Using innovation from block chain technology to address privacy and security problems of Internet of Things

Jitendra Manocha

KTH Industrial Engineering and Management

Master of Science Thesis 2017
KTH Industrial Engineering and Management
SE-100 44 STOCKHOLM

KTH Industrial Engineering and Management

Master of Science Thesis INDEK 2017:68

Using innovation from block chain technology to address privacy and security problems of Internet of Things

Jitendra Manocha

Approved 2017-05-30	Examiner Gregg Vanourek	Supervisor Terrence Brown

Abstract

Internet of things (IoT) is growing at a phenomenal speed and outpacing all the technological revolutions that occurred in the past. Together with window of opportunity it also poses quite a few challenges. One of the most important and unresolved challenge is vulnerability in security and privacy in IoT. This is mainly due to lack of a global decentralized standard even though characteristically IoT is based on distributed systems. Due to lack of standard IoT has interoperability issue between different devices and platform suppliers which implicitly creates need of reliance on the suppliers as they store and control user data. There is no decentralized industry wide solution which can offer the control of user data and security back to the user. While experts in IoT are still wondering on solving the challenge, a new Block chain technology has surfaced in past few years and showed signs of disruptive innovation in financial industry. This technology is decentralized, secure and private. Let alone information, block chain innovation has proven to keep assets secure. Recently few forms of block chains have emerged. This research will focus on analyzing the innovative block chain technology, their characteristics specifically the types of block chain to address the privacy and security challenges of IoT. Research proposes a new concept of hybrid block chain as a solution to IoT security and privacy problem.

Key-words: Innovation, Block chain, Privacy, Security, IoT, Hybrid,

Acknowledgements

I would like to express my heartfelt gratitude to all the interviewees who spared their valuable time to contribute to my thesis.

My sincere thanks to my supervisor Prof. Terrence Brown for his constant support, and timely guidance throughout the thesis process. He encouraged me to limit my boundaries of thesis and seek meaning full conclusion. I am truly indebted to his contribution.

Table of Contents

List of Figures

Definition and Abbreviation

Asset	Anything that produces value and can be controlled or owned, assets can be tangible (Physically owned) or intangible (Financial, intellectual)
Consensus	Process in which majority of validators agree on set of rules or procedure or state (Svensson & Leung 2015)
Decentralized	Delegation of authority in a hierarchy or a network
Diffusion	“Process by which an innovation is communicated or spreads over a period of time among the members of social systems” (Rogers 1995)
Disruptive	Displacing existing market, process, technology and creating something new. (Christensen & Overdorf 2000)
Distributed Ledger	Each Participant in the network has same copy of the ledger
Hybrid	Combination of two or more concepts
Immutable	Record that cannot be changed
Innovation	“An idea, practice or object that perceived as new by an individual or other unit of adoption” (Rogers 1995)
IoT	Internet of Things
Latency	Average transaction confirmation/block creation time
Ledger	A book maintained to keep records of asset transfer transactions
Miner	Node or participant in the network validating the transaction and submitting the proof of work
PoS	Proof of Stake, Type of consensus protocol where incentives are based on stake
PoW	Proof of Work, Type of consensus protocol where incentives are based on work
Pseudonymity	Public keys and transactions shall not reveal real identities
Scalability	Ability to handle changes in latency and throughput when number of nodes in the network is increased
Transaction	Event which captures agreement between two or more parties about transfer of value or information.

1. Introduction

1.1 Background

Internet of things is the network of several physical devices which are connected on Internet (International Telecommunication Union 2015). Ericsson forecasts that by 2022 there will be 18 Billion IoT devices(Ericsson 2016). These devices interact with each other and are constantly evolving with emerging new use cases, such as connected car, connected home. Consequently, these devices generate and collect lot of info and data from general and personal use. With advent of Artificial Intelligence, Robotics as new IoT enhancing technologies data collection and generation will increase exponentially. Though awareness around personal data is increasing it is often undervalued however personal data is a valuable asset in new economy(World Economic Forum 2011). While we all share the benefits of a data-driven society, there is a growing concern about user privacy and security.

Internet of things is not owned by single entity in the world and has a distributed nature where different smart devices are deployed and connected to serve user needs in a distributed fashion (Sicari et al. 2015). This distributed model has devices from different suppliers like Samsung, Apple, Amazon, Bosch, and few niche companies into smart lock, smart homes. It creates supplier dependency as personal data is in control of these centralized companies.

Centralized organizations both public and private, control large quantities of personal and sensitive information. Individuals have little or no control over the data that is stored about them and how it is used. Europol predicted in 2014 that soon there will be organized crime due to internet of things (Press release 2014) as hackers might hack into your smart home or connected car and perform crime. Thanks to the delay of faster adoption of technology there haven't been many incidence however challenge is still there.

IoT may be classified into IoT Platform and connected devices, where platform providers are generally start-ups, large companies, or public institutions. Connected devices providers are small companies, big/small enterprises or Telecom operators. Usually, device provider requires an IoT platform to manage their devices. They sometimes may rely on an external platform provider. Ideally devices provider becomes the user of IoT platform.

Investigating current suppliers of IoT platform we may find Bosch, Ericsson, IBM, Samsung, Yaler, Xively, Thingworx, Everythng (Bosch n.d.; Samsung n.d.; IBM n.d.; Ericsson n.d.; Yaler n.d.; Xively n.d.; Thingworx n.d.; Everythng n.d.) as suppliers. These are just a few from many. All have a different offering and their IoT platforms are not interoperable due to lack of a standard in the eco system.

One the other hand devices provider vary from very large companies to smaller startups, and in many cases IoT platform provider provides its own devices too.(Bosch n.d.; Samsung n.d.).

These companies act as silos and focused on their own solutions with their own interfaces. Currently, there is no vibrant collaborative IoT ecosystem, since the entry barriers are high and the potential gain is low for a single stakeholder invest in an eco-system. (Bröring et al. n.d.).

Individual companies provide their own devices and system, which may not be interoperable with other manufacturers devices or system. These devices need to trust each other and current infrastructure doesn't allow that. This poses a serious challenge on user privacy and security as the individual companies can make illegitimate use of the data (Conoscenti et al. 2016) and may not follow all security related specifications and thus vulnerable to risks.

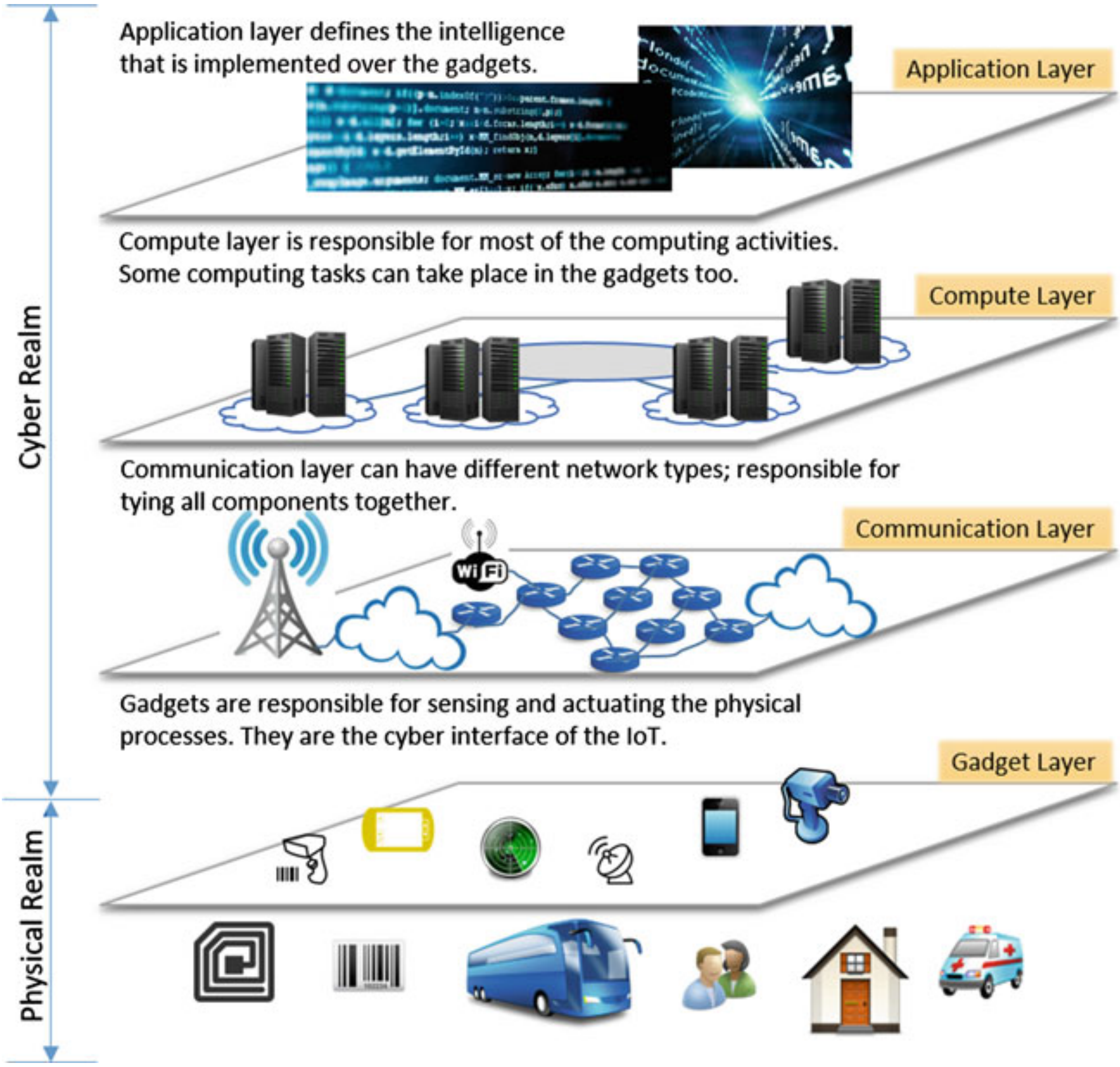

Application layer defines the intelligence that is implemented over the gadgets.
Application Layer
Compute layer is responsible for most of the computing activities. Some computing tasks can take place in the gadgets too.
Compute Layer
Communication layer can have different network types; responsible for tying all components together.
Communication Layer
Wi Fi
Gadgets are responsible for sensing and actuating the physical processes. They are the cyber interface of the IoT.
Gadget Layer
Cyber Realm
Physical Realm

Figure 1.1 Security challenges in different layers of IoT (Misra et al. 2017)

Figure 1.1 visualizes different operational layers above IoT and every layer has its own risks and threats to security. Key security risks are in the physical layers such as counterfeit attacks, false attacks, physical damage to network or information tempering. Rest of the layers are the same since internet era (Cyber security), as an example communication layer is threatened with DoS and DDoS attacks. For the Application Layer, major risks are information disclosure, authentication, illegal human intervention, unstable platform. Challenges in physical layer relate to new IoT devices and appliances and with expansion of IoT it requires new solutions. (Misra et al. 2017)

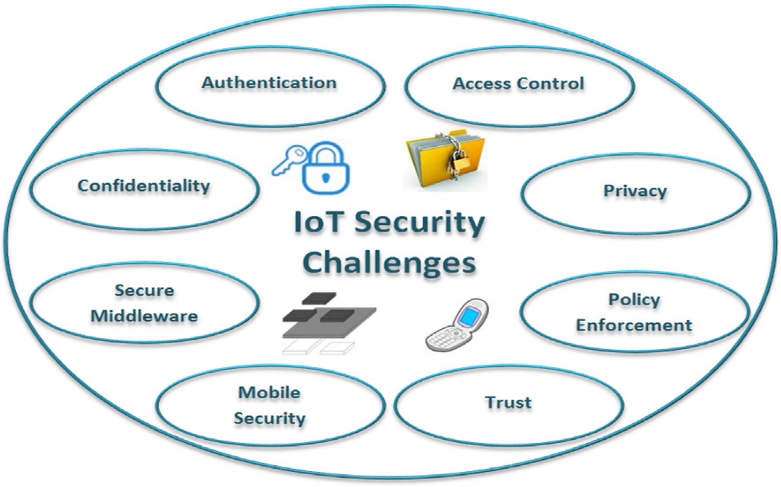


Figure 1.2 Main security Issues in IoT (Sicari et al. 2015)

Further elaborating on security areas of IoT Sicari et al. outlines the number of security issues as depicted in figure 1.2. Sicari described that number of research projects are running across countries and continents to look into Security and Privacy issues of IoT (Sicari et al. 2015), however till date there is no single technological answer discovered.

