Decentralized Digital identity management using Blockchain and its implication on Public Sector

Dissertation submitted in part fulfilment of the requirements

for the degree of

Master of Business Administration

at Dublin Business School.

Sourabh Wadhwa

Student Number: 10354466

Master of Business Administration 2019

Contents

Table of Figures:

Declaration

I Sourabh Wadhwa, declare that this research is my original work and that it has never been presented to any institution or university for the award of Degree or Diploma. In addition, I have referenced correctly all literature and sources used in this work and this this work is fully compliant with the Dublin Business School's academic honesty policy.

Signed: Sourabh Wadhwa Date: 07th January, 2019

Acknowledgements:

I would like to acknowledge few people who have been integral part of the process while writing the dissertation.

I would like to express my gratitude to my supervisor Harnaik Dhoot who shared the article “What Makes a Good Research Question?” in our first meeting to enlighten about the whole research process and encouraged to go above and beyond to complete the whole dissertation.

And thanks to all of my extended family back in India who constantly supported me over the video calls and guided to manage work life balance.

I would like to thank my mentors and colleagues at workplace who shared their journey and tips to remain focused and diligent during the whole process.

Finally, I would like to thank those individuals who took their time away from the pressures of work to be interviewed.

Stan Nazarenko, CFA - Co-Founder & CEO @ Piprate

Eoin Connolly – Technology Director @ ConsenSys

Zia Khan - Co Founder @ Independent Consultant

"Dr Jane Thomason – CEO @ Blockchain Quantum Impact

Stuart Wilson - CTO @ Blockchain Advisory UK

Samrat Kishor – Manager @ Accenture Strategy India

Abstract:

The purpose of this dissertation is to explore the Decentralized Digital identity management using Blockchain and its implication on Public Sector. The literature and latest reports suggests that Blockchain is one of the disruptive technology which will impact several segments of the industry to bring transparency and elimination of third parties.

The research is to look further into existing digital identity management solutions and much greater insights into the emergence of decentralized digital identities and how they are going to impact the public sector to bring more transparency and confidence within citizens. At the beginning of the paper, researcher will focus to analyse the existing literature, journals, newspaper articles, academic books and industrial reports. The overall research is based on qualitative studies which involves multiple interviews with industry leaders who are either Blockchain technology consultants or working directly on developing digital identity management solutions. These interviews will provide the insights with an overview of evolvement of decentralized solutions and their impact on different industries with main focus on Public Sector. One of the objective is to understand whether decentralized identity management solutions based on Blockchain can replace the centralized one along with few more objectives.

Chapter 1 – Introduction

1.1 Background:

This dissertation will focus on the digital identity based on Blockchain technology in a decentralized environment and its impact on users on day to day basis.

Several recent incidents have emphasized that the security issues related to internet in digital world are crucial and challenging. Public personal information is being quite often hacked and spread around the globe for illegal activities leading to disclosure of financial assets of an individual without their consent which directly or indirectly causes the trust deficit for the general online user and even impact the thinking an individual to make internet transactions. Several institutions have tried to provide solutions to safeguard the online user identities and their data but it is still a problem for several internet companies and researchers. (Ferreira, 2014)

Personal data is the primary target for the breach of information since it is traditionally stored on the centralized platforms which makes it relatively easier for dark web users (hackers) to breach into large systems at once and achieve their malicious targets. (Ferreira, 2014)

Satoshi Nakamoto came up with the concept of Digital Currency “Bitcoin” in 2008 which was based on a new technology known as “Blockchain” and Bitcoin let users conduct transactions in the digital world without depending on a third party to inspect and verify (Nakamoto, 2008). Rapid popularity and acceptance of Bitcoin in the market led several technology giants to conduct further research on its foundational technology – Blockchain. Bitcoin based on Blockchain brought a new era in the online world where the intervention of third party could be eliminated to transfer values. Decentralization is the primary feature of the Blockchain technology which gave the way to maintain data by all the nodes on the desired network rather than on centralized location. Blockchain has features like high security, time stamping, cryptography and hard to tamper with since the creation and modification of data is governed by consensus mechanism and agreed by all the nodes or the majority of the nodes on network. Such features proposed to be potential solution for digital identity management (Swan, 2015)

In this way, user are able to perform transactions and save data on Blockchain nodes without worrying about anyone to illegally steal or modify their data, ensuring the information security requirement of an identity management.

1.2 Research Objectives:

The aim of this study is to understand how Digital Identity Management solution work in centralized environment, its divergence to Decentralized platform using Blockchain Technology and the overall impact it is going to create on Public Sector.

The researcher's interest is primarily to learn about one of the disruptive technology "Blockchain" to enhance career and personal development along with desire to understand theoretically and practically about the Decentralized Identity Management solution being developed to change the information technology landscape.

The research needs to be focused and have a clear direction if the research is to be successful. Saunders contends that developing research objectives from the research question to give clear, specific statements of what the researcher wishes to accomplish, will establish the research focus (Saunders L. P., 2012). If the research objectives describe what the research wants to achieve, the personal objectives of the researcher should also be considered. Maylor and Blackmon recommend the addition of these personal research objectives in order to address specific learning or career development objectives (Maylor, 2005). The specific objectives for this research are as follows:

- To develop the researcher's knowledge and understanding of identity management solutions & Blockchain technology.
- To determine the impact of existing identity management solution on an individual's privacy.
- To identify the advantages of developing decentralized identity management solutions and progress so far.
- To describe the fundamental technological advantage of using Blockchain technology to develop decentralized digital identity management solutions.
- To describe the usage and impact of decentralized digital identities on Public Sector.

1.3 Research Question:

The research questions are derived from the researcher's personal interest and experience having worked in the information technology world for over 5+ years. Blockchain has been considered as the era of Web 3.0 which is going to change "How the industry currently works and performs transactions?"

The research questions stem from the researcher's interest in understanding if the adoption of Blockchain technology to develop decentralized Digital Identity Solutions is, in practice, informed by theory and research literature, and the researcher has set the goals of this research to answer the following question:

How will Decentralized Digital Identity Management solution based on Blockchain evolve in the future and the impact they are going to create on Public Sector?

1.4 Scope of limitations of the research:

Researcher has opted for qualitative approach and conducted six refined interviews with Blockchain experts and founders of similar organisations. There are still few limitations from research point of view.

Currently organisations, public sector and government institutions are using only centralized identity management solutions since there was no concept of decentralized. Most of the literature is based on centralized identity management solutions and decentralized solutions are still under the development for future use.

Industry reports suggest that there are around 12-15 organizations working on to develop decentralized identity management solutions and are under pilot phase. Usage and post implementation impact of decentralized identities is yet to be measured and meanwhile 'Decentralized Identity' is just a term with hopes to transform the identity management solutions.

Decentralized capabilities to bring transparency within any technology were missing until Nakamoto came up with the idea of Blockchain in 2008. Development within Blockchain world is at early stages and after performing systematic literature review, researcher could find there are limited number of research papers on Blockchain and most of them are focused on 'cryptocurrency' and economic disruption with Blockchain. Remaining papers focus on technical capabilities of Blockchain.

Despite high expectations from this technology, research into utilization of Blockchain technology for area other than cryptocurrencies is at very early stages. Industry reports and academic research showcase massive potential of Blockchain technology but there are very few examples on how to implement this technology to overcome the barriers.

There is even critical lack of Blockchain talent in the market. Out of 6 responded only 1 was working in the capacity to develop the decentralized identity wallet and was happy to share insights with researcher due to similar interest. Other respondents have wealth of experience and could share as much insights as they have worked on.

Time management was another important limitation for the study since researcher was full time occupied with one of consulting organization in Dublin as an Intern.

Researcher believes that with availability of more academic reading and interviews from decentralized identity developers could have provided in depth analysis.

1.5 The organisation of the dissertation:

The complete dissertation is divided into several sections to get a logical workflow:

Chapter 1 specifies the research question which will be studied during the whole process to get to the logical outcome. It specifies the objectives, limitation, scope and future contribution details.

Chapter 2 revolves around the central theme 'Literature Review' in the area of digital identity management solutions, further covers the Blockchain technology for adopting decentralized mechanism leading to the public sector and its involvement in using identity management solutions.

This review is completely based on secondary sources to draw main themes and findings for further discussion.

Chapter 3 describes the methods, philosophy opted for research along with choice of collecting the data procedure. It specifies the selection of qualitative method to gather data from industry experts. This section also gives the details to techniques considered for data analysis, validity and reliability of the data.

Chapter 4 describes the profile of the respondents, data analysis procedure, findings from the interviews – primary research. Data is further analysed to gather common themes and emergence of relationship with these themes.

Chapter 5 discusses the findings emerged from chapter with respect to literature review.

Chapter 6 draws near to the final conclusion of the overall research and provides recommunication for the decentralized identity management solution using Blockchain with details of opportunities and challenges in public sector.

Chapter 7 concludes the research by sharing the overall experience, learning and value add to personal as well as professional life during the whole course of MBA.

1.6 Major Contributions:

The study is designed to analyse the identity management solutions and Blockchain world. The qualitative approach will provide insights on the impact Blockchain technology is having on traditional identity management solutions and how new entrants are going to bring the disruption with latest innovations.

This study will help new entrants who are looking to develop decentralised solutions and existing providers of identity management solutions to analyse the impact. This will be stepping stone for future studies once decentralized solutions are available and adopted on large scale. Reports from most of academic results give the technical adoption of Blockchain technology and contribution of this research will give insights on adoption process to fill the gaps.

The research conclusion will give a strong understanding of the industry on the basis of findings gathered from six leading experts in Blockchain space.

Chapter 2 – Literature Review

2.1 Introduction:

Literature review gives the opportunity to explore the sources of secondary data for the research study and identifies the progress and limitations of the main topics related to study. Main aim of the literature review is to both define and support the research question and its objectives (Maylor, 2005). Literature review makes sure that there is coherence between the reaming dissertation and literature keeping the research question grounded (Andrews, 2004).

Author Hart shares insights and defines that the purpose of studying the literature is to identify the importance of work that has already been published and work in progress which is relevant to this research. This chapter will highlight the issues, themes which are critical for the emergence of decentralized digital identity management based on Blockchain and the implication it is going to create on public sector. It develops the conceptual lenses that will be used to analyse the subject areas, theories, concepts and models; it is divided into three main sections.

2.2 Digital identity and its emergence:

Identity defines the uniqueness of an individual as a consistent object when compared over a period of time but brings the divergence in matters of public and private matters.

