is the problem of scalability. The rate of transaction execution in the blockchain should facilitate the IoT system but due to the massive numbers of transactions and data exchange, current blockchains are unable to keep up with this. The biggest challenges in this integration are the scalability of ledger and rate of transaction execution in Blockchain [45]. Also implementing blockchain peers into IoT devices can be a lot of resource input and more than the device can handle.

4.7.4 Naming and discovery

The IoT devices need a unified way to discover and interact with the surrounding smart environment which is missing in the existing IoT based blockchain solutions. This has raised the problem of existing heterogeneous ecosystems where each service provider adheres to its own protocols IoT devices from interacting when they are affiliated to different providers. This is creating a mass scale interoperability issue [46].

4.7.5 Privacy

Though blockchain provides an immutable distributed ledger that is available anywhere, this can sometimes be an issue as some confidential data may be available to public.

4.8 Proposed Solutions

4.8.1 Hybrid Solutions

In most of the existing IoT spheres, data exchanges with external ledger takes place in limited section of the whole architecture. Rest of data exchanges take place only among IoT devices.

A more hybrid approach can be taken to optimize the split between the interactions that occur in real-time and the ones and the ones that are validated via blockchain. Instead of saving entire data of the IoT network in the blockchain, cloud storage servers can be used to save the patent data with unique block number, the cloud server can then send the hash of the data blocks to the overlay network [47].

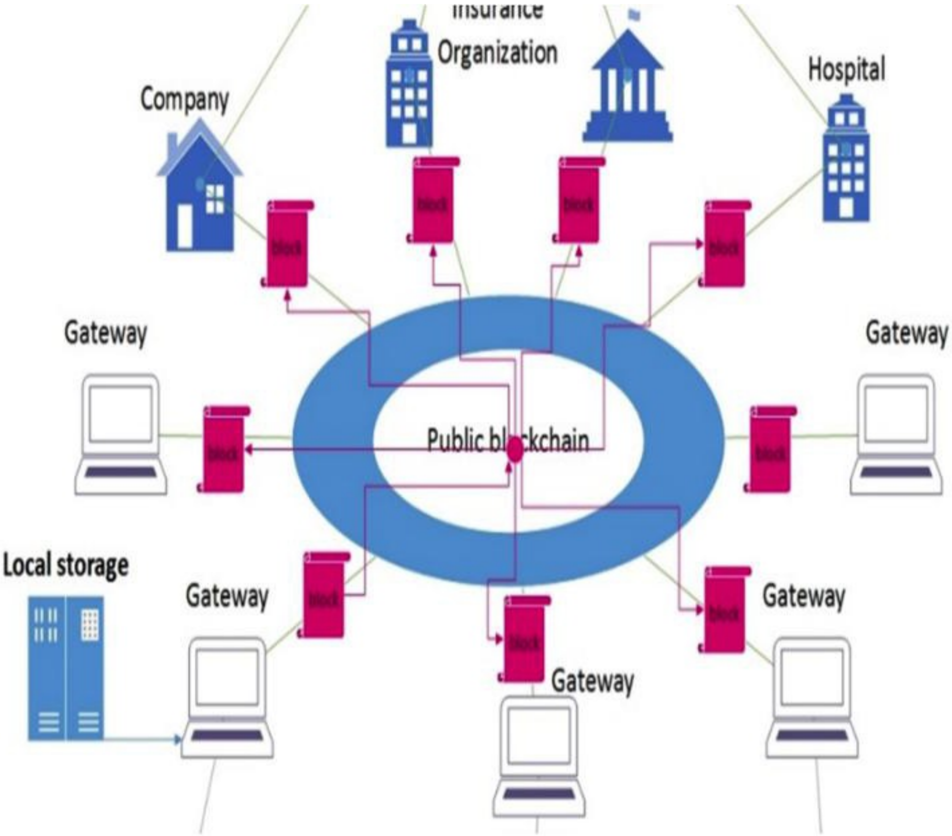


Figure 8 Hybrid Blockchain Implementation in everyday devices

This segmentation into data generating blocks can help categorize data into data blocks, some form of private blockchain can be used in each of these “data emitters” and each of the block can be sequentially added to the blockchain. This solves the scalability issue to some extent and makes the IoT system more secure with more diverse points offailure.