Moreover in a recent study Fernandes A (Fernandes et al. 2016) analyzed the security issues in home appliances and discovered flaws in devices (Smart locks, smart TVs, sensors) from individual suppliers, these flaws could lead to theft, vandalism, annoyance not only to personnel living the connected home but also to the society. Figure 1.3 depicts different IoT application in a smart home.

An example could be a connected oven or the heating system, which could be controlled remotely on smart app. There is a possibility that hacker can trigger a fire alarm and call the fire brigade automatically, and if it is done on a mass scale, this can create chaos in the society.
Most appliances are from different IoT device/object manufacturer and no single body apart from user can take responsibility of the vulnerability across devices.

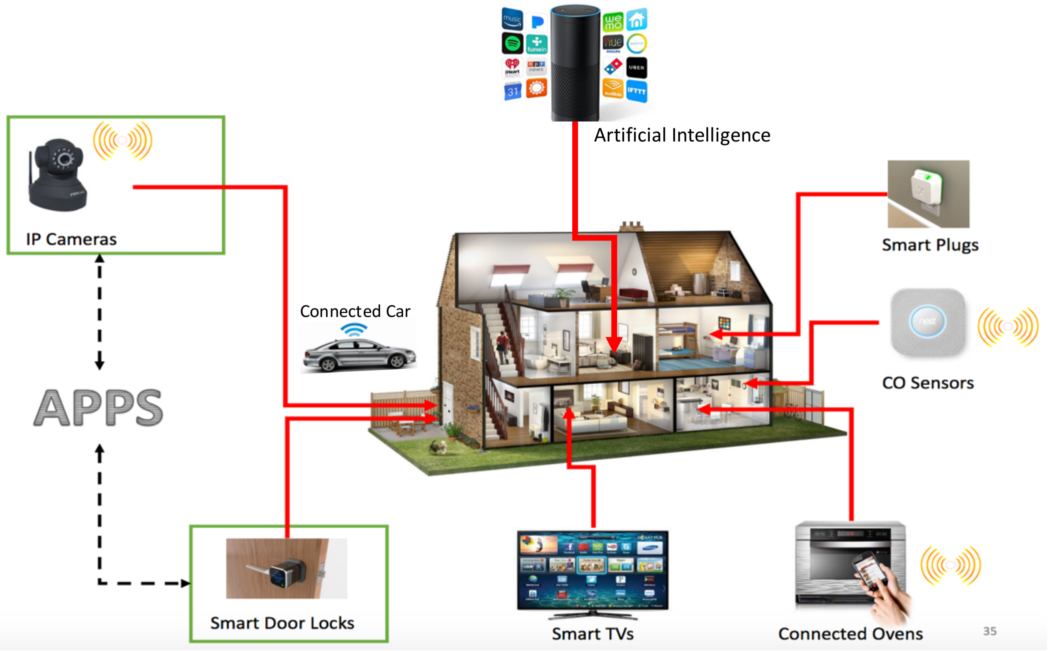


Figure 1.3 Security Analysis of Emerging Smart Home Applications (Fernandes et al. 2016)

Similarly, for privacy of the user and devices in IoT there are equal concerns and according to report from NIST US (NIST 2014), Unlike the traditional energy grid, the smart grid may be viewed by some as carrying private and/or confidential electronic communications between utilities and end-users, possibly between utilities and Third Parties, and between end-users and Third Parties.

Figure 1.4 shows detailed usage collected in minutes and data collected from each appliance such as what time Kitchen lights were turned on, what time was the stove in use and when was the electric heater used. Smart meter is a connected device in IoT and can interact with other devices, collect the data and store and send the data to requesting nodes/server. This data may be very interesting for an adversary to see the pattern of the user daily routine and misuse the information and subsequently remotely trigger or act.

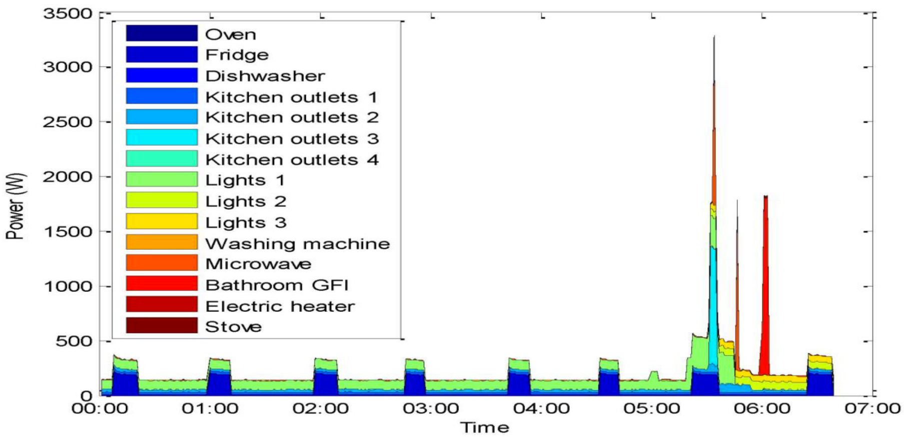


Figure 1.4 Smart meter Data Collected at 1 Minute Intervals (NIST 2014)

Smart grid and smart meter bring new challenges in privacy, which can lead to detailed insights and information about device usage, user behaviour, lifestyle pattern. There is good possibility that in IoT personal information of user may be exposed to a large extent.
An example has been recently published by Prof Stuart M regarding the vulnerability of IoT, which stats that apart from technological solution we may also need to look into infrastructural, governance aspect.(Stuart Madnick n.d.)

When it comes to governance in EU, regulatory bodies (e.g.EU), are making progress after years of efforts in connection to fundamental privacy rights where EU general data protection regulation will pose tough requirements on companies that own consumer personal data.(Union 2016). For IoT specially robotics and artificial intelligence, privacy regulations are still being drafted as it is a challenge to bring robotic devices under law enforcement (GDPR 2016).

It may be argued if IoT is secure and private for an ordinary user, as a user is only secure as long as no adversary is interested in his information and him. It has been observed that privacy and security are one of the few assets which are not valued until compromised.

IoT has vulnerability risks and this implies that there is a need to find a robust and trusted solution and Measures ensuring the architecture's resilience to attacks, data authentication, privacy and access control need to be established. (Weber 2010).

In summary, Problem statement for the research can be phrased as

1. IoT has interoperability problem where devices from one supplier do not always work with other supplier IoT platform, i.e. IoT devices need a common language to talk to each other and trust each other. There is no eco system which enables trust between different devices.
2. IoT devices, due to its nature of exposure, need to be more secure and private as current cyber security solutions may not be robust enough. New solutions with low latency may be required which could be adopted by all suppliers. These solutions need to be based on a distributed technology which is not the case today.

The questions arise if there can be an eco-system and a technology which can help make IoT secure and private? Is there any technology which enables trust in the network without need to trust the network nodes? Is there any solution which is decentralized and supports distributed networks? Is there any innovation in a different sector which has solved similar problems?

While there has been a lot of research, recently some projects have started to develop the IoT ecosystem. One of the prominent one is BigIoT which involves eight companies currently (Bröring et al. n.d.). The project is in infancy phase and has a huge task ahead to integrate all different IoT platforms in one eco system.

The technological aspects are under exploration and definition phase.(Bröring & Mitic 2017).

Another initiative is Industrial Internet Consortium which is also working on accelerating the adoption of IoT devices and trying to address the common concerns. The project is running for past three years and consists of 258 members. Furthermore project is defining the eco system and framework for industrial internet of things, however still under definition.(Previtali et al. 2016)

Fastest initiative in industrial IoT area is introduction of block chain technology for IoT, with many companies committing to further research.

Block chain is the core technology or a distributed ledger, it originated from "Bitcoin" which is crypto currency in digital format. Block chain is the technology behind the crypto currency and realizes a ledger for digital information which is a key component in the Bitcoin system. Bit coin has created a model which can generate and transfer crypto currency without any security issues.
Block chain has proven to be secure and private and managed to solve a crypto currency problem of internet. As compared to current Internet which is called internet of information, block chain technology is being flagged as internet of value due to its robust characteristics.(Tapscott & Tapscott 2016)

There have been some projects considering the block chain technology which is currently disrupting the financial sector primarily, as a solution to security and privacy in IoT. Though block chain builds on decentralization, trust, encryption, security, it may have limitations as well. Thus, there is a need to analyze the block chain technology types and understand what can best fit as answer to the current IoT security and privacy questions. This research will focus on block chain technology.

1.2 Research question and research aim

The purpose of the research is to explore and investigate if privacy and security challenges of IoT can be addressed with emerging block chain technology. Furthermore, to understand if the IoT technology can truly be decentralized using block chain where data owner is the true owner of the data than the IoT platform or service companies. There are several types of block chain in existence currently,
1. Public block chain
2. Private Block chain and third one is proposed in this research which is Hybrid Block chain.
Zhang in his paper (Zhang & Wen 2016) has laid the foundation for hybrid block chain in terms of different business models however his work could be enhanced as technological solution or describing hybrid block chain as well.

The purpose is therefore to evaluate different types of block chains and analyze which ones are best suited to be successful in IoT privacy and security.
The research question is:

"How can block chain technology be used in IoT context to address security and privacy."

The research intends to provide a qualitative evaluation of the question by asking following secondary questions
"What type of block chains exist?, what are the challenges for these block chains in IoT context?"
"How can hybrid block chain impacts the security and Privacy in IoT?"

"Is Hybrid block chain feasible and can scale?"

The result of this research will be valuable to the IoT ecosystem, block chain practitioners as well as entrepreneurs. The study will contribute to advancement of security and privacy research and block chain solution. In addition, the study will implicitly enable learning to connect the dots between technologies and observing the innovation cycle.

1.3 Delimitation

Delimitation is the controllable set of choices made to conduct the research. It can also be defined as boundaries of the research set by researcher.

Literature review has been done on Innovation, IoT and block chain and has been kept on high level. Thereby scope of this research is limited to conceptual and not going into deep technical level to explain. In other words, study doesn't go very deep in the implementation or HOW part.

Study is considering certain aspect of privacy and security hence cannot cover all parts of IoT and all parts of IoT challenges and security aspects specially in block chain context.

Research has considered block chain as possible solution, primarily due to the block chain being disruptive innovation. There may be other solution possible which are not covered in the research.

Additionally, research covers known initiatives of block chain, there may be smaller initiatives which may not have been covered.

Primary data from the research is limited due to limited time for interviews.

2. Literature Review

Following section covers the explanation on the block chain technology, its connection to IoT and current research gap.

Preliminary literature review shows that past studies are primarily focused on understanding Public (Dorri et al. 2016) and private block chains (Zyskind, Nathan & A. Pentland 2015) , in general and some focused-on business models (Zhang & Wen 2016). Limited progress has been made on classifying the technology and its characteristics in a comprehensive manner to evaluate and map the problem with the solution.

Literature has been reviewed from various sources, google scholar, science direct, KTH library, and world wide web searches.
Papers with specific topics in area of security and privacy based on abstract and content overview were chosen for deep investigation. During the literature review It was concluded that that some of the initial research questions were answered so research questions were broken one level down.

2.1 Why Block chain

Block chain technology has been acknowledged as disruptive innovation (Raymaekers 2015), (Enwick et al. 2017) by many banks and financial industry as a whole. A acknowledged this disruption and are investing in research (Seibold & Samman 2016) on how can the industry benefit from this innovation.