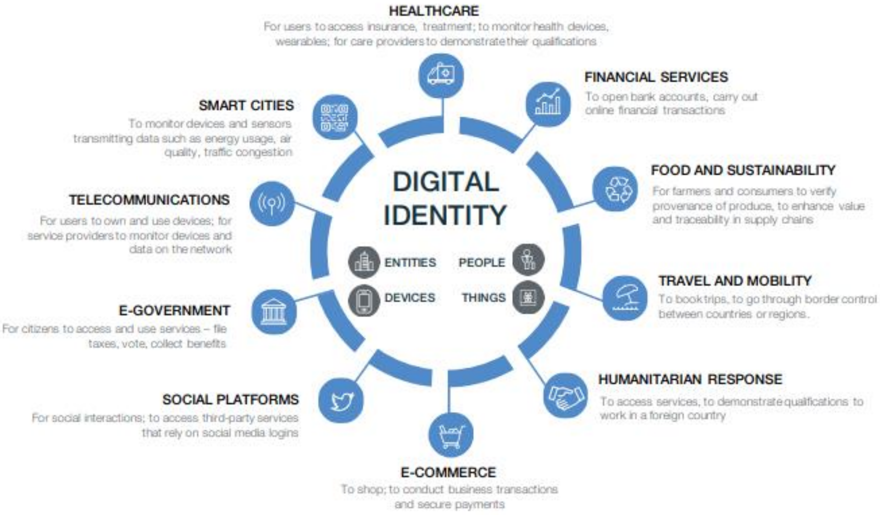
Jared Dunn one of the characters of Silicon Valley's TV series expressed that "a name is just a sound that somebody makes when they need you" (Breckenridge, 2018) and these names should lead to depict uniqueness of an individual, to make sure they are accountable and can be trusted institutions.

Stanford had mentioned in its research "identity" as "The sameness of a person or thing at all times or in all circumstances; the condition or fact that a person or thing is itself and not something else; individuality, personality." (Fearon, 1999)

The purpose of Digital identities is to bring uniqueness and accountability between the names of an individual (physical identity) and government institutions of the society and migration of government institutions from providing paper based services to electronic facilities have made "Digital Identity" as fundamental right for each individual.

As per the report published by WEF, an average internet user has created around 92 accounts to avail, shop or consult private and public services which will increase likely to 200 by 2020 (Forum, 2018). On the other hand, having a digital identity can leave an individual to potential for fraud by collecting their personal details as such bank details, credit information and answer to several personal questions.

In today's world, an individual can be identified by means of attributes, metadata, and data linkage and such attributes help to predict the activities of an individual which was not possible with traditional physical paper identification (OECD, Working Party on Security and Privacy in the Digital Economy, 2015) which emphasizes on the prediction led by analysing the digital identities.


HEALTHCARE
For users to access insurance, treatment; to monitor health devices, wearables; for care providers to demonstrate their qualifications
FINANCIAL SERVICES
To open bank accounts, carry out online financial transactions
SMART CITIES
To monitor devices and sensors transmitting data such as energy usage, air quality, traffic congestion
FOOD AND SUSTAINABILITY
For farmers and consumers to verify provenance of produce, to enhance value and traceability in supply chains
TELECOMMUNICATIONS
For users to own and use devices; for service providers to monitor devices and data on the network
DIGITAL IDENTITY
ENTITIES
PEOPLE
DEVICES
THINGS
TRAVEL AND MOBILITY
To book trips, to go through border control between countries or regions.
E-GOVERNMENT
For citizens to access and use services – file taxes, vote, collect benefits
HUMANITARIAN RESPONSE
To access services, to demonstrate qualifications to work in a foreign country
SOCIAL PLATFORMS
For social interactions; to access third-party services that rely on social media logins
E-COMMERCE
To shop; to conduct business transactions and secure payments

Digital Identity in today's world (WEF, 2018)

There are significant number of definitions related to digital identities:

Global System for Mobile Communications stated digital identity as “in today’s world, our digital identities are becoming imminent part of our life as we transition to a mobile world and these identities only predict the way we will behave, transact and trade. For business world, harnessing the power of digital identities is a crucial element of doing business – particularly when it comes to meeting various compliance and customer due diligence (CDD) requirements (Kvitnitsky, 2018)

Non-Profit organisation “The European Association for e-identity and security (EEMA)” emphasizes that digital identity is long existing but the hardest part is binding a physical person to digital identity which could help them to access their e-mail account, digital money, traditional bank accounts and led to a new journey of digital transformation and identity management technologist are always striving hard to establish secure ways to bring larger part of population to migrate on this pathway in an efficient way (Erik, EEMA.ORG, 2018)

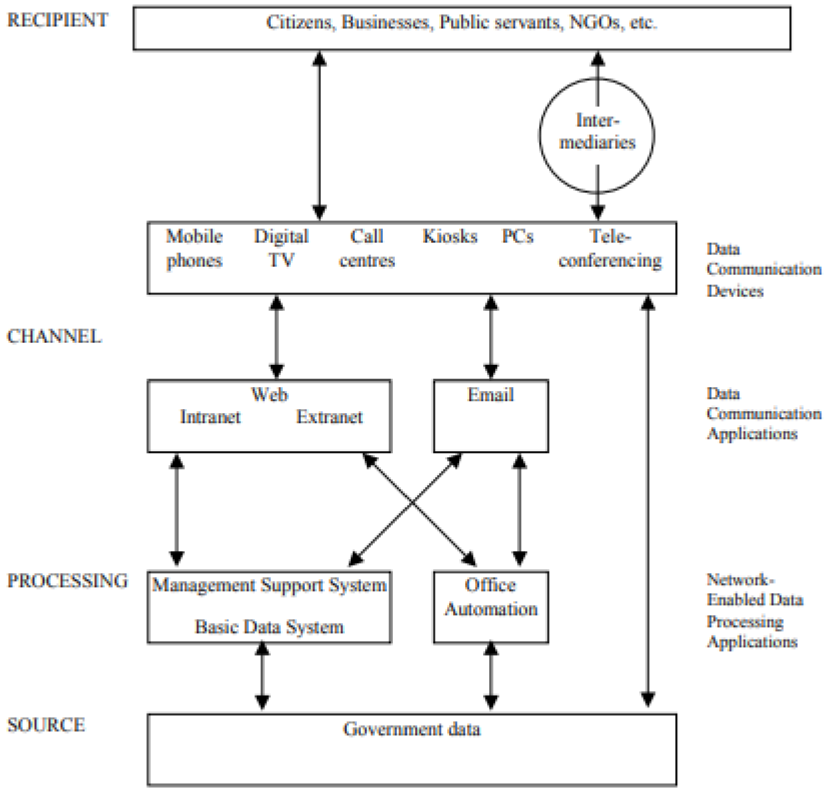
In a paper by SECURE IDENTITY ALLIANCE about “STRONG IDENTITY STRONG BORDERS” emphasizes on ‘effective use of paper based identities of a country’s citizen through records of marriage, death and birth to safeguard its borders and utilizing technology to enable and assure evidence of digital identity which can be directly carried in the form of eiD card or smartphone. This leads to capability of analysing information relating to similar person supported by biometrics, to form a holistic, person-centric view of the person, accurately, across multiple (Alliance, 2018)

Traditionally, world’s business and transactions have relied completely on physical documents and human interactions which were authenticated and issued by regional/national governments and very soon became a substance of forgery resulting in many serious crimes. Before computers became the dominating databases of identity provider, there were manual/paper based databases which were owned by governments, corporations, and banks to access collected data related to their citizens, employees, organizations etc. which is not possible in today’s time and one can’t completely rely only on physical identification. Today’s consumer expects more convenient, agile and reliable business transactions and 24/7 connectivity.

Since the emergence of internet at the end of 20th century and initiatives of government institutions and business transaction to serve citizens/consumers electronically in the beginning of 21st century, it has become inevitable for individuals not to have a digital identity which is backed by some kind of authentication.

(Sachdeva, 2002) published a white paper on "E-Governance Strategy in India" which suggested the idea of replacing traditional functioning of government institutions with the help of electronic/digital media. Scope of this E-GOVERNANCE model consisted of Government to Citizen, Citizen to Government, Government to Government and Government to Business etc. activities to achieve essential achievements like Information for All, Citizen Feedback, Improving services, Citizen Participation etc. and the whole model was based on implementing Digital identities for every institutions for electronic identification and authorisation.

The Architecture of e-Governance



E-Governane Model (Sachdeva, 2002)

After every two years, United Nations conducts an "UN E-Government Survey" for all of its 193 member states to find out the developments in digital area and report of 2018 survey showcase that online transactional services within last two years have increased from 18 % to 47% in different service areas confirming the participation of citizens to utilize digital platforms. Online birth registration number has significantly increased from 44% in 2016 to 86% in 2018 which is comprised of only 45% United Nations Member States and the services are yet not available to least developed countries.

Online transactions are only possible with the utilization of some kind of Digital Identity to utilize online services index. Trends of improvement in online transactional services have been continuously increasing over the last four years in all countries and the most common online services in 2018 are paying for utilities (140 countries), submitting income taxes (139 countries), and registering new businesses (126 countries) (Nations, 2018)

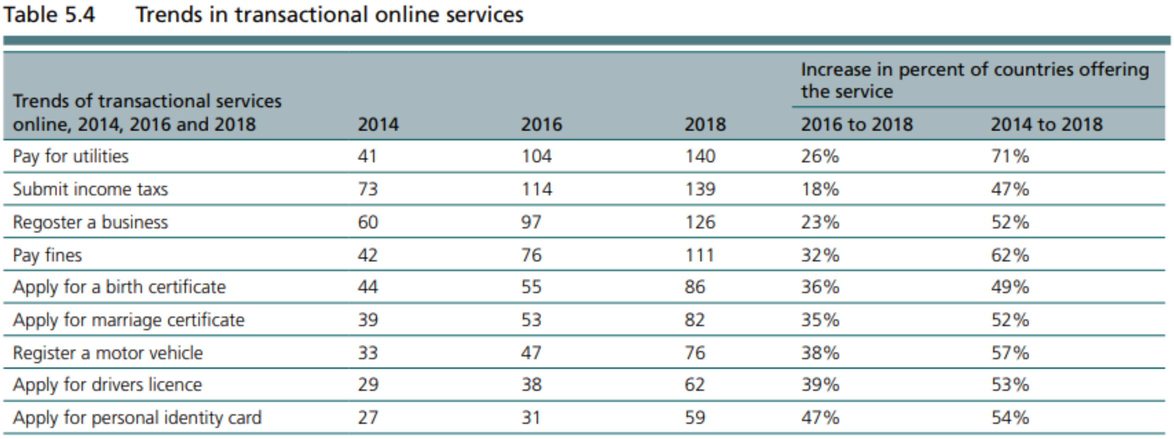


Table 5.4 Trends in transactional online services

Trends of transactional services online, 2014, 2016 and 2018	2014	2016	2018	Increase in percent of countries offering the service 2016 to 2018	 2014 to 2018
Pay for utilities	41	104	140	26%	71%
Submit income taxs	73	114	139	18%	47%
Regoster a business	60	97	126	23%	52%
Pay fines	42	76	111	32%	62%
Apply for a birth certificate	44	55	86	36%	49%
Apply for marriage certificate	39	53	82	35%	52%
Register a motor vehicle	33	47	76	38%	57%
Apply for drivers licence	29	38	62	39%	53%
Apply for personal identity card	27	31	59	47%	54%

Change in % over 2 years (Nations, 2018)

UN E-Government Survey 2018 confirmed that an estimated of 1.1 Billion people all over the world have no means of identity either legal/paper based or digital and are living as migrants, refugees in rural areas as disadvantaged groups and future developments goals plan to provide these section of citizens legal identities by 2030 which will exponentially help the countries to include disadvantaged groups as part of financial inclusion and prevent fraud, corruption while delivering the social benefits. United Nations have identified "Digital Identity" as a mode to expedite the overall process smoothly and effectively (Nations, 2018).