4.8.2 Use of Hyperledger Fabric

Hyperledger Fabric is a modular blockchain framework that acts as a foundation for developing blockchain-based products, solutions, and applications using plug-and-play components that are aimed for use within private enterprises. [47]

Traditional public blockchain are not equipped with the ability to make certain transactions private. Hyperledger Fabric was designed in response to this as a modular, scalable and secure foundation for offering industrial blockchain solutions so that the data can only flow in a permissioned architecture of devices.

Hyperledger Fabric is a blockchain implementation designed by IBM for industry use cases. A blockchain deployed using hyperleger Fabric stores data in the form of chaincode, a programmatic code on the network that functions similar to smart contracts on other blockchains.

A chaincode can be employed to handle business logic agreed to by members of the network, so it may substitute "smart contract" in traditional blockchain systems. In a traditional blockchain, all transactions are executed sequentially by all nodes, in that sense, the scalability and performance are reduced.

To achieve parallel execution of transaction, hyperledger fabric introduces a novel execute-order-validate blockchain architecture, allowing parallelization of transaction execution and validation [48].

Table 1: Attributes of blockchain and hyperledger fabric

Feature	Attribute	Traditional Blockchain	Hyperledger Fabric
Open Membership	Permissioned/Permission less	Permission less	Permissioned
Immutability	Way of reaching consensus	Proof of work	Pluggable consensus framework
Confidential Self Executability	Smart Contract Support	In specific cases (like Ethereum blockchain through the use of solidity)	Traditional programming languages like Java and Golang

Transaction Confidentiality	Encryption, key-distribution Cryptographic mechanisms	No (All transactions are public by nature)	Smart contract (chaincode) level + fabric-level confidentiality

Table 1

Use of hyper ledger fabric can not only solve the privacy issues as not all the transactions in IoT domain should be of public nature compared to cryptocurrency domain, it also helps to scale blockchain based IoT solutions faster.

Hyperledger loop also solves the problem for specialized skill set as blockchain based development platforms, solidity for example may have a learning curve, compared to hyperledger fabric which does not require developers to master one more programming system.

4.8.3 DAG based ledger consensus

The purpose of using IoT for automation will produce a huge stream of constant data, it may raise issues for resource-stricken devices to process the entire blockchain and issue transactions in the chain.

Integrating traditional blockchain solutions in these scenarios can be counter intuitive because the transaction processing abilities of these devices are affected by the block size [49]. Increasing block size can increase the transaction speed but also causes a data burden on all nodes.

IoT nodes continuously generate a large amount of data and send it through the network. Thus, it becomes necessary for devices with small resources and capacities to utilize the entire blockchain (which is one of the blockchain's main properties) and actively issue transactions on the chain. The most popular blockchain platforms, like Bitcoin and Ethereum, cannot handle such a high volume of transactions because their transaction processing ability is directly affected by the block size [12]. Increasing the block size can lead to an increase in the processed transactions per second, but it also causes a data burden on all nodes. This means the transaction speed of blockchain is still not in the level of traditional financial streams.