One of the major disruption in block chain innovation is decentralization of authority, and transparency by having the distributed ledger.

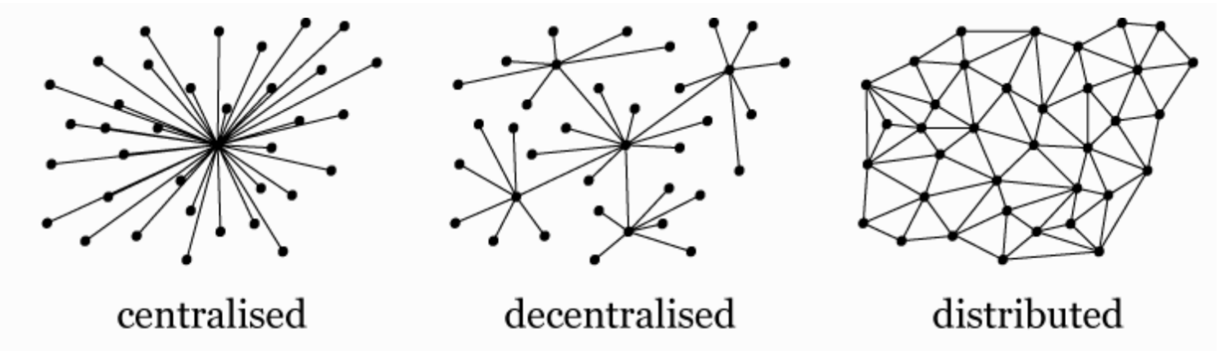


Figure 2.1 Centralized, Decentralized and Distributed networks (Paul 1962)

Paul Baran in his research (Paul 1962) clarified different types of networks, where he suggested that centralized networks are where authority and power is centralized. These networks are vulnerable due to possibility of single point of failure (SPOF). He further explains decentralized networks where there is no central authority and one failed link results into limited disturbance. It becomes impossible to bring down the whole network. Internet is a good example of decentralized network. Although distributed and decentralized network terms used interchangeably, fundamental difference between them is the connection, where every node in distributed networks is connected to every node.

Centralization is not only vulnerable from SPOF in network point of view but also from control point view, as the control and access lies with single party. Banking system, can be used as an example of centralized network where to transfer value between the member every member needs to go through the bank. Bank is in control of all value.

If we refer to requirements of secure IoT, resiliency, device authentication, access control, privacy, decentralization are few listed from research by (Weber 2010),(Ouaddah et al. 2017),(Sicari et al. 2015),(Miorandi et al. 2012).

In comparaison with Block chain technology, the offering from the Block chain serve the requirements listed above, especially in terms of decentralisation, identity management and security (Nakamoto 2008). Due to scaling possibilities block chain technology has potential to develop an eco-system for IoT. Hence block chain was chosen as preferred research.

2.2 Industrial Innovation and Block chain

Following section describes the role of Industrial innovation and diffusion curve of block chain as disruptive innovation.

2.2.1 Innovation and types of Innovations

Innovation is defined as a process of turning opportunities into ideas and putting them practice (Tidd & Bessant John 2009). Definition of innovation according to Drucker “Innovation is the specific tool of entrepreneurs, the means by which they exploit change as an opportunity for a different business or service”. It is capable of being presented as a discipline, capable of being learned, capable of being practiced’ (Drucker, F. 1985).

From the market perspective Innovation can be categorized in different ways such as sustaining innovation vs disruptive innovation. According to Christensen “Sustaining innovation are innovations that make a product or service perform better in ways that customers in the mainstream market already value”. (Christensen & Overdorf 2000)

Christensen defines disruptive innovation as the innovation “Disruptive innovations create an entirely new market through the introduction of a new kind of product or service, one that’s actually worse, initially, as judged by the performance metrics that mainstream customers value.” (Christensen & Overdorf 2000)

Bitcoin, the first application of Block chain has disrupted the whole financial industry and researchers are evaluating different industries where block chain can disrupt.(cb insight 2016). IoT is one of area that can benefit from block chain.

2.2.2 Block chain in Industrial innovation context

ICT industry is constantly embracing transformation in past decade and with Internet of Things and Internet of Value (Block chain) more is in pipeline. To analyze this transformation process different frameworks could be used. First one is the building block framework by Dahmen which acclaims that the transformation of an industry is result of innovation. Secondly, the systems theory by Hughes looking at distinctive types of systems in innovation context. Thirdly, influential factors in diffusion of innovations are considered.

Erik Dahmen a renowned economist from Sweden is known for his development block theory in relation to industrial and technical transformation. Dahmen debated that the economic historians of his time overlooked the means of structural transformation. The framework architected by Dahmen explains means for the transformation of an industry in the form of a causal analysis. Dahmen also claims that industrial transformation is a cycle and moves in steps where new technology (Product or processes) substitutes old, causing a creative destruction and fuels growth. On the similar lines, Schumpeter debated that technological innovations can capsize the existing structure in an industry. (Dahmén 1989)

This creates opportunities for new players, he called this the process of “creative destruction. This can be well connected with block chain technology which is questioning the need of whole financial ecosystem and central authorities. If we further explore the usage of block chain technology in IoT, we can correspond that there is a significant opportunity to replace the old security and privacy solution and replace with new block chain based solutions. Dahmen further develops that Development block is “a sequence of
complementariness which by way of a series of structural tensions, i.e., disequilibria, may result in a balanced situation” (Dahmén 1989).

Dahmen continues to explain further that, structural tensions in an industry are a cause of technological and organization development. Block chain and IoT both can be compared to have created the structural tensions as there is a great deal of similarity in decentralization approach of both technologies which impacts both the organizational systems and technological systems.
Second model that can be applied is systems theory by Hughes (Hughes 1983)

In systems context, contemporary Internet of Things related technological solutions can be compared with Large technical systems which have path dependence or lock-in effects. There is little evidence that IoT solutions from different vendors interwork with each other and provide seamless security. There is an interoperability challenge (Bröring et al. n.d.).
IoT devices are vertically integrated with IoT platform vendors which creates a lock in effect.

Referring to the definition of large technical system from Hughes (Hughes 1983), there are three different phases of adoption of Large technical systems

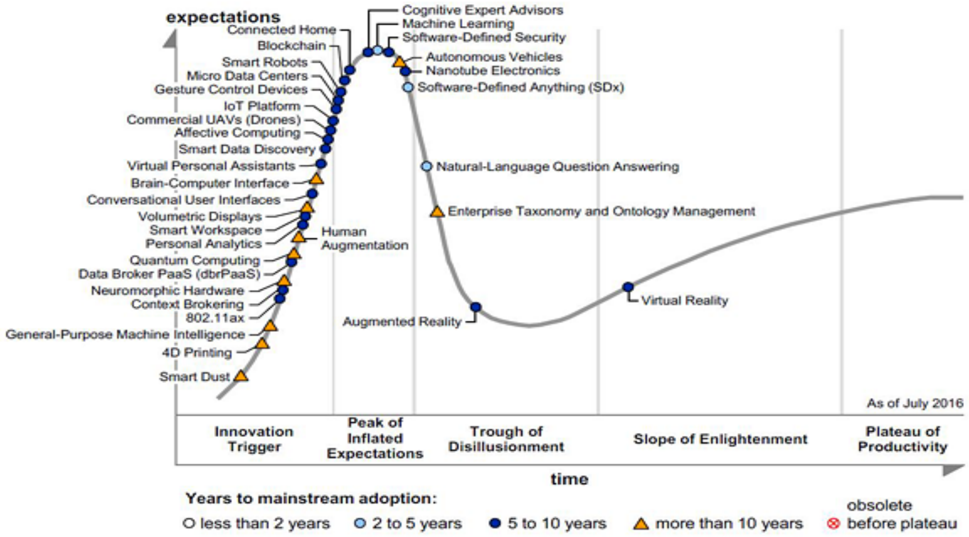
1. Build up phase
2. Expansion phase
3. Stagnation (Maturity) phase,

these phases form an S shape adoption curve referred to as S-curve.

IoT systems can be placed in build-up phase as total number of IoT devices worldwide in 2015 was 5.6 Billion (excluding Mobile phone/tablets) (Ericsson 2016). Industry and Market forecast of IoT in next 15 years is 60 Trillion USD according to forbs. (Columbus 2016)

Similarly block chain technology can be compared with Multi level processing framework (Geels & Schot 2007) which consists of three phases as well,
1. Niche innovation
2. Socio Technical Regime
3. Socio technical landscape.

Referring to Gartner hype cycle (Forni 2016) in figure 2.2 it can be argued if Block chain technology is still in early adopter phase of innovation diffusion curve and at the brink of crossing the chasm.



Source: Gartner (July 2016)

Figure 2.2 Gartner hype cycle 2016 for emerging technologies (Forni & van der Meulen 2016)

2.2.3 Diffusion of Innovation

Diffusion of innovation: Diffusion is the process by which an innovation spreads. If we refer to theory about the diffusion curve from roger, he explains that the diffusion of innovation in a community spreads categorically and defines categories based on adopter profiles.

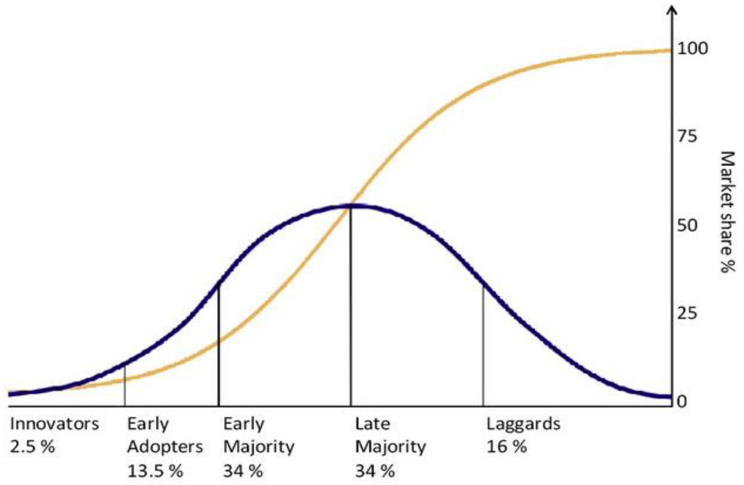


Figure 2.3 Diffusion of Innovation (Roger 1995)

According to latest research from Catalini & Tucker diffusion of innovation is highly influenced by early adopter, the research highlights a case where early adopters can obstruct further diffusion of the technological innovation if they refuse to adopt the technology.(Catalini & Tucker 2016)

Block chain has built up great momentum and through learning process it moved on from early niche innovation to challenge the Status Quo” of finance sector by questioning the need of central authorities. Finance sector has not come to terms with idea of decentralization however has realized the value of block chain as robust and secure platform.

Many companies in financial sector have accelerated research and adoption of block chain in securing their systems. The technology is a breakthrough it is moving in towards socio technical regime where more configuration and use cases are being identified and windows of opportunities are being created to apply potential of block chain technology to other areas. When it comes to application of block chain technology in other areas such as IoT, it may be safely placed in innovator phase.

It may be argued at this stage that this technology has potentially second generation of internet and may move towards social technical landscape, however considering the number of start-ups and investors’ money being invested (1.4B USD were invested in block chain start-ups in (Campbell Rebecca 2016) it can be certainly placed in socio technical regime.

2.3 Block Chain Introduction

Block chain is the underlying technology behind bitcoin which was invented in 2008 by Satoshi Nakamoto (Nakamoto 2008) to create a peer-to-peer digital cash system.

2.3.1 What is Block Chain

Block chain is based on a digital ledger which is immutable, and records transactions in peer to peer public or private networks. The ledger is distributed equally among all members of the network, which implies that each member of the block chain network owns a copy of the ledger. Block chain can be referred as a database of transactions recorded by the nodes in the network in a chronological order.

Transaction can be described as exchange of value from point A to point B. Every transaction is hashed to secure encryption and to make it robust merkle tree hashing algorithm is used. (Merkle 1980).