2.3 Digital identity management systems towards centralization:

Online world of internet is continuously evolving to provide users new ways of communication, knowledge sharing techniques and transact with other citizens or organizations. With continuous evolution of technology and its adoption in the society on digital platforms is leading to collection of sensitive information of millions of individuals while considering protecting and promoting individual privacy. Amount of sensitive personal information has increased over the time and is controlled by third parties without having little or no control (Pimenidis, 2010).

"Identity Management" has emerged as a practices in the electronic world to generate, provide and manage the rights to access, and maintain digital identity with trust and reliability.

Though there is no identified or commonly accepted definition for this term due the fact that it is relatively a new term which is still evolving and understood from a technical perspective only (Miriam Lips, 2008). Few of the most commonly illustrated definitions of identity management are:

"Identity management (ID management) is the organizational process for identifying, authenticating and authorizing individuals or groups of people to have access to applications, systems or networks by associating user rights and restrictions with established identities. The managed identities can also refer to software processes that need access to organizational systems" (Rouse, 2017)

Garter research came up with following:

"Identity management (IM) is the security discipline that enables the right individuals to access the right resources at the right times for the right reasons" (Gartner, n.d.)

OECD came up with a detailed research on IM for the further development of internet economy and defined Identity management as:

"Identity management can be applied to human beings, business entities, devices or software applications. This guidance focuses on natural persons ("individuals") interacting with the information systems of public and private organisations ("service providers"3) through a digital network such as the Internet (OECD, DIGITAL IDENTITY MANAGEMENT , 2011)

The focus in all of the definitions was establishing the relation between individuals in physical world to provide services or access information in online world with trust and reliability.

There have been several identity management solutions in the industry since the inception of internet and researcher will focus on following:

Isolated Identity Management Model:

Service provider plays the crucial role as identity provider and service provider which leads to storage and operations of user on single server. In this model, the authentication, allocation and authorization of a digital identity is empowered by single service provider and acts as an attribute, identifier and authentication provider (Yuan Cao, 2010)

Since the model is completely based on user memory and user needs to keep the identity of each service and service provider acts a responsible for each user (Hasnae L0AMRANI, 2016)

Several researchers have emphasised the fact that due to one of the oldest IDM and availability of relevant knowledge makes it prone to security risks. Isolated model has been recognised as being independent, if there is threat of corruption of identity, there is no impact on other service providers and can raise the bar of security depending on each service provider. Whereas, this approach is a complex activity for the users and they have to repeat the security information steps each time and all details are backed in service provider server leading to centralization of information (Rachida AJHOUN, 2014), due to explosive growth on digital services, users have to keep track of credentials and loss of any forgotten password requires requesting service password to retrieve from centralized database (Yuan Cao, 2010). (Hasnae L0AMRANI, 2016) confirms that service provide have the overall authority to design and deploy his own architecture of identity management system based on business requirement of organizations and this leads to high concentration of data at one place and attack on personal privacy.

Centralized Identity Management:

Centralized identity management comes up with only functioning of identity providers to act as single authority rather than service provides in Isolated IDM. This approach reduces the number of identities to access different platforms and works as single identity (login/password) to access different providers. In general, centralized identity management system of several service providers is outsourced to central identity provider and it looks after overall services identification, credential and overall identity life cycle. Identity data of service providers are stored and maintained in central repository of identity provider (Bernd Zwattendorfer, 2014)

Research shows that the unique and single identity provider is centralized to provide access to all service providers and any kind of technical failures leads to inaccessibility (Rachida AJHOUN, 2014). Issues related to privacy protection, identity theft and unsupportive privilege delegation and access across different domains are quite few limitations (Yuan Cao, 2010). However, unique advantage of this model has unique weaknesses as well like whenever there is cyber-attack on identity database, all information related to users will be hacked and also with increase in number of users the performance of the system automatically decreases (Hasnae L0AMRANI, 2016)

Federated Identity Management:

Federated identity model is the most advanced and futuristic model being utilized by organizations for managing digital identities. Federated identity is considered as a group of organizations which have agreement on the basis of trust relationship to exchange information.

Federation can be defined as commonly set of standards, technologies to enable a set of service providers to authenticate identities from another service providers in federated trusted domain (Yuan Cao, 2010). This approach helps to reduce the number of identities but studies show that certain limitations as such problem to identity the providers of identity and continuous threat to the theft of the identities which breaches the security and privacy, an identity theft gives the access to hacker to access data of all providers in a single federation (Rachida AJHOUN, 2014)

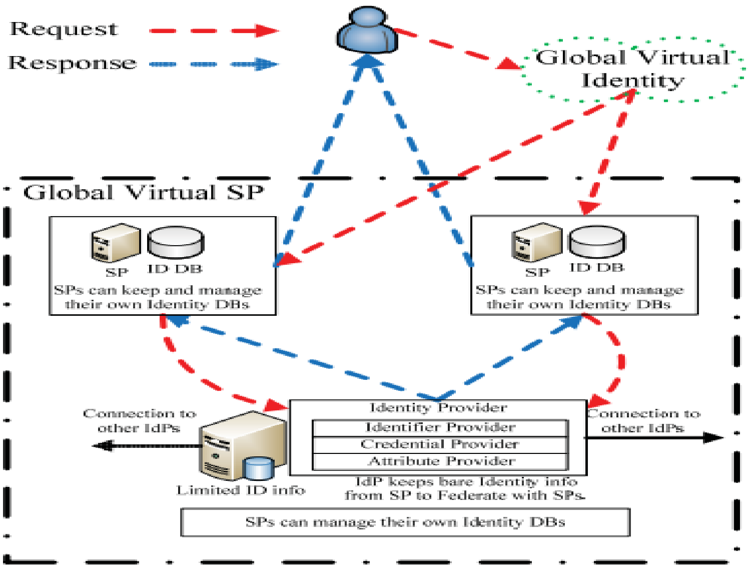


Figure 3. Federated model

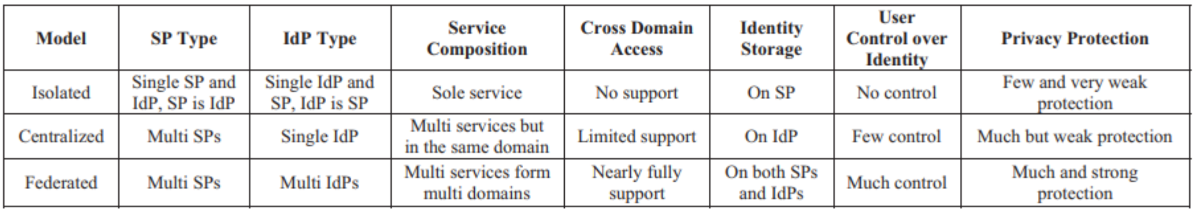
(Yuan Cao, 2010)

(Ali Ahmad Malik, 2015) have discussed in their research article in depth about the existing federated identity management and factors such as trust establishment, trust management and preservation of user privacy etc. as basic elements while deploying models of identity management.

Factors which can be considered to make federated identity management more secure and useful for large scale identity management (Ali Ahmad Malik, 2015):

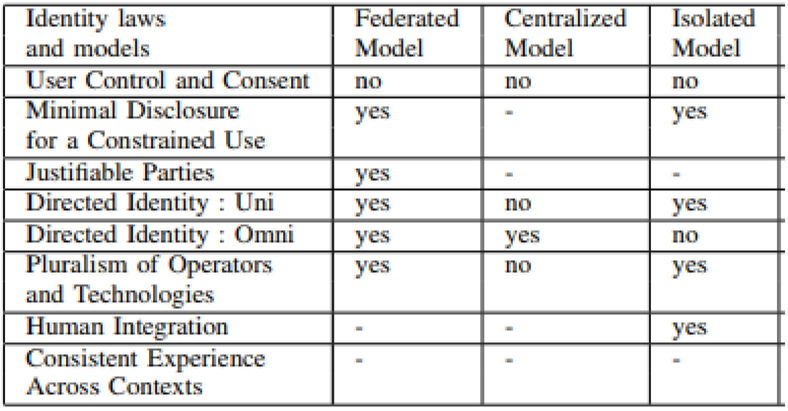
- Trust Management: when all identity providers and service providers communicate with each other directly, this solution can become more scalable in distributed centralized system for larger identities
- Trust Establishment: it makes the user more confident about the services he is using provided by a legitimate provide.
- User Privacy: To make sure the service provider is not malicious and doesn't harm the user by stealing his identity to conduct fraudulent activities on user's behalf.
- Consistent User Access Rights Across CoTs: User should be given role based access across different domains to similar service provider to avoid escalations of privileges attack.
- Continuous Trust Monitoring: There is high probability over time that the trust and quality of services may degrade and it's not worth to maintain such relationship.
- Adaptation to Unanticipated or Environmental Changes: Requirements keep on changing over the time to adjust the needs of the users and systems should be able to adapt to such changes which were not tested/expected beforehand.
- Analysis: Consideration of trust management/trust establishment techniques should be discretionary to the user's choice rather than identity provider.

(Yuan Cao, 2010) in their research paper did a comparative analysis of all three identity management models based on following criteria:



Model	SP Type	IdP Type	Service Composition	Cross Domain Access	Identity Storage	User Control over Identity	Privacy Protection
Isolated	Single SP and IdP, SP is IdP	Single IdP and SP, IdP is SP	Sole service	No support	On SP	No control	Few and very weak protection
Centralized	Multi SPs	Single IdP	Multi services but in the same domain	Limited support	On IdP	Few control	Much but weak protection
Federated	Multi SPs	Multi IdPs	Multi services form multi domains	Nearly fully support	On both SPs and IdPs	Much control	Much and strong protection

(Hasnae L0AMRANI, 2016) also did a comparative analysis of all three identity management models on different set of criteria:



Identity laws and models	Federated Model	Centralized Model	Isolated Model
User Control and Consent	no	no	no
Minimal Disclosure for a Constrained Use	yes	-	yes
Justifiable Parties	yes	-	-
Directed Identity : Uni	yes	no	yes
Directed Identity : Omni	yes	yes	no
Pluralism of Operators and Technologies	yes	no	yes
Human Integration	-	-	yes
Consistent Experience Across Contexts	-	-	-

Both comparison focus on user control and consent which is least in the hands of users and more focused on centralized authorities or identity providers. These IDM systems are source of benefits for identity providers since they gain access to valuable information without concerning the user's privacy and this leads to trust issues between service providers and users where users are reluctant to share required information and replacing with as little information as possible.