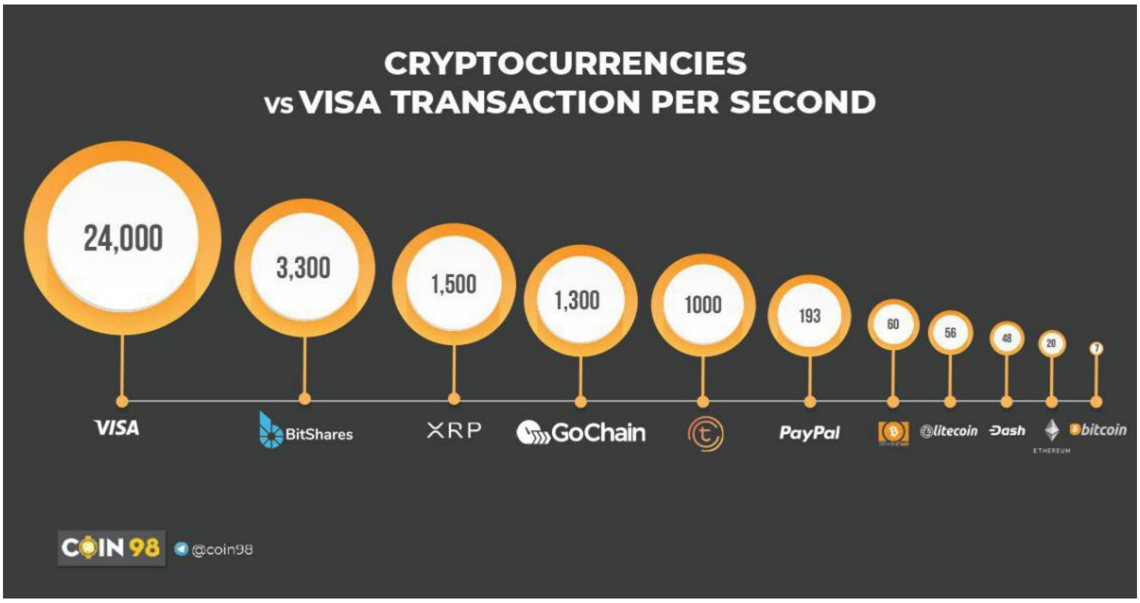


Figure 9 Transaction Speed Comparison Traditional Systems vs Blockchain[52]

Traditional blockchain slows down as the transactions increase, the DAG, on the contrary, works faster as they increase, making it very scalable. There is no mining on DAGs, so that it is no need to charge the participants with high transaction fees. DAGs can be used in many cases where blockchain would not be feasible. A prime example is the Nano-transactions between IoT devices and small sensors [50]

Compared to blockchain which gets more laborious with the addition of more nodes, DAG on the other hand benefits from the addition of new nodes [51].

5 Conclusion

Today's CIA models for IoT devices allow only for a central infrastructure and in themselves they are quite vulnerable. This is due to mainly the constrained resources in IoT devices, immature standards, and the absence of secure hardware and software design, development, and deployment.

The blockchain concept was originally associated with digital currency, but many other potential uses for the technology are emerging, including Integrity applications for IoT data being transacted around a large multi-tier network and or archival systems. Blockchains are powerful tools that go well beyond basic security applications, as described in this paper, because they are principally mechanisms for global shared trust in terms of confidentiality, integrity and availability.

Though blockchain can hop in to the existing IoT ecosystem and facilitate a universal, immutable exchange of data that the devices can use in real time as well as make a robust CIA layers, they are yet to be tested against everyday variables, though it appears blockchain based solutions can be duly implemented, they come with their own caveats. Mainly scalability and privacy issues. Use of hybrid systems, hyperledger fabrics and DAG can solve the scalability issues of a blockchain.

6 Future Work

This paper was limited by the amount of studies done to compare blockchain against the existing technologies side by side, this meant hypothesizing and extrapolating of the information found from the existing research paper and information on the Internet.

There is a lot to be done to make a comparative multivariate analysis for the same system, one with and one without blockchain.

Decentralization certainly helps for quicker adoption and eliminate the single point of failure, but more studies should be made how they solve the existing problems with scalability issues, storage, processing time and lack of market skills.