Figure 2.4 visualizes the block and the way transactions are encrypted in a block by means of a merkle tree.

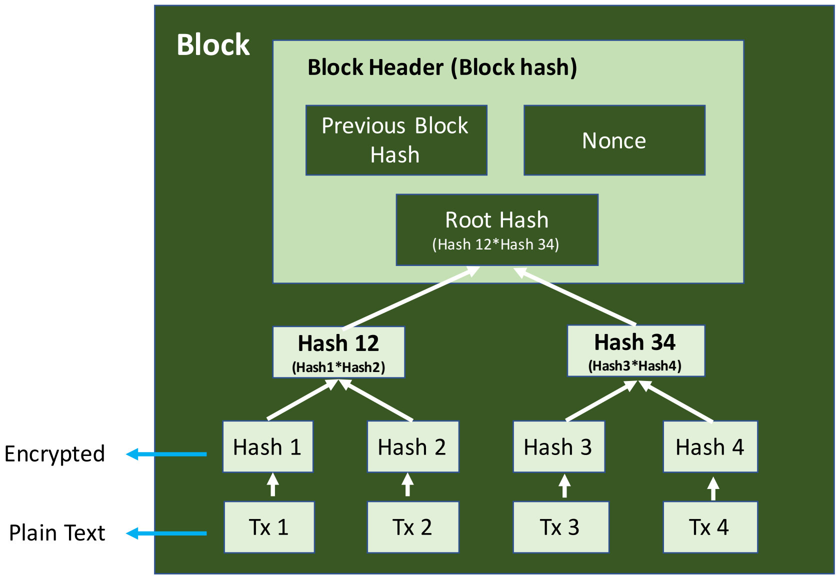


Figure 2.4 What is a block (Nakamoto 2008)

1. Every transaction has a time stamp and is encrypted with hash algorithm using cryptographic signatures.

2. Every hash is further encrypted with hash tree with hash of hash and multiplied with another layer creates a root hash.

3. Nonce represents the level of difficulty in solving the hashing algorithm (Mining the block).

4. Blocks are interlinked, tempering with one transaction means the corrupted chain and whole history of block chain needs to be recreated.

Characteristics mentioned above make block chain immutable.

Figure 2.5 shows the interconnection of blocks thereby forming a block chain.

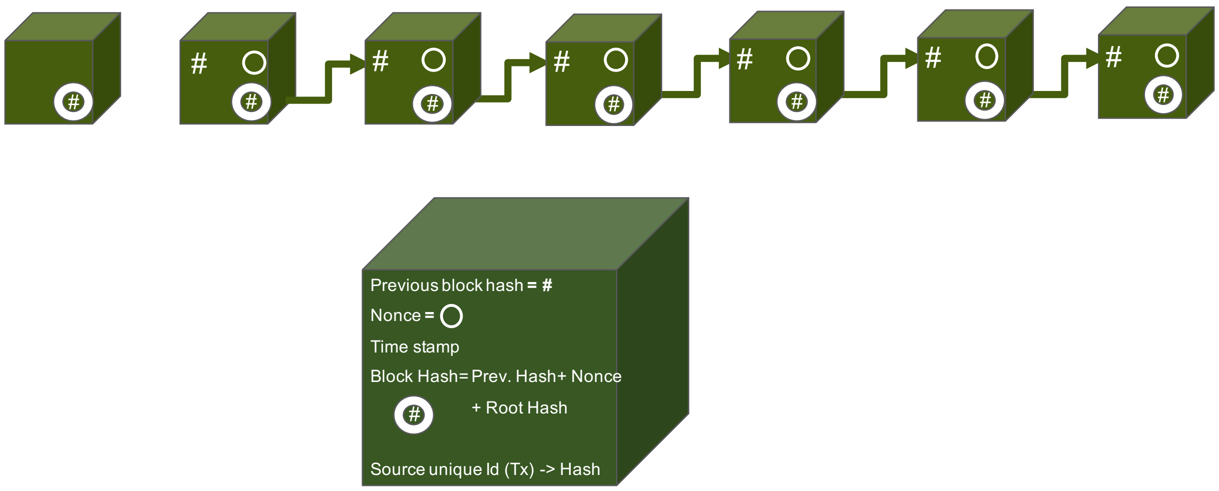


Figure 2.5 What is block chain.

Bitcoin which was the first application of block chain had made a significant breakthrough in cryptographic currency research by providing solution to long standing “Double spend “problem of digital cash. (Swan 2015). Prior to Bitcoin it was not possible to transfer digital assets online due to trust problem as all digital assets such as email attachments, photographs, could be downloaded number of times. There was a high possibility to spend digital assets twice. Therefore, while transferring, an intermediary third party such as PayPal or banks was always needed to ensure the trust. Third party ensured to keep the account when one user transferred the asset, it was deducted from his account and credited to the receiver’s account.

If the trust was outsourced to multiple parties to avoid dependency on one party then the challenge was the Byzantine General’s agreement problem (Canetti & Rabin 1998) where a multi parties having a need to agree on the battel field but having difficulty in making consensus due to adversaries in the group who participate in the agreement in a malicious way. Hence, Multi party trust mechanism to solve double spend problem never worked.

Bitcoin and block chain solved double spend problem by introducing the cryptography currency, online distributed shared ledger and consensus protocol (e.g. Proof of Work) where the consensus around the transactions is decided by members of community based on computational challenge and if majority agrees with the solution then a consensus is reached. One way to achieve this is to make the whole history of ledger available to the community. Block chain uses cryptography to secure the user privacy in publicly available ledger. (Nakamoto 2008)

Next section explains how does block chain work to ensure the security of transactions and confidentiality of the users.

2.3.2 How does block chain work

Block chain technology can be described as having four main components.

1. Digital currency
2. Cryptography hash based identities
3. The transaction ledger or the chain of transactions
4. Consensus Mechanism

Digital currency: Most implementation of Block chain use digital currency such as bitcoin, Ether, Lite Coin, XRP (Ripple n.d.; Litecoin n.d.; Ethereum 2017; Bitcoin n.d.). Currency is the center of the block chain as it is used to incentivize the consensus network. Currency is represented by set of strings in the ledger. In short, Digital currency is merely a transaction in the ledger. The transaction is identified by use of public key and private key.

Cryptography hash based identities: Each user owns public key and private key in block chain to ensure anonymity. While in public block chain public key is visible to everyone, it is possible to have different public key for each transaction. While sending a transaction private key is used to sign the transaction and public key address is used to send it. The role of public and private key enables strong privacy in different implementation of block chains.

Transaction Ledger: Transaction ledger is digital record of all transactions in the network and is immutable. Transactions are encrypted using the hash algorithm and creating hash of hash i.e. merkel tree. Once a certain size limit is reached a block is created. These blocks are then inter connected using cryptographic hash to enable robustness.

Consensus Mechanism: Consensus mechanism takes away the role of central authority in verification of transactions by reaching on consensus among the participating nodes, thus making the block chain decentralized. Consensus protocol was the main innovation from block chain, there are several implementations of consensus protocol exist today. Bitcoin block chain used Proof of Work consensus mechanism where all miners (members) participated to solve the mathematical puzzle and validating the transactions. Ethereum block chain uses proof of stake mechanism, where members can mine or validate the transactions according to their assets and stake in the currency. Consensus mechanism as the name suggests works on majority principle where longest block chain is considered as original. Addition of a block to a block chain is connected to majority of miners agreeing to the validity of the block.

Another component that is being used and introduced in IoT context is *smart contract, though it is* in niche market.

2.3.3 Elaborating the block chain process

When a transaction is initiated by one node or member the network members verify the transactions and based on majority when consensus is reached the transaction is approved. This network is called mining network ad members are called miners.

The transactions are permanently stored in the ledger and after a defined size limit a new block is created which is then connected to previous block, thereby creating an immutable block chain.

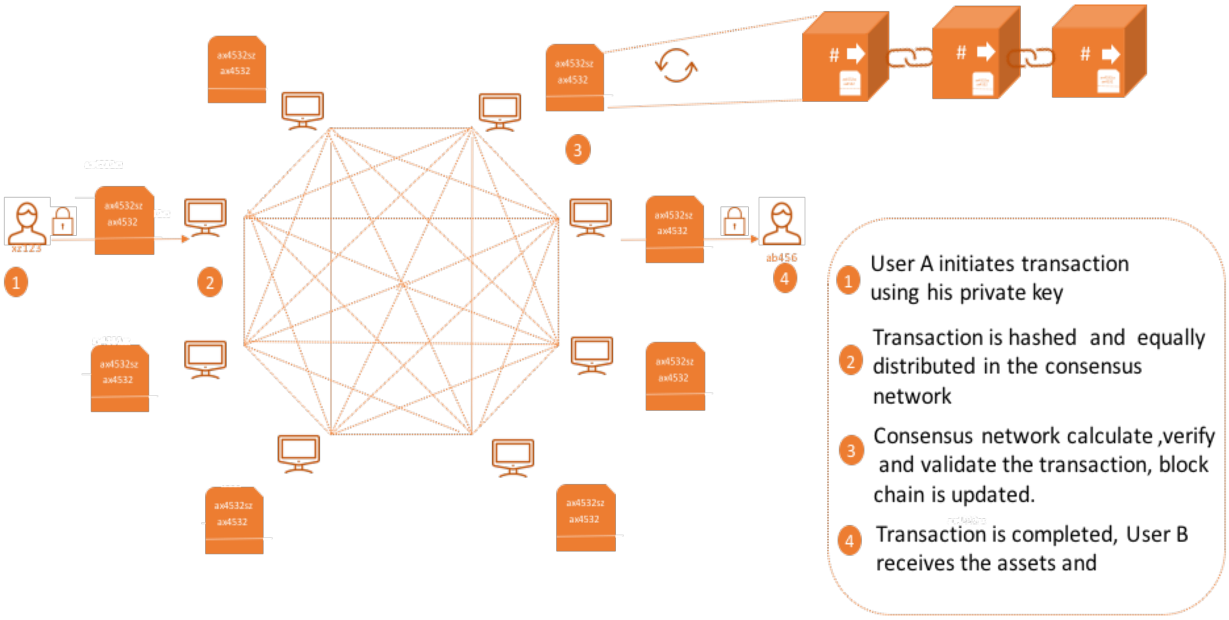

ax4532sz
ax4532
xz123
ab456
1
2
3
4
#
User A initiates transaction using his private key
Transaction is hashed and equally distributed in the consensus network
Consensus network calculate ,verify and validate the transaction, block chain is updated.
Transaction is completed, User B receives the assets and

Figure 2.6 visualization of the main steps in block chain transaction

The notion of block chain has been well received in the finance industry and lot of innovation and research is being conducted to spread the use of block chain in different industries. This implies that different types of block chains being used in different industries, however few block chains are widely deployed.

2.3.4 Types of Block chain

Based on four components described in section 2.3.2 there are several types of block chains however it can primarily be categorized in two types.

1. Public Block chains
2. Private Block chains

Public block chains: Bitcoin is the first example of public block chain. The main characteristics of public block chain is the availability of ledger. The digital ledger or database with list of all transactions since inception of the ledger is publicly available and visible to all participating members of the network. Anyone can view the ledger and modify it anywhere.

Public block chains are not controlled by anyone, hence require volunteers to secure the validity of transactions. Public block chains are completely open and transparent databases where everyone can submit transaction, contribute and participate in network security and privacy.

In connection to transparency, if there is no permission needed to be part of the network as miner the block chain is called as *permission-less* block chain. Similarly, if the network of miners is restricted to selected members it is considered as permissioned block chain.

Another level of abstraction is *public permissioned* block chain where the block chain is public and open to all however you need to be trusted to be part of the public network. There are several implementations however Ethereum block chain is famously known as public permissioned block chain.

Private Block Chains: Private block chains contrast with public block chains, differ in all characteristics. They are controlled by a central organization or company. The ledger is open to only those parts of the organization network. Complete history of the databases is not available to everyone, as it is controlled who can see the transactions or ledger. It can be argued if private block chains can be referred as new type of databases then block chains since they do not offer the flexibility. Most acknowledged benefit of private block chain is the immutable database and limited transparency between trusted parties. Though private block chains offer limited openness and flexibility to outside world, they can be very flexible within the network.