Sharing personal identifiable information is a great concern when it comes to protecting data, managing privacy and complying with government regulations and it is mandatory within federated identity to share such information which raised privacy issues (Eve Maler, 2008)

Limitations:

David Shoemaker in his research has stressed on following "identity management" (Shoemaker, 2010)

Algorithmic Manipulation: Public surveillance, facial recognition and gathering of sensitive information like date of birth, driving license, marriage records and storage of these information on online platforms which is being harvested in the form of secondary resources with the help of computer algorithms to find out future facts and forecasts.

Self-Autonomy: When large amount of personal information is accessed and analysed in an unauthorized way, it leads to undermine of specific aspect of autonomy which is the ability to manage one's reputation in public domain and these information tend to last for indefinite period of time.

Due to the emergence of abundant social and e-commerce platforms, vast majority of communication and commercial interactions take places in online world and these transactions are of informational, communicative, or commercial categories and include personal information stored in a "digital dossier" which can be traced back by the identity provider and user become a victim of analysis without knowing the boundaries between private and public domain (Ali Alkhalifah, 2012)

Today's identity management systems are more focused on collecting personal information to avail customized services and use of identifiable information consisted of digital identity are involved between individual's transactions and has come to a point where the anchors of identity trust are lost (Piotr Pacyna, 2009). The internet environment entails a high degree of vulnerability related to data storage, maintenance and management of the user's authentication data which varies on the utilization of different authentication systems and methods and hacking activities have led to exploit that vulnerability to become a social problem. (Yeonjung Kang, 2008) came up with the research model to provide a safe identity management measure by allowing the user to control the flow of his/her personal information in order to protect his/her privacy and prevent the misuse or abuse of personal information on the Internet.

(Ayed, 2011) in his research paper discussed about information abundance age where organizations are now exploring new opportunities by accessing and analysing information related to personal identities and providing services based on them. Digital memories fuel "unforgetting" and this is leading to "unforgiving" syndrome and digital identities could be consequences of stolen digital memories.

Self-Sovereign Identity Management:

Self-sovereign is being considered as the final step in the evolutions of identity management systems in the era of internet and provides combination of security, individual control and portability letting the organisation/individual completely owner and controller of the identity. Similarly, individual in itself is the identity provider without intervention of any third parties (Andrew Tobin, 2017)

Articles show that self-sovereign concept is not new rather from the 1970's when pioneers like Whit Diffie, Martin Hellman, and Ralph C. Merkle, creators of Public Key Cryptography aimed to help people protect their privacy in the new digital age of computers (Preukschat, 2018). Emergence of Self Sovereign identity has been considered as a storm which was required to wipe out the ongoing data breach, cyber-attack and assurance of an individual's privacy and is based on emerging distributed-ledger/decentralized technologies.

It enables multiple organizations and public/private institutions to work in coherence for the first time by assuring to form a decentralized network where personalised data will be located on multiple different locations to avoid fault and tampering and when this concept is combined with peer to peer encryption and distributed key management technologies, distributed ledger technology makes self-sovereign identity a futuristic possibility (Andrew Tobin, 2017)

Self-sovereign identity must protect the individuality, defend against financial and other losses, prevent human rights abuses by the powerful and support the rights of the individual to be oneself and to freely associate and guide the technologist to develop an identity management system which brings transparency, fairness, and support of the commons with protection for the individual (Allen, 2016).

Self-Sovereign in summary: (Andrew Tobin, 2017)

Security the identity information must be kept secure	**Controllability** the user must be in control of who can see and access their data	**Portability** the user must be able to use their identity data wherever they want and not be tied to a single provider
Protection	Existence	Interoperability
Persistence	Persistence	Transparency
Minimisation	Control	Access
	Consent	

Research articles on internet are flooded with positive impact Self-Sovereign identity can create for the future but John Erik (*Setsaas is Identity Architect at Signicat and a member of the EEMA Board of Management*) emphasized that “people” who are the central to the ownership of identity make mistakes which is an undeniable risk. Identity owners need to keep credentials safe of private key since there is no option to use “forgot my password” facility. Natural unforeseen disaster or traumatization of memory will lead to permanent loss identity and assets linked to it (Erik, EEMA, 2018)

Gelmato published a white paper which emphasizes that successful implementation on Self-Sovereign identities would require the development of an ecosystem consists of not only financial institutions but also merchants, mobile operators, government and each platform which has become the necessity in today’s time and this consortium can lead as a model of governance to craft rules of participation (gemalto, 2018)

2.4 Blockchain Technology and its Adoption:

Is Blockchain technology the next big thing?

(Di Battista G, 2015) Showcased multiple uses of Blockchain technology rather than just maintaining the Bitcoin transaction network. Some prototype applications have been developed and suggested for using Blockchain such as smart contracts, smart property, digital content distribution, Botnet, and P2P broadcast protocols. This shows that idea of Blockchain is not confined to Bitcoin rather than idea of a decentralized database can be applied in the form of customized applications in almost each industry. This makes the research more interesting to study the different aspects of its uses.

(Rick Kuhn, 2017) Blockchain-based Digital identity and access management systems can be leveraged to strengthen identity management solutions. Such systems have already been used to securely store information about goods’ provenance, identity, credentials, and digital rights. As long as the original information entered is accurate, Blockchain’s immutability device is genuine and that its software and settings have not been tampered with or breached.

Writing in 2017, Dr Garrick Hileman & Michel Rauchs in their study “GLOBAL BLOCKCHAIN BENCHMARKING STUDY” is one of the most populous studies with Blockchain domain conducted with over 44 organisations from 13 different countries and 29 public sector institutions of 19 different countries. A number of key findings such as 50% of infrastructure providers are currently utilizing Distributed Ledger Technology framework which can be utilized for new use cases of Blockchain applications within organization and there is upward momentum in non-financial use cases as compared to previous years and certainly focusing on government agencies where around 36% of Distributed Ledger Technology service providers are there customer. Certain challenges as such scalability of platforms, performance and security still remain the common one. Despite the challenges of trust boundaries and INTEROPERABILITY mentioned in the study, the prominence of adoption of technology and reaping its benefits clearly demonstrates the focus in overall study (Rauchs, 2017).

The approach of PwC and challenges it found in its reports regulatory uncertainty, lack of trust among users, and ability to bring a network together did undermine the confidence of the organizations planning to adopt such technologies but Blockchain leader at PwC, Steve Davies, said (Alexandre, 2018)

“Businesses tell us that they don’t want to be left behind by Blockchain, even if at this early stage of its development, concerns on trust and regulation remain. Blockchain by its very definition should engender trust. But in reality, companies confront trust issues at nearly every turn.”

Despite their outcome of crucial challenges, they did undertake the study with a sample size of over 600 executives from 40+ countries and came up with factor which influenced the adoption.

Study conducted by Infosys in 2017 have some overlapping findings of advantage reduction in settlement and transaction time was defined as challenging factor in study by EY same year. Similar study confirm that 74% of banks surveyed have executives on C Level who are driving these initiatives and early innovator banks (15%) are close to defining one of the futuristic first Blockchain ecosystem in the industry (Infosys, 2017)

While comparing the study reports of both (Accenture, 2018) and (Deloitte, Deloitte, 2018), researcher could find both have similar views on benefits of adopting Blockchain technology such as Secure and shared transaction ledger, Trusted third party elimination, Lower costs and Greater speed compared to existing systems. While Accenture study has limited information, Deloitte have covered the annual survey Blockchain with over 1053 senior executives and came up with different perspective by industry suggesting Automotive industry – supply chain as the most disrupted and public sector as least disrupted sector and the overwhelming majority of respondents (83%) believe that Blockchain based solutions are more secure than conventional IT systems which was opposite till last year 2017.

Gartner one of market research concluded the results of their *Gartner's 2018 CIO Survey* according to which among 293 CIOs, 77% CIOs confirmed that they have no interest in technology and factual evidence should be considered which is "It is critical to understand what Blockchain is and what it is capable of today, compared to how it will transform companies, industries and society tomorrow" and called Blockchain adoption as massively hyped (Asia, 2018).

Overall studies showcase that it's hard to analyse Blockchain adoption on common platform e.g. industry, country, sector, organizations etc. since this technology is yet to be completely adopted on large scale and abundant number of data to produce coherent output.

2.5 Blockchain based decentralized identity in Public Sector:

Reports suggests that Public Sector is being often laggard in terms of adopting the emergent technologies and there are very few of research studies across public sector of different countries.

Several researcher have emphasized that self-sovereign identity is the much required evolution of identity management solution and it can be achieved only on the basis of decentralized and distributed characteristics of technology which Blockchain has as its basic characteristic (gemalto, 2018)

Public sector is the crucial identity provider to citizens for their recognition in physical sphere which is normally paper based and one of the first use case for Public sector is discussed as "Identity Management" for Establishing and maintaining identities for citizens and residents (birth certificates, marriage licenses, visas, death records) (OECD, oecd.org, 2018)

Published in 2018 on “Challenges and Opportunities of Blockchain-based Platformization of Digital Identities in the Public Sector” to support transnational digital identity management without a central party and utilize Blockchain’s characteristics of being tamper-proof, transparent, decentralized, trust-less and public sector of several countries like Estonia have already started to utilize and provide decentralized digital identity which have saved a large amount money and time (Gilbert Fridgen, 2018)

Similarly, few challenges like performance, and scalability since these platforms are yet not fully scalable globally and integration to existing system (Gilbert Fridgen, 2018)

Blockchain based financial model (Gustav, 2017) have suggested that tax fraud and increasing transparency regarding the flow of dividends can be eliminated by including Blockchain base Smart Contract and integration into existing payment processes and when analysing the similar study (Antipova, 2018) when utilizing traditional data-management method to monitor continuous Blockchain systems and government auditor will be automatically alerted about the pre-determined integrity constrained transactions.

The Techruption Blockchain Project which is a public-private partnership project in the Netherlands and its seven members (Accenture, APG, Brightlands, Chamber of Commerce, De Volksbank, Rabobank, and TNO) are currently working on to develop a self-sovereign identity model which would allow exchange of limited open data, data from “things” (from IoT frameworks) as well as personal data in a decentralized environment and ultimately evolve as a solid framework for self-sovereign identity (ERCIM, 2017)

(Ahmed Alketbi, 2018) described several use cases in their study and discussed the technical advantages of Blockchain such as Cryptography & Digital Signatures, Hash, Public-Key Cryptography and consensus mechanism etc. to extend identity management with record keeping to increase overall compliance.