The integration of existing technologies for one or more pillars of CIA triads into a global blockchain system has also left a lot for wanting. These can be addressed, and a functional ecosystem can be designed integrating these technologies with the power of the blockchain.

7 Required Reflection

When the paper was set out, it was to compare and contrast existing technologies regarding identification, authentication, and secure data transfer using blockchain. However, this appeared to be more daunting for the lack of existing research and data to compare this side by side.

Initial idea for data generation was to find existing IoT based blockchain solutions and ask them to provide data for measurable metrics, this could not be attained for several reasons, the impending force majeure being one of them.

The research though thoroughly done, could have been expanded but it would have been beyond the scope of a bachelor thesis so it may appear a bit inclusive and general except a niche based study, but there are plenty of room to pick up an individual branch and conduct further study on that.

8 References

[1] "10 IoT Security Incidents That Make You Feel Less Secure," 10 January 2020. [Online]. Available: https://www.cisomag.com/10-iot-security-incidents-that-make-you-feel-less-secure/. [Accessed 14 April 2020].

[2] J. &. R. S. &. D. S. (. Sengupta, "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT," Journal of Network and Computer Applications, 2019.

[3] G. &. L. I.-Y. Ra, " A Study on KSI-based Authentication Management and Communication for Secure Smart Home Environments.," KSII Transactions on Internet and Information Systems, 2018.

[4] M. Rouse, " internet of things (IoT)," 2019. [Online]. Available: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT. [Accessed 15 April 2019].

[5] M. P. A. R. a. J. S. O. i. p. Fredrik Dahlqvist, "Growing opportunities in the Internet of Things," [Online]. Available: https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things. [Accessed 14 April 2019].

[6] "The future of IoT: 10 predictions about the Internet of Things," 2019. [Online]. Available: https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html. [Accessed 2019].

[7] "Machine learning for internet of things data analysis: a survey," Digital Communications and Networks, vol. 4, no. 3, pp. 161-175 , August 2018.

[8] "5G and its Impact on the Internet of Things," [Online]. Available: https://www2.stardust-testing.com/en/5g-and-impact-on-iots. [Accessed 17 April 2019].

[9] "https://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable," October 2015. [Online]. Available: https://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable. [Accessed 17 April 2020].

[10] N. Singh, "Benefits of Blockchain Technology," November 2019. [Online]. Available: https://101blockchains.com/benefits-of-blockchain- technology/. [Accessed 18 April 2020].

[11] "Worldwide Blockchain Spending Forecast to Reach $2.9 Billion in 2019, According to New IDC Spending Guide," 4 March 2019. [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS44898819. [Accessed 17 April 2020].

[12] R. Nagappan, “When to use blockchain,” 9 July 2018. [Online]. Available: http://websecuritypatterns.com/blogs/2018/07/09/when-to-use-blockchain-infographic-from-dhs-technology-update/. [Accessed 17 April 2020].

[13] C. Tard, “Genesis Block,” September 2019. [Online]. Available: https://www.investopedia.com/terms/g/genesis-block.asp. [Accessed 20 April 2020].

[14] T. K. Sharma, “What is Solo Mining and How it Works,” 8 August 2017. [Online]. Available: https://www.blockchain-council.org/blockchain/solo-mining-works/. [Accessed 18 April 2020].

[15] A. Tar, “Proof-of-Work Explained,” 17 January 2018. [Online]. Available: https://cointelegraph.com/explained/proof-of-work-explained. [Accessed 21 April 2020].

[16] B. Asolo, “Double Spending Explained,” 21 December 2018. [Online]. Available: https://www.mycryptopedia.com/double-spending-explained/. [Accessed 20 April 2020].

[17] S. Kamara, “Proofs of Storage: Theory, Constructions and Applications,” in International Conference on Algebraic Informatics.

[18] A. K. ,. a. D. Z. Kostis Karantias, “Proof of Burn”.