Private block chains are permissioned block chain as there are gatekeepers who control the accessibility of the block chain.
Example of private block chains are Ripple, Stellar and a recent one is Hyper ledger which is aiming to serve the private enterprises. (Schwartz et al. 2014)(Linux Foundation 2016)

2.5 IoT and Block Chain

Recent research shows a vast interest in block chain implementation in IoT, specifically in authentication, connectivity, access control, security, privacy, data storage and business models. However, the research has been on high level and implementation gaps have been underestimated. Which means that Block chain for IoT is still in its infancy phase.

Device authentication or identification in IoT is key to IoT success, as today there is no technology which can help securing identities of IoT devices however Block chain offers a promise. Block chain can be used to provide a platform to offer IoT device authentication there by identifying each device in the eco system. This will enable direct communication between devices and will prevent spoofing attack from adversaries with foul intentions. Device identification is an identified use case for block chain.
(Gaurav et al. 2015) in their research suggested that IoT devices shall need to be connected to cloud directly using HTTPS protocol and a basic prerequisite for this is the unique identification of each device, for which the researcher proposed block chain without going further in details. Though their research was not backed by any experiment and appeared as an idea only, during two years of development this seems much progress has been made and block chain for identification is being studied by many professional companies and academics.

Study by (Ouaddah et al. 2017) has described the challenges of IoT related to access control and have analyzed several existing solutions and technologies,

however challenge related to centralized vs distributed control remained as is. Authors have analyzed the distributed and centralized access control methods for access control and concluded that existing commonly used internet protocols cannot be applied in physical devices constrained environment. IoT needs to ensure end to end security, avoiding the risk of SPOF (Single point of failure), in addition to give control of user access data to user, reduce cost of expensive centralized management. Authors have not clearly provided a recommendation however suggested a future work on exploring the block chain to implement access control for IoT devices. This research will enhance the depth to evaluate the feasibility.
In a similar study authors (Dorri et al. 2016) investigated challenges of IoT specially in security and privacy area and implementation of block chain. Authors emphasizes the required solution to IoT security and privacy issues is a technology which is decentralized, distributed, ensure user/device anonymity, privacy and security over untrusted party.

Authors further explain the challenges with using block chain on high latency, too much consumption of computing power and resources, additional overhead traffic and scaling issues to name a few. Authors propose an architecture which is based on local block chain, local storage, access and policies however authors did not explore different types of block chains in the research and clarify the exact IoT challenge and mitigation. While the proposal includes a future study, there are open questions regarding the proof of work protocol robustness. The study didn’t analyze the different consensus mechanisms and their characteristics.

In another recent study (Dorri et al. 2017) authors propose a block chain based architecture for automotive industry use case, where block chain based overlay network OBM (Overlay Block Manager) and LBM (Local Block Manager) have been introduced. While study brought forward an interesting point regarding use of block chains as access control using public block chain, and transaction control using local (Private) block chain, authors do not specify the latency demands, and how they plan to overcome SPOF (Single Point of Failure) in LBM.

Referring to the study by (Bröring et al. n.d.) it is evident that IoT needs an interoperable eco system and hence there is an initiative started in EU with name BigIoT, the project is in infancy phase and has acknowledged the problem with the commitment to find a solution. Project hasn’t come up with the solution proposal yet.

On the critical side (Huberman 2016) analyzed the role of trusted third parties and also block chain in making Industrial IoT a success. Author has been critical of using block chain for IoT and suggested third method as zero knowledge technique where devices can still communicate without information on the data being collected by them. The study describes the concept on a high level without going into the details of implementation.

In a systematic literature review (Conoscenti et al. 2016) analyzed IoT use cases and bit coin block chain to enable the use cases. The study concluded that while bitcoin block chain is most secure and private, there are scalability issues, furthermore study concludes that public block chain only guarantees pseudonymity and fully anonymity is not assured. This is due to public key traceability and openness of ledger to all participating node. The conclusion validates the thesis assumption that public block chain in its current form cannot be a solution for IoT security and privacy issues.

Block chain in IoT has been mostly implemented using the smart contracts, according to Nick Szabo is defined as "a computerized transaction protocol that executes the terms of a contract". (Szabo 1994). In the block chain context, smart contracts can be defined as scripts of programs (algorithms) with unique address on the block chain. Smart contract is triggered by addressing a transaction to it and then it executes independently according to the data included in addressing the transaction. Smart contracts are considered to be a vital component in Internet of Things where devices can communicate without trust and in an automated manner.

Research by Christidis and Devetsikiotis (Christidis & Devetsikiotis 2016) identified use cases where IoT devices interact using smart contracts on block chain, providing security, transparency, decentralization and automation between the devices. Though the research concludes the significance of using block chain for IoT, and describes few concrete use cases, it only remains focused on theoretical level without going into details of specific block chains and its characteristics.

The literature review illustrates that block chain technology is being considered as an option to address IoT privacy and security problems and academic research is accelerating in this area. The research however is either on a high level very high level or on a very use case specific. There is a gap when it comes to critical analysis of block chains and addressing IoT security and privacy on a eco system level.

3. Methodology

3.1 Research Paradigm

A research paradigm is the structure which guides the research based on researcher's philosophical beliefs. This research is based on interpretivism paradigm which suggests that social reality is highly subjective because it is formed by our perceptions. (Creswell 2007)

3.2 Research Approach

Two main approaches which relate to research paradigms are quantitative approach associated with positivism and qualitative approach associated with interpretivism paradigm. While quantitative approach examines data from numerical perspective qualitative approach interprets data from nominal perspective. (Smith 1983)

Unlike the positivist paradigm approach this study will be qualitative and will seek to describe block chain technologies and its relation to IoT. The data collection was focused on high quality sources.

There exist two methods based on the logic of the research, Inductive and deductive methods. While inductive method describes generalization of the subject from specified, deductive method on the other hand focuses on specific subject from generalization. This research follows a deductive method by moving from general block chain technologies to specific types of block chains in IoT Security & Privacy context.

3.3 Collection of data

The data was collected through multiple sources and the unit of analysis was block chain industry experts. Focus was on working professionals who are working on block chain based products in technology segment. Three different segments were chosen, expert from financial implementation of block chain, experts from technology implementation of block chain and expert on privacy and security.

Collis and Hussey define primary data as the data which is generated from original sources and secondary data as data collected from existing sources. For this research, Primary data has been collected in the form of interviews and secondary data was collected via online search and references. (Collis & Hussey 2014)

3.3.1 Primary data

Empirical data was collected via iterative semi structured interviews, with different experts. Total 5 Interviews were conducted. The interview process entailed general introduction to the topic and information regarding anonymity where interviewees were informed about anonymity and privacy of information. Interviews were mix of formal and informal and with some experts was about testing the hypothesis and validity of the concept. Interviews were prescheduled and timed. While a list of questions was designed, interviews were kept flexible and allowed divergence from the exact question in the subject. Block chain is fairly new to IoT and there are many implementations possible hence fair amount of time was spent on understanding initial details of public block chain and private block chains.
Interviews were conducted in person, and on skype where personal meeting couldn't be arranged due to distance and time constraint. Notes were made during the interviews which were transcribed further.

The profile of interviewees included Business developer and co-founder of a block chain based start-up, Technical product manager working with block chain based product implementation and development in a large company, a senior expert researcher in research department of a large company who is designing a breakthrough product in block chain, an expert in block chain in the research department of a large company, and finally an expert in product privacy and general privacy in a large company. Privacy expert was interviewed to test the validity of the problem with security and privacy.

Interviewees were selected from different industries and from different projects those in same industry. Selective approach was taken in determining the interviewees, papers were read, references checked, and related work was identified. This was to ensure right competence, relevance and high quality of knowledge in the response. Interviewees were contacted in person or mail by the

researcher and some references were taken from academics to approach the interviewees. The duration of interviews was 60 Mins and questions served as guidance rather than strict time adherence and linear path on completion of set of questions. This allowed extra flow of information and few iterations were done with the interviewees on different days to get more details on the subject. While researching on a privacy topic, to respect the privacy, no interviews were taped or recorded, still notes were made and transcribed to capture the learnings.
Primary data helped in testing the initial hypothesis and pivoting into a new concept while maintaining originality of the solution.

3.3.2 Secondary data

As a compliment to primary data extensive search was performed to collect secondary data from various sources such as Science Direct, KTH library, IEE Xplorer, and google scholar and many other science journals. Block chain is rather new technology hence many thesis projects were analyzed too. Secondary data resulted in collection of around 300 papers based on defined strings.

3.4 Ethics and Sustainability

Ethical considerations were taken into account while conducting the research. Anonymity of the interviewees has been maintained. The contribution of interviewees has been acknowledged. Interviews were transcribed on notes.

Sustainability is defined as separating the needs of present generation from the future generation. (Kuhlman & Farrington 2010). Sustainability is about ensuring no compromises are made for a sustainable future while creating the present (Brundtland 1987). The research on block chain and addressing IoT privacy and security problem is addressing the sustainability to create a safe secure and sustainable future.
Interviewees were very keen in contributing towards the development of the technology there by contributing towards sustainability of the future.

Block chain technology is enabling the much needed eco system and disrupting different industries, the research is aiming to explore the disruption of finance industry to solve a long-standing problem of IoT, thereby contributing towards sustainability.

4. Findings and Discussions

Following section presents the discussions with interviewees and key findings. First section describes the difference between different types of ledgers which was result of the discussion with interviewee.

4.1 Transaction Ledger vs Information Ledger

Current block chain implementation do not differentiate between ledger and define it as digital ledger however one of the finding from the study is to differentiate the ledgers in two types, especially in IoT context. IoT devices may execute transactions with exchange of direct value, however devices may also exchange an indirect value such as information. An example could be the temperature sensor in a green house or apartment, the exchange of temperature data has an indirect value and can be categorized as information. Therefore, Block chain ledgers in IoT context can be categorized as two types, *transaction ledger* and *information ledger*.

Since transaction ledgers are of more importance due to direct value being involved, they have high involvement of miners and consensus network, therefore the validation of transactions precedes over execution speed of transactions. More miners mean better validity but slower execution. On the other hand, information ledgers have indirect value can have a mix of autonomous miners and can be faster as speed takes priority.

In one of the interview with the block chain industry expert when discussing the speed of public block chains, it was reported that the assumptions being made in the study (e.g. public block chains are slow) needs to be further detailed, as there are different public block chains based on different consensus mechanisms. An example is the Ethereum block chain which is faster than Bitcoin block chain. (Ethereum 2017)

Related to IoT privacy the discussion was to also determine “what type of information are we planning to store in block chain. How much information you are using on the protocol, how are we going to use the information, why shall we put this information in the ledgers.”

Third point was the security of consensus networks which work on domain level, in bit coin we need 51% of consensus before a transaction is approved, there are policies defined to choose the which domain will be chosen. Policies define the mining.
There were some risks associated with block chain when it comes to long range attack (Vitalik Buterin 2014) for proof of work consensus method. If a transaction is approved and a block is created, there may be an adversary interested in faking the chain, can create another parallel block, and depending on consensus he may be able to create a parallel chain and alter the original amount of money which was there in current structure.

Since consensus and proof of work requires computing power and there is chance that large centers hosting Proof of Work, producing large amount of consensus may influence hacking. This limitation is known and there is ongoing work to address this by bitcoin community.

One aspect of using block chain for privacy was, that public block chain by nature is transparent and all transactions and ledgers is available to all in the network, moreover these records are immutable. The way the information is encrypted is with the use of public and private key. There is a need to consider privacy aspect if due to any reason private key is hacked then the information gets hacked then it ll be open to everyone. At least in traditional ledgers information expire based on time, but in block chain the information stays forever. Data retention is a privacy requirement according to new general data protection regulation in EU, how is block chain going to deal with that.