Deloitte report distinctly mentioned about the Voting with decentralized identity as potential emerging application of Blockchain in public sector which couldn't be found in other industry reports and Australian government has unveiled plans to conduct digital voting via the Blockchain technology in a bid to reduce costs and improve efficiency of parliamentary election (Deloitte, Deloitte, 2018)

A number of literature studies, such as (BOJANA KOTESKA, 2017) and (Josep Lluis de la Rosa, 2017) have dedicated to explore the challenges from existing research and came up with similar findings.

(Pîrlea, 2016) have performed exhaustive review but it's similar to most of the studies such as proposed improvements of Scalability which they themselves have cited from other research undermines the critical review of their research.

The study by (Jesse Yli-Huumo, 2016) took a different approach by conducting Systematic Review on Blockchain, second they confirmed that their proposed solutions lack concrete evaluation which led to untypical findings such as challenges and limitations in latency, size and bandwidth, throughput, versioning. Their choice of considering systematic review couldn't specify the industry of research.

Finally (Francesco PIGNATELLI, 2018) an (Standford, 2018) adopted speculative research methodology to conduct Blockchain for Digital Government and found that digital identity and identity management reforms are one of the top priorities for Government all over the world. These studies reviewed as inclusion of large amount of social issues inclusion and approach to future solutions.

2.6 Conclusion:

Detailed discussions on Digital identities and centralized identity management solutions have brought to the conclusion that there is significant need of decentralized identities which could provide self-sovereign rights to individuals to own, access and preserve personal data instead of becoming victim of data breaches or algorithmic analysis. Blockchain has emerged as a fundamental technology which could fulfil the technical requirements to establish a network of self-sovereign identity management and organizations need to make understand their customer's about advantages of adopting Blockchain and make overall value proposition a success for everyone.

Chapter 3 – Research Methodology and Methods

3.1 Introduction:

The literature review section has come up with the findings on topics, current themes and concerns that are relevant to Decentralized Digital identity management using Blockchain and its implication on Public Sector

And in this chapter, researcher will discuss and review his decisions on choice of research methodology and methods used to gather and analyse data from industry experts who have been working on Blockchain based identity management solutions.

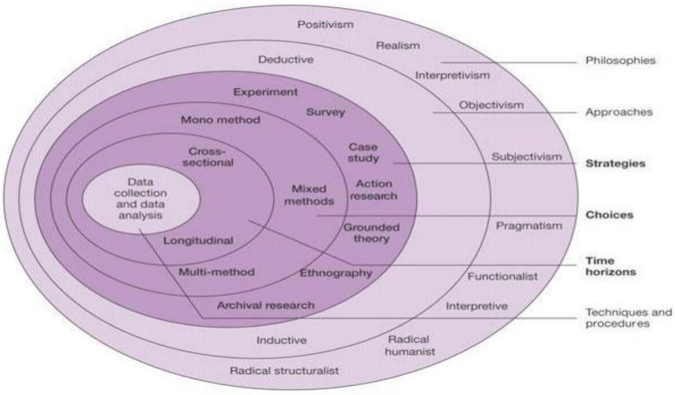
According to (Saunders L. a., 2009), research process is “a defined pathway of linked stages” which one needs to undertake in order to accomplish the research study and according to (Wayne Goddard, 2004) research can be explained as method of finding the answers of unanswered questions.

The researcher’s decision to opt for these questions to make layer of defined research objectives and this chapter will discuss, deep dive and evaluate the methods to conduct this research.

The objective of this evaluation is to draw various elements of the study for the readers to link the findings and its foundation.

Research Onion analogy proposed by (Saunders L. a., 2009) will help the researcher to make this complex study simpler and researcher will adopt the each layer this onion as a framework for deciding the format of the research.

(Saunders L. a., 2009) emphasised that solid philosophical knowledge helps the researcher to explore in a systematic way which poses a positive impact on the quality of the findings.



Research Onion (Saunders L. a., 2009)

(Holden, 2004) suggests that understanding the research philosophy is eminent part of research process since it opens up the researcher's mind to several different possibilities which will improve the research skills and methodology adoption.

The researcher has adopted to a research paradigm which is aligned with his own ideas, views and thought process and linked to realistic framework leading to the prioritization of research objectives.

3.2 Philosophy:

The research philosophy adopted for a particular research is accompanied by the assumptions perceived by the researcher about the world. Each stage of the research is carried with several assumptions like human understanding and knowledge of particular field and the nature of findings occurred during the research defines how one can understand the research objectives and question.

It can be significantly discussed that researcher's assumptions defines the final outcomes and the selected methodology imminently affects what has been discovered (Jackson, 2013).

There are major four research philosophies described in the "research onion" which are Positivism, Realism, Interpretivism, Pragmatism and they help the researcher on identifying how the knowledge can be developed and considered to be acceptable (Saunders L. a., 2009).

Positivism focuses mainly on society as the main viewpoint of the research and tries to understand it's the facts related to the behaviour of an individual in certain way (Walliman, 2011). The researcher with this viewpoint considers how centralized identity management solutions are helping the industries to control the freedom of an individual in a value free manner.

Realism is completely based on the fact that the existing reality is independent of human viewpoints and beliefs (Saunders L. a., 2009).

Interpretivism focuses on capturing the uniqueness and diverse complexity of social situations (Saunders L. a., 2009) and this defined the significant difference while organizing research among people and physical objects. As per (Saunders L. a., 2009) phenomenology and symbolic interactionism are the originating traditions of interpretivism. Phenomenology suggests how humans makes decisions in the world and symbolic interactionism as interpretation of social world around us and the interpretation of actions of other with whom we interact to make adjustments of our own meanings.

Pragmatism approach plays an integral part of this research since it helps the researcher to avoid becoming part of discussions such as truth and reality and majorly focuses on adopting valuable findings and use it to bring positive viewpoint of overall system (Saunders L. a., 2009)

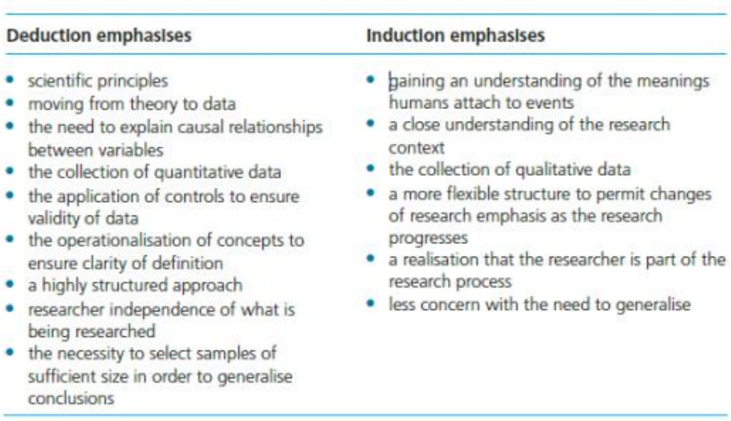
Researcher has chosen to apply combination of Interpretivism and Pragmatism research philosophies for this dissertation. The interpretivist view along with pragmatist considered by the researcher is that social reality is a dynamic synergy of the perceptions and actions of the actors within a subjective reality (Saunders L. a., 2009)

Since this research aims to investigate and explain the reality of Decentralized movement of Identity Management on Blockchain and an interpretivist along with pragmatist approach is the most appropriate as it is the researcher's belief that the context in which phenomena take place is an integral part of the phenomena themselves.

3.3 Approach:

The second layer of the research onion is described as research approach. Both inductive and deductive approach have their own pros and cons since researcher can choose to work with inductive approach where researcher can first collect the qualitative data and based on derived findings, draws suitable theory or pattern Or deductive approach where based on the existing data sources is utilized to draw hypotheses (Saunders L. a., 2009)

Research based on inductive approach emphasises on the complexity carried by individuals which is aligned with interpretivist philosophies (Saunders L. a., 2009).



Deduction emphasises	Induction emphasises
• scientific principles • moving from theory to data • the need to explain causal relationships between variables • the collection of quantitative data • the application of controls to ensure validity of data • the operationalisation of concepts to ensure clarity of definition • a highly structured approach • researcher independence of what is being researched • the necessity to select samples of sufficient size in order to generalise conclusions	• gaining an understanding of the meanings humans attach to events • a close understanding of the research context • the collection of qualitative data • a more flexible structure to permit changes of research emphasis as the research progresses • a realisation that the researcher is part of the research process • less concern with the need to generalise

Attributes of the deductive and inductive approaches (Saunders L. a., 2009)

This research aims to construct theory from discussion with industry experts, while relying on qualitative data. This research is concerned with understating of existing centralized identity management solution and emergence of decentralized identity management solution based on Blockchain and impact it is going to create on Public sector from the experience of industry experts who are working or teaching about such concepts. The researcher seeks to elaborate the data captured and draft the phenomena of Blockchain technology for Decentralized Identities adoption and formulate a theory in the context the Decentralized Identity Management solutions based on Blockchain.

While having option to choose any one of the theory, the researcher has chosen to conduct an inductive based study. This approach is consistent with methodological perspective and due to exploratory demand of this study which is in relatively immature environment of rapidly evolving technology, researcher is of the belief that inductive approach will help to draw greater insight and value.

(Saunders L. a., 2009) has specified that deductive research requires large samples of data and discussions to generate valuable results where inductive approach comes worthy with small and non-existing samples of data and discussion to draw findings and discussions.

This research approach shares the techniques to collect and analyse the data and how this data will be interpreted to answer the research question.

3.4 Strategy:

The research strategy can be defined as a systematic plan undertaken by the researcher to answer the research questions (Saunders L. a., 2009). Research strategy plays the vital role as a methodological link to establish the relation between research philosophies and subsequent choice of collecting data and analysing it.

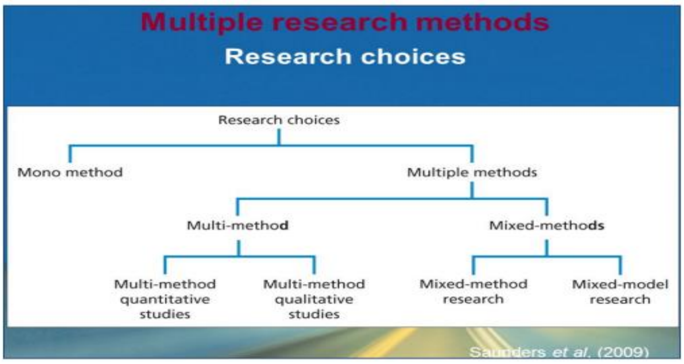
(Saunders L. a., 2009) states that the research strategy is not just influenced by the research question, but also by the research philosophy; research approach and purpose; concerns with the author's existing knowledge and experience; amount of time and data available; and the access to potential participants.