[19] J. Frankenfield, “Proof of Capacity(Cryptocurrencies),” 2018. [Online]. Available: https://www.investopedia.com/terms/p/proof-capacity-cryptocurrency.asp. [Accessed April 2019].

[20] I. Ivanitskiy, “You Do Not Need Blockchain: Eight Popular Use Cases And Why They Do Not Work,” 22 February 2019. [Online]. Available: https://blog.smartdec.net/you-do-not-need-blockchain-eight-popular-use-cases-and-why-they-do-not-work-f2ecc6cc2129. [Accessed April 2020].

[21] M. A. Q. S. H. G. S. U. Mirza Abdur Razzaq, “Security Issues in the Internet of Things (IoT): A Comprehensive Study,” (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 8, no. 6, 2017.

[22] C.-R. &. H. O. &. T. I.-A. &. O. G. Rad, “ Smart Monitoring of Potato Crop: A Cyber-Physical System Architecture Model in the Field of Precision Agriculture. Agriculture and Agricultural Science Procedia. 6.,” Agriculture and Agricultural Science Procedia, vol. 6 , pp. 73-79, 2015.

[23] S. M. Pattterson, “5 reasons why device makers cannot secure the IoT platform,” 11 September 2017. [Online]. Available: https://www.networkworld.com/article/3223952/5-reasons-why-device-makers-cannot-secure-the-iot-platform.html. [Accessed April 2020].

[24] “Internet of Things (IoT) Cyber Security Guide,” 1 January 2019. [Online]. Available: https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/consultations/open-for-public-comments/consultation-for-iot-cyber-security-guide/imda-iot-cyber-security-guide-annex-a.pdf. [Accessed April2020].

[25] M. B. A. Iftikhar ul Sami, “DoS/DDoS detection for E-healthcare in Internet of Things,” [Online].

[26] Q. Z. Ahead Muhammad Junaid Farooq, “oT Supply Chain Security: Overview, Challenges, and the Road,” Tandon School of Engineering, New York University, Brooklyn.

[27] C. Bannan, “https://techcrunch.com/2016/08/14/the-iot-threat-to-privacy/,” 14 August 2016. [Online]. Available: The IoT Threat to Privacy. [Accessed April 2020].

[28] K. &. K. M. Salah, “ IoT Security: Review, Blockchain Solutions, and Open Challenges. Future Generation Computer Systems.,” Future Generation Computer Systems, 2017.

[29] S. N. Digambar Jadhav, “Need for Resource Management in IoT,” International Journal of Computer Applications, 2016.

[30] “Sink Hole Attack using RPL in IOT”.

[31] A. &. K. D. &. M. M. Hezam, “A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Mode. International,” Journal of Advanced Computer Science and Applications, vol. 9, 2018.

[32] M. Rouse, “machine to machine(M2M),” [Online]. Available: https://internetofthingsagenda.techtarget.com/definition/machine-to-machine-M2M. [Accessed April 2020].

[33] “Top 100 Cryptocurrencies by Market Capitalization,” Coinmarketcap, 2020. [Online]. Available: https://coinmarketcap.com/. [Accessed 2020].

[34] J. Donaldson, “Public vs Private Blockchain In A Wide World Of Unique Applications,” 2017. [Online]. Available: https://mojix.com/private-blockchain/. [Accessed 2020].

[35] A. H. K. a. H. R. H. a. M. H. Davis, “From ABAC to ZBAC , The evolution of access control models,” 2009.

[36] Oren Harell, “The Problem with Role Based Access Control,” 30 May 2019. [Online]. Available: https://blog.plainid.com/problem-with-rbac. [Accessed 2020].

[37] A. J. LEE, “TOWARDS PRACTICAL AND SECURE DECENTRALIZED ATTRIBUTE-BASED AUTHORIZATION SYSTEMS,” University of Illinois at Urbana-Champaign.

[38] T. &. Z. A. Zia, “ Security Issues in Wireless Sensor Networks. 40. 10.1109/ICSNC.2006.66.,” 2006.