When it comes to use of hybrid block chain, the study proposed to separate the consensus protocol (Proof of Work and Proof of Stake) of block chain and replace it with Distributed Autonomous Corporations (DACs) and during the discussion with the interviewee following questions were raised such as owner of distributed automatic consensus, who is going to run that, what services are going to be run on that. What is recommendation of the study with regards to communication with the external ledger. Different miners communicate with ledgers in different protocols, what will be default choice of the protocol.

It was also discovered that industry has many different implementations of hybrid block chains hence there is a need to have a unified approach.

While discussing the hybrid block chain it was identified that a hybrid block chain with DACs concept may be helpful in accelerating the eco system of creating standards and block chain based companies. It is important to choose what consensus method will be hybrid (Proof of work or Proof of stake or an alternate method).

The questions raised were further validated with secondary data and the method was refined based on learnings.

Another interview was with the business developer of a block chain based company. The interviewee has been working Bitcoin since 2011 and currently working as business developer and considered a (Block chain/ bit coin expert) in Stockholm.

His definition of public block chain is connected to bit coin which has been in existence for 8 years, most trusted, most valuable theoretical perspective. Bit coin is about establishing consensus on who has both money and asset in a way you don’t need any third party.
Block chain as technology has several unique aspects like cryptographic hash (fingerprint of data), (Hash of hash) (Nakamoto 2008), merkel tree (Denning 1984), public and private key and Private key and more over distributed consensus method. Biggest innovation from bit coin was the solution of double spent problem on the internet which was solved with proof of work. However, the interviewee also brought in the limitation with the protocol around the long-range attack.

On the private block chain, there are different implementations and one of them is the signature scheme. This is used as alternate to proof of work where if majority of static member sign the transaction, it gets validated. The risk with this is also the long-range attack (Vitalik Buterin 2014) where members can be allured into making fake record.

Interviewee suggested that bitcoin is the most secure block chain and the consensus method of bitcoin may be used to avoid the long-range attack issue. Private block chains are least secure and prone to long range attack however they are safer that a normal database.

There are pros and cons with public and private block chains, while public block chains are more secure due to large consensus network, the private block chains are more privacy aware as they can decide the authority of who can view the transaction or the data.

He further elaborated that block chain is not meant for storing the data it is there to maintain the transactions record of the data. To address the privacy issue one way is to encrypt the data, store the record in block chain and keep the data on a cloud. However, there are not many solutions addressing the privacy concerns in this way.

Another interviewee stated that there is a trust anchor when it comes to block chains, IoT devices use the public block chain then it is completely decentralized where better scalability is guaranteed however privacy and performance may be compromised.

There was a consensus among interviewees that block chain is a good solution to IoT privacy and security as it offers identity, immutability of records and secure transactions thereby giving control to user. However current implementations of block chains need to be evaluated to understand which implementation can serve the need of IoT security and Privacy.

Based on the above discussions and interviews more secondary data was collected and analyzed and next step came as analyzing different block chains and their characteristics to evaluate which block chain is useful for IoT security and privacy.

There are different implementations of the block chain in the industry today, some are public and some are private. Every block chain is unique in one way and to evaluate the needs of IoT the characteristics, block chain parameters were analyzed.

4.2 Comparison of different block chain characteristics in IoT Context

While many variants of block chains exist today, an analysis has been done of major block chain characteristics to evaluate which block chains can be suitable for IoT and why.

Bitcoin, Ethereum, and lite coin have implemented PoW (Proof of Work) consensus mechanism, Hyper ledger implements a pluggable consensus framework however currently supports PBFT (Practical Byzantine Fault Tolerance) protocol. Stellar on the other hand developed its own consensus mechanism. Ripple block chain has developed a variant of PoS (Proof of Stake) protocol .

One of the main important characteristics for IoT is the latency, which is speed of executing transaction. The requirements from connected cars, connected oven,

connected light, is that the transaction on the network shall take Mili seconds which is very far from the objective today if certain block chain is to be used with exception of Hyper ledger block chain which is permissioned (Private) block chain.
The table shows different consensus mechanisms used in the block chains.

Block chain / Characteristics	Bitcoin	Litecoin	Ethereum	Ripple	Stellar	Hyper ledger
Consensus Mechanism	Proof of Work	Proof of Work	Proof of Work	Distributed (PoS)	Distributed	Pluggable Consensus Framework (PBFT)
Latency	10 Mins	2.5 Minutes	12 Seconds	3 Seconds	2-5 Seconds	< 1 MS*
Currency	BTC	LTC	ETH	XRP	Lumens	No
Decentralized Control	Yes	Yes	Yes	No	No	No
Transaction Confidentiality	No	No	Smart Contract Level	No	Smart Contract Level	Smart Contract Level

Figure 4.1 Comparison of different block chains in IoT context (Richard 2016)

Among other characteristics compared were decentralization and confidentiality which are another important factor for IoT security and privacy.
Above comparison depicts different challenges in current block chain implementation.

4.3 Challenges with use of current block chains (Public & Private) in IoT

Latency: A key factor in success of IoT is the latency for the time critical applications or devices. Public block chains when compared show high latency.
A comparison shown in figure 4.1 depicts that public block chains Bitcoin, Lite Coin and Ethereum have varying latency from 12 seconds to 10 minutes which may not be efficient for a *time critical IoT device* that is transferring critical data to a remote center. One can question if miners use high capacity mining machines then what could be the reason of slow consensus. The reason being the way consensus is built, as consensus is verified by first miner, followed by endorsement from another and in continuation, that causes slow speed.
Analyzing Private block chains such as Ripple, Stellar and Hyper ledger, it can be comprehended that private block chains as well have varying latency however are faster as compared to public block chains, mainly due to smaller network and due to different consensus mechanism used. Particularly, the latest block chain project “Hyper Ledger” is fastest and can come closer to solve IoT latency requirements.

Scalability: Decentralization in public block chain entails expandable network of nodes or miner. Expansion comes with challenges in throughput and latency as the throughput slows down and latency increases. Block chain illustrated that it is scalable however scalability comes with a cost of increasing latency and decreasing throughput. IoT needs a scalable solution to cater needs of billions of devices and transactions. Depending on consensus mechanism used scalability is directly affected.

Security issues with decentralized control: Though public block chains offer decentralized control, there are challenges associated which could be exemplified as security attacks. As described earlier, public block chains are permission less and anyone is allowed to join the network as a miner and validate the transaction. One of the consensus method "Proof of Work" consensus protocol works based on 51% consensus. Which means in order to hack the block chain one needs to have control of 51% of total computing power of the network. Though it is difficult to achieve this number in widely used public block chains (Bitcoin and Ethereum) however it is not impossible. It can be assumed that new public block chains are more vulnerable to such attacks since no one is aware of who is participating in validation process. An adversary can easily employ more than 51% computational resources and own the block chain. The logic of consensus protocol is hard coded according to the rules. There are very subtle connections between those solutions of proof of work, that are needed since there is no organized governance. It is realized by majority of miners endorsing the work (Validation).

Though there are improvements being made still the protocol is not full proof. One more issue related to PoW method is waste of computational resources, where the participating nodes are competing to solve the validation challenge. Even if first miner validates the transaction, whole network has to validate the transaction to continue in mining process. This results in waste of computational resources. Thus, public ledgers can be considered as slow with need of substantial computational power.

Another consensus protocol that is considered as replacement of PoW is Proof of stake protocol where a miner is allowed to participate in the mining process according to his stake in the digital currency. As an example, if one has 1% stake in the digital currency he is allowed to mine 1% of the transactions. This protocol also has a security flaw which is known as "Nothing at stake". The miners have possibility to participate in all block chains (Real and fake) as they have nothing to lose and hence if majority of miners participate in all block chains then due to adversary's own stake fake in block chain the fake block chain will be considered as real and adversaries can take control of the block chain. This event is rare though however cannot be ignored. There is significant research being done to find a solution to such problem. The positive aspect of PoS is that to attack the whole block chain one has to put 51% stake in it which doesn't offer any monetary benefit and hence no motivation. In IoT context this may change. IoT security critical devices may benefit from not using the new public block chains and may use large public block chains with some risk awareness.

Watnabe (Watanabe et al. 2016) described the short coming of proof of stake protocol where it could be prone to deterrent attack in the event of collapse in coin value. Authors claim that an alternate method may be a better choice in smart contracts where coins have no value. Authors presented an alternate hybrid block chain mechanism which builds the consensus mechanism on credibility score and proof of stake.

The work proposed by authors is to specially enhance the robustness of proof of stake method against the security lapses in consensus protocol. The authors have only shown initial work and future elaboration on how it will work in crypto currency is part of future work. Furthermore, they have not specified anything about public and private block chain.

Confidentiality & Privacy: Another issue in public block chains is the confidentiality and privacy. Even though anonymity is maintained in the networks by using the public key, due to open distribution of the ledger everyone has visibility of all transactions. Thus, there is a chance to trace the transactions if same public key is used. Once connected to the block chain explorer, one can check all the history about all transactions and it is possible to connected the identity to the user. To avoid this problem some block chains, offer different public key for each transaction. However, there may be associated risks to be traced. An example can be a list of transactions, and if the pattern is repeated then it is possible to get all history of transactions.

Private permissioned block chains do not have this problem due to control on accessibility of ledger and participating miners. In IoT security and privacy context it is essential that privacy critical devices do not use public block chain.

4.2 Analysis of ongoing initiatives

Hyper ledger fabric block chain: Hyper ledger fabric (Linux Foundation 2016) is the latest implemented block chain intentioned at creating an open source block chain to be used by enterprises to solve different industrial problems.
Hyper ledger has very low latency, works on PFBT (Practical Byzantine Fault Tolerance) consensus protocol and is supported by a community of companies.
Hyper ledger has deployed a permissioned block chain where membership of miners is restricted to trusted parties, giving it faster speed, and confidentiality of transaction. It is worth mentioning that Hyper ledger doesn’t use any cryptocurrency such as coins, since it is totally permissioned and aimed at enterprises.
One can claim that Hyper ledger is current best implementation of block chain that can address the security and privacy issues of IoT, primarily due to its characteristics. (Tuan et al. 2017)
One argument to above statement could be the control and transparency which is limited due to only certain members are allowed to participate.

Federation of block chains: Another initiative is driven by a block chain company called Blockstream, where a federation of block chains is proposed as a solution to high latency of public block chains and specifically in Proof of Work consensus mechanism.(Dilley et al. 2016). The research proposed a concept of side chains to offload the main block chain. Side chains is a promising concept where a transaction is initiated on main block chain and transferred to a side chain which ideally is meant to be smaller. Due to its smaller size of mining network side chain is faster and has high through put and low latency coupled with high security. It

does come with implementation challenges though where an HSM (High security Module) module is needed to implement a side a chain. This module is an extra hardware which may be a costly affair for wide deployment of this chain.
Current working deployment of federation of block chain is Liquid which is mainly focusing on financial and other use cases than IoT(Dilley et al. 2016).

4.4 Different purpose of block chain in IoT

Block chains have properties which could be fit to purpose depending on the use cases. These properties could be classified in three categories and are dependent on the type of consensus protocol a block chain is using.

These properties are

1. **Scalability**: Defined as size of the block chain and number of users.
2. **Performance**: Defined as high speed, and low latency
3. **Availability**: Defined as transparency of information, availability and access to the ledger.

It is assumed to be difficult to get all three properties optimized.

Scalability is achieved by de-centralizing the block chain as centralizing the block chain doesn’t scale. Referring to the example of bit coin block chain which is decentralized, it is difficult for any private (centralized) block chain to achieve the similar scale as bitcoin.

Performance is achieved by centralizing the block chain, by making it limited and smaller as decentralization affects the performance in terms of latency.

Availability is achieved by distributing copies of ledger to the whole network and creating millions of databases which affects the performance.

Referring to an example of supply chain logistics where block chain can be used in supply chain to enable faster and secure transactions and where trust and transparency is of utmost importance we may need to use public block chain for consensus mechanism since it is perceived as more available and trust worthy. Performance takes second priority.