The third layer of the research onion which is baseline for gathering the data for research findings is "Research Strategy". Strategy helps the researcher to decide how to carry out the research and when considering the strategy both overall goals of the research and perspective of the researcher play vital role and the ultimate goal of any chosen strategy should enable the researcher to find out the answers to research objectives (Saunders L. a., 2009)

This research which is predominantly focusing on the role of Blockchain to develop new generation decentralized identities is exploratory in nature and the researcher choice of conducting "interviews" as a research strategy can help to achieve the overall goal of the research. Considering interviews over Surveys, case studies etc. is also appropriate for this study since it inclines with research philosophy Interpretivism. The exploratory aims of the research in conjunction with the interpretivist world view of the researcher make the interview as a choice of research strategy a sound choice.

3.5 Choice:

According to (Saunders L. a., 2009), the terms quantitative and qualitative are mainly utilized in business and management research to differentiate data-collection techniques and data-analysis procedures. Numeric data-collection techniques such as questionnaires, surveys are associated with quantitative method whereas non-numeric data capturing techniques like interviews, open ended discussions fall under the category of qualitative methods.



Multiple research methods

Research choices

Research choices

Mono method

Multiple methods

Multi-method

Mixed-methods

Multi-method quantitative studies

Multi-method qualitative studies

Mixed-method research

Mixed-model research

Saunders *et al.* (2009)

Mono-method – can be adopted by either the quantitative or qualitative data collection technique. Quantitative methods leads to collection of numerical data and qualitative methods gather the non-numerical data such as interview responses and are more widely used in the social sciences (Saunders L. a., 2009). When it comes to exploratory studies, qualitative methods are useful for building the theories with the help of small samples. This combination of characteristics and capabilities make qualitative methods the optimum choice for achieving the objectives of this research.

Multi-method – is more commonly adopted by business and management research, providing a richer approach to data collection, analysis and interpretations. This method can be used with more than one data collection technique, but restricted within either a quantitative or qualitative design. (Saunders L. a., 2009)

Mixed-methods – it may use quantitative and qualitative research equally. One methodology will be supporting the other. The weight and priority may vary depending on the research project. Mixed-methods research has become popular amongst researcher and is being considered as 'third methodological movement' after mono-method quantitative and qualitative methods (Venkatesh, 2013)

Considering the use of a mono method of qualitative research with collection of data from a single point of view is perfect for the study and researcher since the complex environment of Digital identity based on Blockchain cannot be answered by surveys which would provide the outcome such as Yes or No and each individual is not qualified enough to provide feedback on such complex topic unless they have also worked upon the same studies which would limit the overall population of the respondents.

Thus with the overall benefits of mono-method qualitative research over multi-methods to achieve the research objectives, researcher has selected the mono-method as the optimum research choice.

3.6 Sampling:

As per (Saunders L. a., 2009), sampling is required in situations when there is no possibility or requirement to gather data from large set of population and suggests mainly two types of sampling techniques which are Probability and Non-probability sampling.

Non-probability which is the most considered technique but doesn't impact the extent of research problem to determined (Saunders L. a., 2009). While considering this technique, researcher emphasizes that the selecting each element from a large sample is unknown (Riley, 2004).

Probability technique will help the researcher to make considerations about sample population and given parameters, helping the researcher to find common generalization about the population from selected sample (Riley, 2004). As per (Saunders L. a., 2009), the probability of selecting samples from selected population is known to the researcher.

Overall, sampling is being considered as an important catalyst while conducting qualitative research.

In general, sample is a part of targeted population where it is not fruitful or beneficial to undertake the study of entire population.

The sample criteria for this research was defined based on experience and knowledge of individual's expertise in the sector of digital identity management solutions consulting and Blockchain consulting and development skills. Individuals with such expertise were searched on LinkedIn with keywords like (Blockchain Consultant & Strategy, Digital Identity solutions, emerging technology leaders) globally and the filtered candidates were sent the connection request to establish further communication.

For this study, the research population was considered as individuals who have worked or working on developing decentralized identity management solutions or involved in providing Blockchain based consulting services for Digital identity solutions. Since there is no such list available for these individuals, researcher opted to consider non-probability sampling technique to define the sampling.

Major drawback of this technique is the inability of the researcher to draw characteristics of such working population, thus targeted respondents were selected based on their experience in relevant field to gather quality data.

According to (Saunders L. a., 2009), homogeneous sampling suggests to select the sample which are informative in nature to allow the study in greater depth and this technique is suitable when the size of sample is relatively small and the selected respondents do possess greater knowledge of the study topic.

Main reason to select homogeneous sampling for this research by the researcher are:

- Since the overall research is based on utilizing Blockchain technology for developing decentralized identity solutions and research was time constrained, certain specific individuals from relevant organizations were approached to gather their feedback.

- References from my current organization and LinkedIn connections did help to establish a good relation with respondents
- Researcher was aware of few organizations and individuals who were working on developing real time solutions and approached them with a positive mind set to discuss the study.

Using LinkedIn, around 100+ individuals from relevant field were sent connection request on time and researcher approached the accepted connections through personal message to give a brief review about the study to gain their interest for further discussion.

LinkedIn did come out as a useful tool to search the respondents and further communication. A Brief letter was sent to around 50+ candidates and 10 candidates agreed to have further communication for to share their knowledge. Out of these 10 candidates, few were working in the capacity of C suite level and overall decision making of relevant ongoing projects. All respondents were initially positive about the discussion and researcher set up the audio/video conference based on their feasibility. Only 6 candidates appeared for the discussion with great insights on the topic and remaining candidates requested to requested not to go ahead due to personal reasons.

Researcher believes that large number of respondents would have helped to gather valuable data and industry trend, however researcher was quite happy with number of respondents appeared for discussion with similar interest for detailed analysis.

3.7 Time Horizons:

Planning and executing the overall research within a defined timeline is another fundamental activity to be undertaken by the researcher. According to (Saunders L. a., 2009), time horizons are independent of the overall research strategy where directly dependent on research design.

Time horizons are generally divided into **longitudinal studies** where the researcher have the feasibility to gather the data several along with the development of relevant research study in real time whereas cross-section studies where the data is being collected just once within a defined time independent of future developments.

Since the researcher was itself fulltime occupied with industrial internship and deadline communicated by the institution, it will be desirable for the researcher to adopt cross-sectional approach as a feasible approach over longitudinal study.

In general, longitudinal studies are considered while observing the changes overtime and making it for useful for the researcher to attain the data developments over a long period of time (Saunders L. a., 2009) but such approach is not practical for the overall objectives of this study.

3.8 Data Collection:

Overall study was conducted utilizing the qualitative research method to understand the trend of decentralized digital identity solution and role of Blockchain with the help of industry experts. Semi-structured interview were conducted over the audio/video call to gather the data.

Researcher was happy to adopt the choice of conducting interviews for collecting the primary data to sync with the nature of the exploratory study and fulfil research objectives.

(Saunders L. a., 2009) suggests that an interview can establish a powerful and quality discussion between two or more people and advises a number of interview techniques can be considered to achieve the overall objective of the research. Unstructured interviews gives the opportunity to respondent to talk freely to explore the study whereas structured interviews revolve around quality discussion to avoid any kind of bias and collect quantifiable data to draw relevant findings (Saunders L. a., 2009)

Semi-structured interviews provides the interviewer opportunity to have limited open discussion along with specified questions to make sure certain topics are mandatory covered along with some new findings in each interview. This helped the researcher to select semi-structured approach as primary data collection method for this study.

After selecting the respondents and understanding their work background, researcher drafted certain similar questions for each respondent and added few more during the interview based on the feedback received from the respondent to participate in the discussion and gather something unique from each interview.

Within limited timeline, researcher made sure that semi-structured interview format did come up with valuable findings and area of research study was discussed to a full extent. Researcher drafted a schedule and interview guide for the interviews to be conducted only once and appropriately to avoid requirement of repeating the same process again with each candidate.

Interview guide helped the researcher to showcase appropriate amount of professionalism and agility and helped with each interview. Since most of the candidates were on senior positions and had limited time, researcher made sure that their time was utilized in a professional manner and healthy participation to capture their inputs.

Audio/video recording of the conversation in accordance with compliance and data guidelines is an important practise and main source of analysing the data. All of the respondents were informed about their rights and their permission was requested before starting the discussion.

3.9 Analysis:

Transcripts of semi-structured interviews already had presupposed design from the interview questions and this structure guides to undertake data analysis techniques.

Transcribed data was continuously checked against the audio/video recordings and repeated examination of interview transcripts helped to allocate the data into themes and findings.

Literature review studies gave structured idea of the study and transcripts of the interview helped the researcher to utilize approach to data analysis. Transcripts allowed the researcher to understand subjects in scientific manner and this way the collected data linked with literature review and research objectives and brought coherence in the overall research.

The Thematic analysis provided the researcher a deep understating of utilizing the qualitative data and meaning to semi-structured interviews of the respondents.

Braun & Clarke (2006) suggest that it is the first qualitative method that should be learned as 'it provides core skills that will be useful for conducting many other kinds of analysis'. A further advantage, particularly from the perspective of learning and teaching, is that it is a method rather than a methodology (Braun & Clarke 2006; Clarke & Braun, 2013).

3.10 Ethics:

Ethics plays central role for undertaking meaningful and effective research. As such, the ethical behaviour of individual researchers is under unprecedented scrutiny (Trimble & Fisher, 2006).

While conducting research, ethics guide the researcher to maintain high and positive standards of behaviour and about the rights of candidates who have participated in the research work (Saunders L. a., 2009). People are centric to the area of research conducted in business areas which makes it inevitable to abide the ethical standards (Burns, 2008)

Privacy of the candidates and their concerns about identities is a sensitive issue which can't be revealed without their prior consent. Therefore, while conducting the audio/video interview, researcher made sure to take the consent as first thing. As stated by (Burns, 2008) the participants' rights are: the right to voluntary participation, the right of safety and freedom from harm, the right to be informed, the right to privacy and confidentiality.

Researcher made sure to clarify to the candidates about the overall objectives of the research, aim behind collecting this data to come up with new findings and confidentiality of the collected data which will only be utilized for research purpose and not to be shared further with any third party.

Research study has been designed in such a way that it justifies the ethical standards to all the involved parties and the researcher made sure no such unethical approach was utilized which could bring up the sensitive issue.

Even though the research topic doesn’t require any individual to discuss their personal or organisation’s internal information still researcher made sure that non-maleficence was central to the overall to avoid any ethical issue.

Considering the theme of the research topic, respondents were open to the idea of sharing their identities rather than being anonymous but the researcher did mention about the rights of respondents to remain anonymous and their request would have been respectfully acknowledged.