[39] Y. &. I. E. &. W. Chang, “ Blockchain in Global Supply Chains and Cross Border Trade: A Critical Synthesis of the State-of-the-Art, Challenges and Opportunities.,” 2019.

[40] S. Radoccia, “Here’s How Blockchain And IoT Are Going To Impact The Pharmaceutical Cold Chain,” 2017. [Online]. Available: Here’s How Blockchain And IoT Are Going To Impact The Pharmaceutical Cold Chain. [Accessed 2020].

[41] Ivan Kourza, How IoT and Blockchain Help Secure Food and Pharmaceutical Cold Chains. [Online]. Available: https://perfectial.com/blog/iot-blockchain-solution/.

[42] *. X. R. J. E. S. J. L. a. A. J. P. Ye¸sem Kurt Peker 1, “A Cost Analysis of Internet of Things Sensor Data Storage on Blockchain via Smart Contracts,” Electronics — Open Access Journal, 2020.

[43] A. &. N. H. &. L. R. &. M. R. &. K. S. (. Zorzo, “Dependable IoT Using Blockchain-Based Technology,” Latin-American Symposium on Dependable Computing , 2018.

[44] M. Swan, “Blockchain Technology: Platforms, Tools and Use Cases,” 2018.

[45] A. G. H. Kaihua Qin, “An overview of blockchain scalability, interoperability and sustainability,” Luzern Imperial College London Liquidity Network.

[46] V. &. P. R. &. K. I. &. S. M. (. C. C. N. d. f. b.-b. s. i. t. I. 1.-6. 1. Daza.

[47] G. S. S. D. a. R. S. Ashutosh Dhar Dwivedi, “ ”A Decentralized Privacy-Preserving Healthcare Blockchain for IoT”,” Big Data Cogn, vol. 10, 2018.

[48] Will Kenton, “Hyperledger Fabric,” February 2020. [Online]. Available: https://www.investopedia.com/terms/h/hyperledger-fabric.asp. [Accessed May 2020].

[49] A. B. Y. M. Y. T. Hagar Meir, “Lockless Transaction Isolation in Hyperledger Fabric,” IBM Haifa Research Lab, Haifa, Israel.

[50] D. Vujičić, D. Jagodić and S. Ranđić, “,” in Blockchain technology, bitcoin, and Ethereum: A brief overview., East Sarajevo, Bosnia-Herzegovina,, 17th IEEE International Symposium INFOTEH-JAHORINA (INFOTEH), 2018.

[51] Q. WangI, “Improving the Scalability of Blockchain through DAG,” Middleware 2019 Doctoral Symposium , Swinburne University of Technology & CSRIO, Data61.

[52] [Online]. Available: https://www.iota.org/. [Accessed 2019].

[53] L. S. Sterling, The Art of Agent-Oriented Modeling, London: The MIT Press, 2009.

[54] [Online]. Available: https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html.

[55] “Internet of Things (IoT) Cyber Security Guide,” 1 Jan 2019. [Online]. Available: https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/consultations/open-for-public-comments/consultation-for-iot-cyber-security-guide/imda-iot-cyber-security-guide-annex-a.pdf.

[57] “The future of IoT: 10 predictions about the Internet of Things,” [Online]. Available: https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html.

[58] “A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. Journal of Network and Computer Applications.,” Journal of Network and Computer Applications, 2019.

[59] J. &. R. S. &. D. S. Sengupta, “A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT.,” Journal of Network and Computer Applications, 2019.

[60] D.-H. K. Lei Hang, Department of Computer Engineering, Jeju National University, Seoul, 2019.

Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Basanta Lamichhane

1. grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis

Security Considerations For Implementation Of Blockchain In IoT Infrastructure
supervised by Tauseef Ahmed

1.1 to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

1.2 to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.

3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

7th January 2021

[1] *The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.*