There are different sizes, needs for a block chain depending on the use case, even in IoT as logistic industry is going to be automated.(Christidis & Devetsikiotis 2016), Similarly, for time critical IoT devices, speed is the main issue, If there is an open/public block chain that everybody trusts, then its slow. If IoT uses a private block chain then it is faster however has less credibility and doesn’t address centralization problem. It can be argued if one size fits all.

There was a consensus with three interviewees that speed problem of block chains is connected to consensus and need to be addressed for IoT.

Block chain has business logic and decision logic, separating the logics of block chains could be one way to gain the latency for IoT.

The points of separating business and decision logic of block chain is that technically it may not provide the solution to speed, which raises a question on how to configure the efficient solution. The answer could be that different IoT applications have different needs when it comes to time critical applications, privacy critical applications and control critical applications. Consensus mechanism could be tailored for specifics domains of use, rather than relying on one size fits all.

Much research is going on consensus mechanism and the conclusion is that it is not easily accessible and possible to find a solution to BFT problem(Seibold & Samman 2016).

4.5 Hybrid Block Chain

Hybrid block chain is a concept proposal from this research. Hybrid block chain relies on componentization of block chain where four components of block chain are separated from each other. Specifically, consensus mechanism is separated from the block chain and is made flexible to support different needs of IoT applications based on their property. Scalability, performance and availability (Transparency).

Hybrid block chain can be described as a consensus method which is automated with help from Decentralized Autonomous Organizations (DAO) and Distributed Autonomous Corporations (DAC) (Svensson & Leung 2015) to address IoT's latency problems.

Looking at the figure 4.2, it can be assumed that different IoT devices or applications have different needs of latency. Similarly, they have different needs of privacy and control (Decentralization). One application in the smart home doesn't need to compromise on privacy due to latency need of other application in the smart home.

On the other hand, different devices shall not be on different block chains or platforms, in that case IoT interoperability problem will remain unaddressed.

IoT Interoperability problem can be solved by on boarding each IoT to device to a block chain and providing the devices public and private key i.e. unique identity. That means by having a distributed ledger and cryptographic identities where each and every device will have a block chain based identity, IoT interoperability problem can be addressed, which in turn will address IoT security, privacy.

There has been some research in this area (Fromknecht et al. 2014; Axon 2015; Conoscenti et al. 2016) also from hyper ledger block chain (Linux Foundation 2016) there are proposals to use block chain for identity management.

However, the problem with different needs of latency and decentralization can be addressed using a specific version of block chain, called Hybrid block chain.

In a simplified way Hybrid block chain is a mix of consensus system where different consensus mechanism can be chosen based on a Policy (Zyskind, Nathan & A. S.

Pentland 2015). Policy will have dynamic consensus mechanism allocation calibrated to cater need of each application.

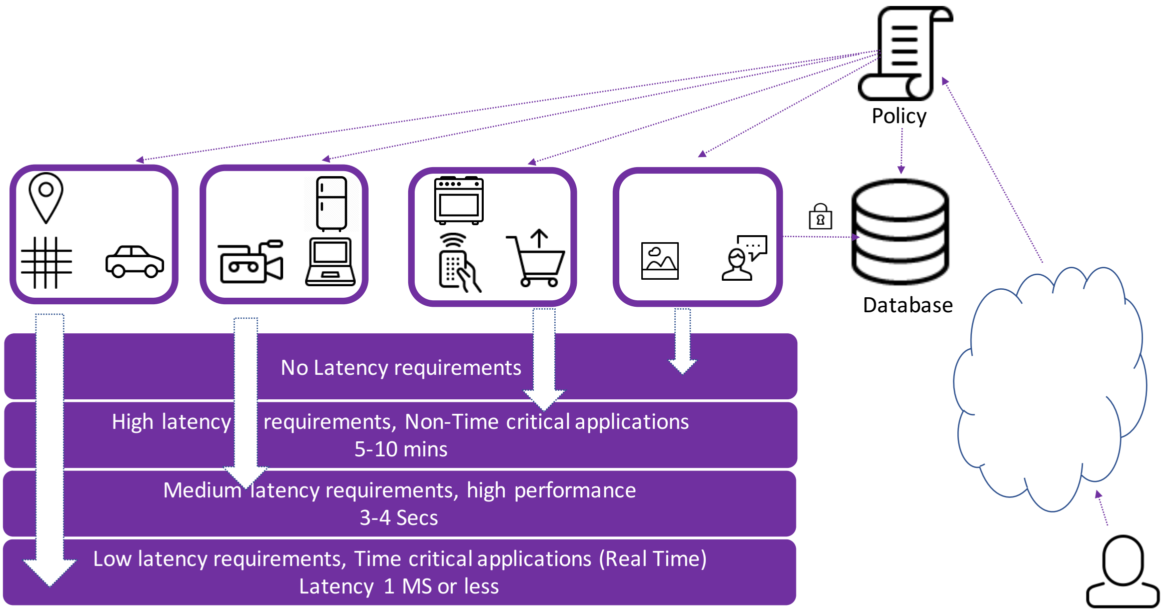

Policy
Database
No Latency requirements
High latency requirements, Non-Time critical applications
5-10 mins
Medium latency requirements, high performance
3-4 Secs
Low latency requirements, Time critical applications (Real Time)
Latency 1 MS or less

Figure 4.2 Latency needs of Different IoT devices

IoT device user connects to IoT device using internet or cloud connectivity and based on latency, control and privacy need, a consensus mechanism can be chosen. There is a provision of local database in order to have extra privacy control on the device data.

The ledger, Identity management remains same however consensus component is separated as a logic to provide flexibility. It can be argued if Hybrid block chain is feasible and scalable.

4.6 Hybrid Block chain feasibility and scaling

Referring to Hyper ledger which has chosen a PFBT consensus mechanism and aimed to have pluggable consensus (Linux Foundation 2016) it can be safely assumed that Hybrid block chain is feasible and it is possible to separate the consensus mechanism from block chain to cater needs of different applications (Swanson 2015). Currently Hyper ledger is working in this direction and implementation of the concept is still to be seen. The role DAO and DAC can be used to implement different consensus mechanism to serve different block chains. In case a connected car needs a low latency consensus, based on policy query output the transaction will be diverted to low latency Hyper ledger block chain. Similarly, for temperature sensor where the transaction can be forwarded to Ethereum block chain or PoW consensus mechanism. Using the public block chain consensus may give the needed scale to this IoT application.

It is assumed that conceptually hybrid block chain is feasible and can scale. There may be few implementation related limitations in the concept though that need to be further elaborated.

5. Conclusions

5.1 Conclusions

This final section describes insights and conclusions on what new possibilities may open with marriage of two great technologies. How a disruptive innovation in one sector can disrupt another technology sector. We conducted a Review to investigate which are the uses cases of the block chain can be implemented in IoT to benefit from its secure technology. The objective of research was to leverage the block chain for a private-distributed IoT where data produced by devices are not kept in centralized companies.

We have concluded that block chain has a definite role in IoT security and privacy as the requirements from IoT and characteristics of block chain technology have a clear match. However, Block chain technology comes in different deployment options, such as public block chain, private block chains.

We have discussed different types of block chains and have identified that current block chains have limitations in terms of standardizing the IoT eco systems. Public block chains have very high latency and private block chain are not scalable enough to cover the eco system as there will be different implementations from different suppliers.

We explored a concept of a hybrid block chain where the decision logic or consensus mechanism has been separated from the block chain. Essentially, to cater the latency demands of IoT time critical applications there is a need to employ high processing and execution capacity compute systems. These systems are separately managed by professional organizations or (DAO) which provide high availability and offer high speed. Instead of receiving the reward unlike in Proof of work and prof of stake, these organizations offer consensus as a service for different block chains. For the non-time, critical application consensus as a service can also use public miners as shared computing resources. This means that consensus mechanism can be a mix of private and public computing resources.

Finally, we have looked at feasibility and provided an example of hyper ledger block chain supported by a use case that hybrid block chain is feasible and can scale.

Consensus as a service concept is powerful in a way as it can be offered to different applications being run on different block chains. There are type of IoT applications which needs time critical consensus with extreme low latency and there are applications which need consensus with high trust and latency can be higher as well. Different IoT use cases will benefit from different consensus.

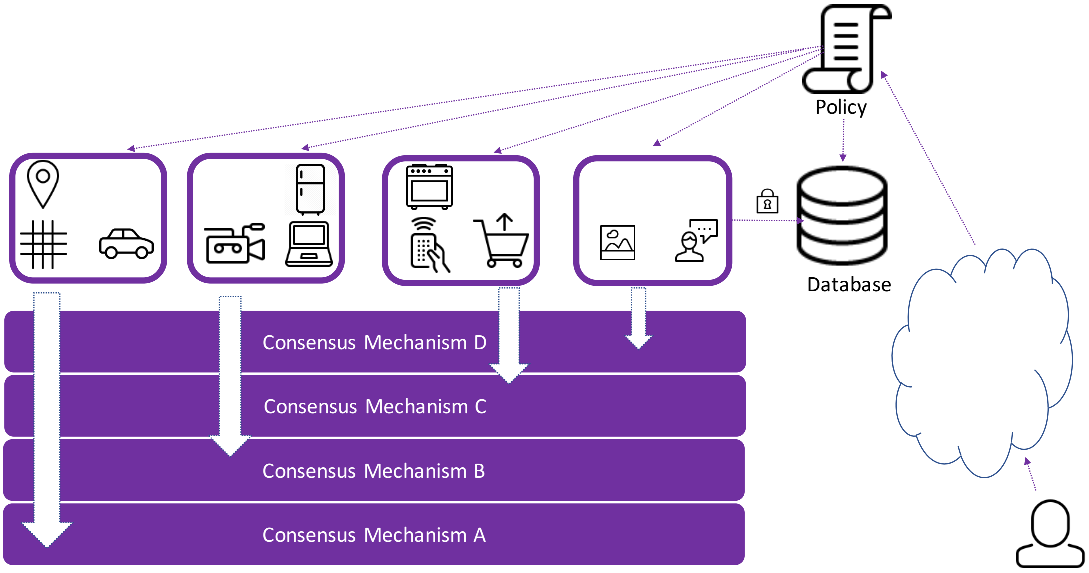


Figure 5.1 Hybrid Block Chain

In addition to high computing power there will be a need to modifying the rules of the consensus protocol, which is outside the scope of this thesis.

Hybrid block chain will ensure the data integrity when it comes to privacy as the control of data will remain in the user's authority since he holds the private key to his data. Related to security the data is immutable and verified by many nodes in parallel. Adversary will have to initiate attack on many systems at the same time to bring down the system or to steal the information.

5.2 Block chain and Business Model Innovation

The research has proposed a mechanism to separate the three-different part of the block chain. This brings enormous possibility in opening new businesses and new business models. One such business model can be "Consensus As a Service" CaaS (Swanson 2015). Together with Decentralized Autonomous Center there can be different organizations which can outsource their services to gain efficiency. The business model innovation need to be studied further as part of future work.

5.3 Limitations

Methodological limitations of the research must be acknowledged. Among few weaknesses one of the major weakness was finding academic experts due to short duration of the study. In addition, Industry experts Interviews were scheduled and sometimes moved which made it difficult to get lot of sampling to get larger primary data.
Due to block chain technology hype, it was very difficult to find reliable sources (research based) of secondary data online. There is a race in the industry to be first in block chain and volumes of papers or blogs or article are being written which made it a tedious task to identify reliable sources to validate.

Another aspect was the cognitive biases of researcher and the interviewees, even though researcher tried his best to keep away from confirmation bias, there may be some kind of influence. On the knowledge bias side, interviewees had share info as per their knowledge of block chain implementation and experience and some results may have been influenced by knowledge bias.

As the interpretivism paradigm results into high validity and low reliability of results, if the interviews are conducted again, there is a slight chance that result will differ. However, for this research, it may be due to knowledge bias, but researcher has ensured the high reliability despite of interpretivism paradigm.