Ethical standards also apply while analysing the data captured from semi-structured interview to ascertain that the derived results are originating from discussions and are valid. Analysed data was reported in systematic manner and each interview was transcribed to understand the trends and draw out the valuable findings.

3.11 Limitations:

Over the course of dissertation some sort of obstacles did occur which deviated the completion of study from its original plan.

Since the area of Blockchain in itself is new to the industry and the technology is still evolving with limited number of resources available to conduct literature review, researcher had to rely on large number reports published by few organizations working in this area. Also, the concept of decentralized digital identity is still a term and several decentralized digital identity management solutions are being developed for operational use. Researcher had to link the attributes of the Blockchain technology to critically review the literature and come up with a potential solution case for implementing decentralized identity in public sector utilizing Blockchain based smart contracts, identity management solution and smartphone which can only be implemented with technical skills.

Similarly, researcher faced several issues while searching the potential candidates for semi-structured interviews and it became inevitable to accept the fact there is acute shortage of experienced candidates. LinkedIn was utilized to search several candidates which had mentioned keywords Blockchain, Digital Identity or wallet, decentralization, Blockchain developers, Hyperledger, cryptography etc. and randomly connection request was sent to over 100+ results.

LinkedIn allows to conduct certain number of search on its platform for free and paid subscription is required to continue the search. Researcher didn't opt for this facility as it was an expensive approach and had to limit within free search criteria's.

LinkedIn provides the facility to send personal messages to the accepted connections and it was the only option to reach out to the candidates with a brief message about the research study and to know their interest. Similar brief message was sent to over 60+ connections and only 10 responded back with their interest while others either did not respond back or mentioned the reason for not participating.

Another limitation was regarding the discussion carried out with candidates having less than 5 years of experience which could have affected the overall conclusion of the study. Recordings revealed that most of the information shared by certain candidates generic in nature or repetitive which led to elimination of these interview for analysis purpose and rely completely on interviews conducted with high profile candidates.

3.12 Conclusion:

Research methodology section described the methods undertaken by the researcher to conduct the overall research and these methods heled the researcher to understand the nature of the study to answer the research question and objectives. Adopting the combination of Interpretivism and Pragmatism as research philosophies helped the researcher to understand the reality of decentralized movement and adoption of Blockchain technology for developing decentralized identity management solutions.

Researcher applied the inductive approach to conduct the semi-structured interviews as research strategy. Interviews were conducted in a professional manner over audio/video conference with equal participation of the researcher to probe questions based on the ongoing discussion.

To respect the rights of the respondents, consent before starting the interviews was requested from each candidate and the overall aim of the study was also shared. Researcher did mention about the confidentiality of personal data and maintained high ethical standards.

Nevertheless, several factors such as time and limited number of highly experienced respondents resulted in less number of overall quality interviews than originally expected. Still it was possible to draw quality analysis and come up with several futuristic themes and findings.

Chapter 4 – Data Analysis & Findings

4.1 Interviewees Background:

Stan Nazarenko, CFA - Co-Founder & CEO @ Piprate

Stan Nazarenko, CFA is the co-founder and CEO of PipRate; a Dublin based company that builds permanent digital footprints of real world objects as an enabling platform for a wide range of applications from on-demand insurance and IoT data markets to recycling and green economy. Stan is a technology leader with 20 years of experience in the areas of reinsurance, quantitative finance & risk management. He is also a member of Open Knowledge Ireland, a local non-profit organisation which uses advocacy, technology and training to unlock data and enable people to create, manage and share knowledge. He is part of Tech-Ireland advisory board on Blockchain with Tech-Ireland. TechIreland.org is a not for profit whose mission is to become the definitive source of data and insights on Irish Innovation globally.

Eoin Connolly – Technology Director @ ConsenSys

ConsenSys develops solutions on a particular Blockchain called Ethereum, which is an open-source software platform for building applications, such as payments services, tools for carrying out know-your-customer checks and Digital Identity wallet.

Eoin has around 21 Years of experience with several organisations like System Dynamics, Deloitte Blockchain Lab and currently working as technical director with ConsenSys in Dublin. He is software developer by profession and started his journey with Blockchain Identity solutions from 2016 in Deloitte EMEA Lab and currently leading the development of Decentralized Digital Identity product of ConsenSys which is known as "uPort".

Zia Khan - Co Founder @ Independent Consultant

Zia has around 20 years of experience with organisation such as IBM India, Microsoft, HCL, Ricoh where has was COO for IT services division and now an independent consultant. He described himself as an Idea, Tech and Growth Evangelist, using cutting edge technologies in sales and technology. Building solutions with Blockchain, IoT, AI and Bots. Helped organisations develop solutions, strategies, sub-divisions, and even separate companies through this approach.

Dr Jane Thomason – CEO @ Blockchain Quantum Impact

Entrepreneur, social capitalist, experienced CEO, energetic change maker and thought leader in the applications of Blockchain technology for social impact. A regular commentator and global conference speaker on Blockchain and social impact. Adviser to several Blockchain start-ups with applications that solve global problems, currently working with collaborators to co-develop Blockchain POCs in several emerging economies. Hackathon judge and mentor at London Blockchain Week, London Fintech Week, Consensys Blockchain for Social Impact Coalition Hackathon and EOS Hong Kong. A passionate advocate for the education and empowerment of women and #WomeninBlockchain. Dr Thomason is a Global Ambassador and Advisory Board member of the British Blockchain Association and Global Adviser on Digital Transformation for Abt Associates, and section Chief Co-Editor Blockchain for Good: Frontiers in Blockchain. She was named in the Top 10 Digital Pioneer Women and was awarded the UN Decade of Women Quantum Impact Champion Award on International Women's Day in New York. In 1999 she founded and international development company which merged with Abt Associates in 2013. She then led the growth of Abt Australia to achieve a tripling of revenue and diversification into governance and women's empowerment across Asia and the Pacific. Jane has been a leader of a wide range of development programs globally, regionally and in Australia, Asia and the Pacific. She has also held senior appointments including Director of Women's Health, CEO of the Royal Children's Hospital, and Chairman of the Wesley Hospital Board.

Stuart Wilson - CTO @ Blockchain Advisory UK

Stuart is an IT professional who has worked for around 20 Years with several organisations leading the highest position as Vice – President Technology @ American Express and now working as Guest lecturer at Warwick Business School - delivering lectures on Fin-Tech Innovation. He became involved in Blockchain in 2014, and worked with San Francisco start- ups on concepts which lead to Comakery.com, a flexible token platform that rewards freelancers for their collaboration on project work.

Samrat Kishor – Manager @ Accenture Strategy India

Samrat is a technology consultant with a decade of rich experience working with firms like GT, KPMG, Deloitte and presently Accenture Strategy. He advises businesses on innovative business models driven by technology and design thinking. He is a strong believer in open innovation and is presently contributing to Blockchain technology as a member of NASSCOM's Blockchain SIG. He is adept at spotting technology trends and has successfully predicted many technology applications to new business models.

Samrat is also a mentor on the Start-up India Program and Atal Innovation Mission, both initiatives of Niti Ayog - Government of India. He is currently mentoring 2 start-ups and nurturing 2 innovative ideas through these initiatives. He has a knack for influencing young minds and shaping their thoughts in a way that they are able to think, reason and debate on a variety of topics outside of their regular curricula. He enjoys presenting real-world concepts in simple ways and has impacted over 2000 students from diverse backgrounds.

4.2 Data Collection:

Based on the feasibility of respondents, researcher conducted both telephonic as well video conferencing interview with a series of questions. Each interview lasted on an average of 30+ minutes. Researcher focused to make it a quality discussion by involving deeply in conversation and asking question which were not planned earlier. This resulted in a series of 10-12 questions and with few respondents it reached up to 15.

Each interview recording was analysed same day to identify the common themes and patterns from the data and similar data captured from different respondents was extracted to avoid duplication.

4.3 Data Analysis:

Researcher followed the thematic process to analyse the overall data from the recordings. An inductive way to code the data into several common themes as directed by the data was followed. Since respondents had no issues to reveal their identity, researcher didn’t make any changes with the identity.

Researcher made a rough data sheet after listening to recording to understand the patterns and ordered these patterns into categories which led to identification of themes.

4.4 Findings:

4.4.1 Centralization Focus:

Researcher had focused to select respondents from different backgrounds to gain overall experience of different sectors and markets. Eoin who is s solution architecture with ConsenSys discusses following about Centralization:

"I am not a massive fan of Centralized Digital Identity Management Solution since they act as central honey pots for data facts and leads to abuse of data. Current solutions give more power to the Organizations rather than an individual" **(Eoin Connolly)**

"Natural progression from pre-internet era which are not successful in current landscape of cyber risk and forward looking. It is the only choice for most of the organizations unless they are ready to move forward from it to bring disruption." **(Stan)**

The need to establish a direct relation with individuals, providing untapped support and trust led to the ever growing acceptance of such solutions so far:

"There is still lack of Digital Identity and identity management solutions being used whether centralized or decentralized and now since the ongoing hacking and attacks on personal information, citizens/individuals are particularly asserting to preserve their personal information, financial data and being receptive to disclose the personal identity using the existing identity management solutions." **(Dr Jane)**

"Dependency on a single organization to manage the personal information and communicating with information owners on how their personal data is being used other than the original purpose. Several organizations are not even sharing the information on data loss due to security breach until the

> *personal information of an individual has already been misused. It does lead to a natural sense of worry and conduct of mistrust."* **(Stuart)**

The underlying motivation for utilizing centralized identity management solutions were partly influenced by the absence of any other alternative and only choice to consult their clients in order to strengthen the security of such systems:

> *"Centralized identity management solutions do work well but always prone to data integrity, audit challenges, unavailability for authentication at several intervals and always considered to be replaced by any other highly secure and robust technology".* **(Samrat)**

Given the maximum use of centralized identity management solutions, respondent had a different viewpoint than others and how it can be utilized for scalability by managing both internally and externally:

> *"Most of the organizations and public sectors (including world's largest database Aadhar) has utilized the benefits of centralized digital identity management solutions but due to the basic fact these systems are 'single point of failure' leading to disclosure of financial as well as personal information shred on several platforms. When manager internally (by the identity providers) and externally (by individuals not sharing information on spam e-mails, accessing fake links etc.)"* **(Zia)**

4.4.2 Decentralization Pathway:

Each respondent had different view on the future towards Decentralization and discussed about different solutions which are being currently developed:

> *"There are a number of solutions in process and one of them "uPort" on which I am directly working on within ConsenSys. They are yet not fully ready for the individuals since there is need for a reason to exist, need of capability and requirement of partners to attach value but they do give a great capability back to the hands of an Individual to enhance privacy and save personal data from the hands of an organization".* **(Eoin Connolly)**