6. Future Research

Study has concluded that combination of different block chain properties can help to address IoT's latency, privacy and security problems among many. However, concept of Hybrid block chain needs to be further detailed towards implementation. Future research is needed on implementation of hybrid block chain to overcome IoT and public ledger speed challenges.

The research has highlighted differentiation of ledgers, a future research on categorizing different IoT applications into different ledgers will help in scaling issue of IoT.

Current research has proposed a possibility of new business model innovation without going into details, future research shall cover business model innovation of consensus as a services and technical implementation of consensus protocol for hybrid block chain.

7. References

Axon, L., 2015. *Privacy-awareness in Blockchain-based PKI*.

Bitcoin, Bitcoin - Open source P2P money. Available at: https://bitcoin.org/en/ [Accessed June 9, 2017].

Bosch, Bosch IoT Suite. Available at: https://www.bosch-iot-suite.com/ [Accessed June 6, 2017].

Bröring, A. et al., Enabling IoT Ecosystems through Platform Interoperability The Problem of Missing IoT Interoperability.

Bröring, A. & Mitic, J., 2017. index @ big-iot.eu. Available at: http://big-iot.eu/.

Brundtland, G.H., 1987. Our Common Future: Report of the World Commission on Environment and Development. *United Nations Commission*, 4(1), p.300.

Catalini, C. & Tucker, C., 2016. Seeding the Technology S-Curve ? The Role of Early Adopters in Technology Diffusion.

cb insight, 2016. Banking Is Only The Start: 20 Big Industries Blockchain Tech Could Disrupt. *cb insight*. Available at: https://www.cbinsights.com/blog/industries-disrupted-blockchain/ [Accessed June 4, 2017].

Christensen, C.M. & Overdorf, M., 2000. Meeting the challenge of disruptive change. *Harvard Business Review*, 78(2).

Christidis, K. & Devetsikiotis, M., 2016. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, 4, pp.2292–2303.

Collis, J. & Hussey, R., 2014. *Business Research*, Plagrave Macmillan Higher

Education.

Conoscenti, M., Vetro, A. & De Martin, J.C., 2016. Blockchain for the Internet of Things: a Systematic. , (November).

Creswell, J.W., 2007. Research Design: Qualitative, Quantitative and Mixed Method Aproaches. *SAGE Publications*, pp.203–223. Available at: http://libproxy.unm.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=51827937&site=eds-live&scope=site%5Cnhttp://content.ebscohost.com.libproxy.unm.edu/ContentServer.asp?T=P&P=AN&K=51827937&S=R&D=a9h&EbscoContent=dGJyMNLr40Seprl4.

Dahmén, E., 1989. `Development Blocks' in Industrial Economics. In B. Carlsson, ed. *Industrial Dynamics: Technological, Organizational, and Structural Changes in Industries and Firms*. Dordrecht: Springer Netherlands, pp. 109–121. Available at: http://dx.doi.org/10.1007/978-94-009-1075-1_5.

Denning, D.E., 1984. Digital Signatures with RSA and Other Public-Key Cryptosystems. *Communications of the ACM*, 27(4), pp.388–392.

Dilley, J. et al., 2016. Strong Federations: An Interoperable Blockchain Solution to Centralized Third Party Risks. Available at: http://arxiv.org/abs/1612.05491.

Dorri, A. et al., 2017. BlockChain: A distributed solution to automotive security and privacy. Available at: http://arxiv.org/abs/1704.00073.

Dorri, A., Kanhere, S.S. & Jurdak, R., 2016. Blockchain in internet of things: Challenges and Solutions. *arXiv:1608.05187 [cs]*. Available at: http://arxiv.org/abs/1608.05187%5Cnhttp://www.arxiv.org/pdf/1608.05187.pdf.

Drucker, F., P., 1985. *Innovation and entrepreneurship.*, New york: Harper & Row.

Enwick, M.A.R.K.F., Aal, W.U.L.F.A.K. & Ermeulen, E.R.I.K.P.M. V, 2017. *Legal education in the blockchain revolution m*,

Ericsson, IoT Accelerator Platform | Ericsson. Available at: https://www.ericsson.com/en/internet-of-things/iot-platform?gclid=Cj0KCQjwpdnJBRC4ARIsAHC6k2IxJ58oXbvZhHMiYgBQNJfpT4T4zvKia2WHGwHWS9zuzgSoh2r-YlcaAqXBEALw_wcB [Accessed June 6, 2017].

Ericsson, 2016. Mobility Report. , (November), pp.7–8. Available at: https://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf.

Ethereum, 2017. Ethereum Project. *Ethereum.org*. Available at: ethereum.org [Accessed June 9, 2017].

Everythng, EVRYTHNG IoT Smart Products Platform |. Available at: https://evrythng.com/ [Accessed May 21, 2017].

Fernandes, E., Jung, J. & Prakash, A., 2016. Security Analysis of Emerging Smart Home Applications. *Ieee S{&}P '16*, (May), pp.636–654.

Fromknecht, C., Velicanu, D. & Yakoubov, S., 2014. CertCoin: A NameCoin Based Decentralized Authentication System 6.857 Class Project. , pp.1–19.

Gaurav, K. et al., 2015. IoT Transaction Security. *Iot-Conference.Org*, pp.5–6. Available at: http://www.iot-conference.org/iot2015/wp-content/uploads/2015/11/IoT2015_PS06_1570213099.pdf.

GDPR, E., 2016. Artificial intelligence, Robotics, Privacy and Data Protectuion. *International Privacy Conference*.

Geels, F.W. & Schot, J., 2007. Typology of sociotechnical transition pathways. *Research Policy*, 36(3), pp.399–417.

Huberman, B.A., 2016. The Internet of Things (IoT). *Nursing Education Perspectives*, 34(1), pp.63–64. Available at: http://nlnjournals.org/doi/abs/10.5480/1536-5026-

34.1.63.

Hughes, T.P., 1983. *Networks of Power*,

IBM, IBM - Watson Internet of Things Platform. Available at: http://www-03.ibm.com/software/products/en/internet-of-things-platform [Accessed June 6, 2017].

International Telecommunication Union, 2015. *Measuring the Information Society Report 2015*,

Kuhlman, T. & Farrington, J., 2010. What is Sustainability? *Sustainability*, 2(11), pp.3436–3448. Available at: http://www.mdpi.com/2071-1050/2/11/3436/ [Accessed June 14, 2017].

Linux Foundation, 2016. Hyperledger Whitepaper v2.0.0. , pp.1–19. Available at: https://github.com/hyperledger/hyperledger/wiki/Whitepaper-WG.

Litecoin, Litecoin.com - Open source P2P digital currency. Available at: https://litecoin.com/ [Accessed June 9, 2017].

Merkle, R., 1980. Protocols for Public Key Cryptography. *Synopsis on Security and Privacy*, pp.122–134.

Miorandi, D. et al., 2012. Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7), pp.1497–1516. Available at: http://dx.doi.org/10.1016/j.adhoc.2012.02.016.

Misra, S., Maheswaran, M. & Hashmi, S., 2017. *Security Challenges and Approaches in Internet of Things*,

Nakamoto, S., 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. *Www.Bitcoin.Org*, p.9. Available at: https://bitcoin.org/bitcoin.pdf.

NIST, U.D.O.C., 2014. Guidelines for smart grid cybersecurity. , 1, p.668. Available at: http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf.

Ouaddah, A. et al., 2017. Access control in the Internet of Things: Big challenges and new opportunities. *Computer Networks*, 112, pp.237–262. Available at: http://dx.doi.org/10.1016/j.comnet.2016.11.007.

Paul, B., 1962. On distributed communications network. , pp.3–4.

Previtali, D. et al., 2016. The Business Viewpoint of Securing the Industrial Internet - Executive Overview. , pp.0–15.

Richard, W., 2016. Blockchain Eco System. *www.Firstpartner.net*, p.2016.

Ripple, Welcome to Ripple | Ripple. Available at: https://ripple.com/ [Accessed June 9, 2017].

Rogers, E.M., 1995. *Diffusion of Innovations*,

Samsung, Samsung ARTIK Internet of Things (IoT) Platform. Available at: https://www.artik.io/ [Accessed June 6, 2017].

Schwartz, D., Youngs, N. & Britto, A., 2014. The Ripple protocol consensus algorithm. *Ripple Labs Inc White Paper*, pp.1–8. Available at: http://www.naation.com/ripple-consensus-whitepaper.pdf.

Seibold, S. & Samman, G., 2016. Blockchain Consensus. *KPMG*, 51(3), pp.187–190. Available at: http://csi.sagepub.com/cgi/doi/10.1177/0011392103051003001.

Sicari, S. et al., 2015. Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, pp.146–164. Available at: http://dx.doi.org/10.1016/j.comnet.2014.11.008.

Smith, J.K., 1983. Quantitative Versus Qualitative Research: An Attempt to Clarify the Issue. *Educational Researcher*, 12(3), pp.6–13.

Stuart Madnick, Security Surprises Arising from the Internet of Things (IoT). *Forbs.com*. Available at: https://www.forbes.com/sites/ciocentral/2017/05/08/security-surprises-arising-from-the-internet-of-things-iot/#7883a1a22495 [Accessed June 6, 2017].

Svensson, D. & Leung, P., 2015. an Investigation Into Use of Public Ledger Technology To Create Decentralized Digital Resource-Sharing Systems.

Swanson, T., 2015. Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems. , p.66. Available at: http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf.

Szabo, N., 1994. Smart Contracts. Available at: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html [Accessed June 11, 2017].

Tapscott, D. & Tapscott, A., 2016. The Impact of the Blockchain Goes Beyond Financial Services. *Harvard Business Review*. Available at: https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services [Accessed May 13, 2017].

Thingworx, Enterprise IoT Solutions and Platform Technology. Available at: https://www.thingworx.com/ [Accessed May 21, 2017].

Tidd, J. & Bessant John, 2009. *MANAGING INNOVATION*,

Tuan, T. et al., 2017. BLOCKBENCH: A Framework for Analyzing Private Blockchains.

Union, E., 2016. How will the EU ' s reform adapt data protection rules to new technological developments ? , (January), pp.10–11.

Vitalik Buterin, 2014. Long-Range Attacks: The Serious Problem With Adaptive Proof of Work - Ethereum Blog. *Ethereum*. Available at: https://blog.ethereum.org/2014/05/15/long-range-attacks-the-serious-problem-with-adaptive-proof-of-work/ [Accessed May 15, 2017].

Watanabe, H. et al., 2016. Blockchain contract: Securing a blockchain applied to smart contracts. *2016 IEEE International Conference on Consumer Electronics, ICCE 2016*, pp.467–468.

Weber, R.H., 2010. Internet of Things - New security and privacy challenges. *Computer Law and Security Review*, 26(1), pp.23–30. Available at: http://dx.doi.org/10.1016/j.clsr.2009.11.008.

World Economic Forum, 2011. *Personal data : The emergence of a new asset class*, Available at: http://www.weforum.org/reports/personal-data-emergence-new-asset-class.

Xively, IoT Platform for Connected Devices| Xively by LogMeIn. Available at: https://www.xively.com/ [Accessed June 6, 2017].

Yaler, Yaler.net - access devices from the Web. Available at: https://www.yaler.net/ [Accessed June 6, 2017].

Zhang, Y. & Wen, J., 2016. The IoT electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Networking and Applications*, pp.1–12. Available at: http://dx.doi.org/10.1007/s12083-016-0456-1.

Zyskind, G., Nathan, O. & Pentland, A., 2015. Enigma: Decentralized Computation Platform with Guaranteed Privacy. *arXiv:1506.03471 [cs]*, pp.1–14. Available at: http://arxiv.org/abs/1506.03471%5Cnhttp://enigma.media.mit.edu/%5Cnhttp://enigma.media.mit.edu/enigma_full.pdf%5Cnhttp://www.arxiv.org/pdf/1506.03471.pdf.

Zyskind, G., Nathan, O. & Pentland, A.S., 2015. Decentralizing privacy: Using blockchain to protect personal data. *Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015*, pp.180–184.