While designing their system, respondent had the choice to opt for either centralized or decentralized identity management system and with a fair research, they decide to choose the decentralized model to bring more transparency and trust in their solutions:

> *"With much easier on-boarding choice for customers (avoiding the same steps of registration and authentication) and removing the friction between service providers and customer to improve the services."* **(Stan)**

Some respondents based on their interactions with government of certain countries came to suggest that the benefit of decentralized identities is to strengthen the relationship between both citizens and service providers:

> *"Future is to have a unique identity which you earn and can use for a variety of things. Traditional players will for sure resist to accept it but with time successful trials and acceptance by organizations and government institutions, this will bring disruption in the existing model."* **(Dr Jane)**

> *"You as an individual will be the owner and controller of your identity and personal data operating in a fully self- sovereign way without any individual third party to control or access it. Decentralized solution like zero knowledge proof based on cryptography, which can prove an individual's age (18+), gender etc. for without asking their D.O.B will be the pathway for secure and trusted transactions."* **(Stuart)**

According to the respondent, decentralized identity will do more than just providing a smart ID in the hands of an individual. They suggested the ongoing implementation of such IDs for several seamless benefits:

> *"Integration of existing identities of a particular system with new agency would tend to become seamless without any major technical challenges on decentralized systems. Identities will be recognisable beyond borders e.g. international travel platforms like sea where an individual can verify himself/herself without having to show a proof of paper or prove his status of residency etc."* **(Samrat)**

The focus on decentralization was seen as parallel framework by this respondent since technology never dies, it just takes years of time to replace the legacy systems and overcome limitations:

> *"Decentralization might not so early impact the market segment but will substitute the centralized solutions by providing option to the individuals and organizations and run parallel to each other. Once the maturity of decentralized identities grows, it can become the reliable solution with alternative and advantageous choice".* **(Zia)**

4.4.3 Blockchain - Technology Effect:

The respondents view towards Blockchain were driven largely by their direct/indirect involvement in pilot projects based on Blockchain and what could these project offer:

> *"Blockchain is all about Digital storage system which is not controlled by any one authority rather is completely decentralized. Blockchain like "Ethereum" which is global, publically available and are sensitive persistence which means an individual with same cryptocurrency can transact on same platform without the intervention of any third party by just setting up a Digital Identity. Attributes like explicitly owned by Individual, non-temperament and 24*7 availability without any support makes it unstoppable".* **(Eoin Connolly)**

Opportunity to establish a shared consensus on how the identities should be used was considered as one of the transformative factor:

> “*Blockchain in itself is very young & one of the most appropriate solution right now due to its attributes of consensus mechanism and easy to manage. Depending on the Global appetite and establishment of global network, Blockchain will evolve with new solutions*.” **(Stan)**

Respondent saw Blockchain as a transformative technology in relation to data privacy and prone to sybil attacks and even share the insights on overcoming the limitations of existing challenges:

> *“Decentralized nature of the technology makes it next to impossible to hack the data since a minimum of 51% of network needs to be hacked to breach the personal information. Since the data is cryptographically tagged and in case of breach only cryptographic hash will be revealed rather than the data of an individual. There are new platforms being developed right now to overcome the limits of 51% attack which will make it more secure and fast.”* **(Dr Jane)**

Opportunity to rethink how communication and transactions can be scaled without involving any third party was seen as the transformative attribute with Blockchain:

> *“Communication between two individuals to transact without any third organization orchestrating between can only be filled with Blockchain. With solutions like Smart contracts linked with the decentralized identities, the overall progress of the activities and the fulfilment of conditions can only be possible with Blockchain.”* **(Stuart)**

Blockchain offers access to improvise the scale of applications which was so far not possible with other technologies:

> *“Interoperability which is the new evolution within Blockchain lets two Blockchains connect with each other and facilitate the transaction of digital identity owners.*
> *Similarly, alterability is another innovation within Blockchain which brings the possibility of auditing concurrent system on high value transactions of any organization which was earlier not possible and later on would require tracing back to original papers.*

> *As of today only 2% of the organizations use Blockchain as an evolving technology but 2019 will be dawn of many Blockchain based identity management applications e.g. Smart Id. “* **(Samrat)**

According to this respondent, Blockchain technology provides more than just technical advantage by bringing the opportunity to trace back the integrity of data in its real form with availability to parties involved in certain agreement:

“Blocks within a Blockchain are tamper-proof and to alter a single block would require the permission from whole network participants along with mandatory changes in whole chain. This leaves the audit trail, reason for making changes with time stamps brining forward the transparency as a mandatory attribute.” **(Zia)**

4.4.4 Technical Alternatives:

All of the respondents had common viewpoint which either they have gained from their development works or by proving the consulting services to their clients:

> *“Blockchain is not the ultimate solution. Individuals can carry their own digitally signed identity and present to organizations to add to their systems. Blockchain gives the path to let this identity be publically available. Alternatives like hash-graph, pseudo Blockchain, semi-private Blockchain can be utilized but they all are only successful when the framework of Decentralize Blockchain is utilized”.*
>
> **(Eoin Connolly)**

This focus resulted in to focus certain similar technologies but they couldn’t stand alone to provide large scale transformations:

> *“There are several proof of concepts based on emerging technologies within web 3.0 like Tangle, hash-graphs and several mesh technologies using cryptographic algorithm but they all are based on similar principles of Blockchain. “****(Stuart)*****`**

Traditional technologies did manage the Digital identity Management solutions so far but Blockchain and its alternatives offered access to scaling applications:

> *"Blockchain in itself is a game changer with no other technology at current to provide same level of technical advantage. But future is quantum computing with which Blockchain's features like cryptography and algorithm are going to become much more advance and will be utilized for developing far better solutions."* **(Samrat)**

Technology is not meant to stagnate the growth of industry rather come up with opportunities and new models to bring efficiency and eliminate obstacles:

> "with the emergence of technologies like GPU & TPU by Google, Blockchain can overcome the challenge of speed issues depending on several factors. Overall Blockchain has its own properties which other technologies were not able to provide and utilizing with other technologies makes it more useful and mature to develop any kind of solutions." **(Zia)**

4.4.5 Public Sector Viewpoint:

All respondents were of same viewpoint to utilize Blockchain based solutions in public sector with some kind of initiatives:

"There is difficulty to maintain a gigantic centralized identity management solutions by the government since it create the confusion between what an individual wants to do and what the public sector wants to do for them. In coming 5-7 years, public sector might start utilizing such services by citizens using their private keys and public sector their Public Keys to cater services like social welfares etc." **(Eoin Connolly)**

Moving towards accepting decentralized identity management solutions should be well planned and accepted as part of governance model:

> *"There has to be a global operational network for e.g. Ethereum before planning to accept such solutions. Besides, governments are lagging behind in more innovative sector of the economy and need to step forward to function with innovative ideas and serve the citizen.* **"(Stan)**

Given the concern over knowledge issues, respondent had different view about the post implementation issues which can be overcome with large scale of knowledge sharing programmes:

> *"Knowledge is the biggest weakness since governments don't have no knowledge about such systems and would need a high degree of education reforms. Scalability of transactions on a country level when compared to a city for existing Blockchains platforms is very slow. Blockchain like EOS.IO are claiming to conduct millions of transactions per second which can be utilized by public sector to provide services."* **(Dr Jane)**

> *"Public sector involvement begins the minute anyone is born and entitlement of identities is a process which carries on for a long period of time. There are different identities citizens rely on like passport number, driving license number etc. One identity for one individual along with the self- ownership can avoid many crisis."* **(Stuart)**

Looking at the overall scenarios in current public sector processes, there is need to establish a direct relationship between citizens & trust and delivering the strategy to eliminate fraud, inappropriate entitlement and open to auditability:

> *"By utilizing Smart IDs (decentralized IDs) based on Blockchain for citizen and their own employees, there will be straight elimination of fraud. Since, most of the fraud happens due to the inappropriate entitlement of public services. Entire public sector system will become much transparent & agile by eliminating the duplicate identities from multiples databases and leading to next level of governance by opening the public sector records open to citizens for audit which is currently not happening anywhere in the world."* **(Samrat)**

The decision to choose decentralized identities is not a forceful choice for public sector rather an opportunity to bring back the trust in overall governance:

> *"Entitlement of services can always be found on papers and digital records which doesn't happen in reality. Services like land records are always subject to dispute and this has already been resolved with successful completion of pilot projects. Combinations of decentralized digital ID, smart contracts and unalterable blocks are solution of Blockchain technology and are opening new models for public sector."**(Zia)***

4.4.6 Public Sector Challenges:

There need to be strategic planning before rolling out such solutions with the emphasis on looking at common platforms.

> *"Adoption is the first and foremost barrier since there is none widely accepted decentralized identity management platform supported for public sector services and the existing market force is not ready with such big platform."* **(Eoin Connolly)**

Understating the limitations of existing models and using innovative designs to overcome it are the features of success:

> *"Maturity, security of the solution, stability, accessibility and complexity of the roll outs are the few which needs to be tested during the pilot phase before making them available to citizens for public services."* **(Stan)**

Speed of the smaller and developing nations was seen as added advantage and a role model governance for larger and developed nations:

> *"Public sector of developed countries are going to be much slower due to existing legacy system, process, concerns of the citizens with new process and owing a single identity only when compared to developing countries where citizens don't yet own a digital identity and brining the new system in itself will be the first and the most secure choice for the citizen to avail public services."* **(Dr Jane)**

It all starts within the system and a good intention to eliminate the malpractices combined with technology can overcome majority of challenges:

> *"Public sectors are always subject to suspicions since the intent of services providers is to make money for personal advantages rather than serving the citizens, Intent of senior officials not to implement such technologies will bring back the fraud and corruption within the system."* **(Zia)**

4.4.7 Public Sector Reforms:

The true nature of Blockchain based decentralized identity management solutions need to be fully understood:

> *"Citizens can move from using Gmail & Facebook as their identity to log on to utilize public services (varies from country to country) and will provide only minimum required information to access the services. Example of it in Ireland right now is "MyGovID" MyGovID gives you safe, online access to Irish government services. Create a basic account for instant access to simple services or verify your account to unlock all MyGovID services like Revenue Income Tax service, My Welfare and health portal etc."* **(Eoin Connolly)**

This leads to utilize technology to ease the services and potential cost benefits:

> *"General cost of providing public services will go down. Having public sector involved in the decentralized identity management solutions is critical to bring trust in the overall system and government approved identities would be easily acceptable to perform commerce transactions leading to issues with confidence will improve. Citizens feel to share as little information as possible to government whereas government wants to collect as much information about their citizen as possible. Decentralized identity solutions will bring shift of power and balance the paradigm."* **(Stan)**

> *“With such solutions in practise, citizens who don’t own a digital identity (around 1.*5 Billion in the world) can own an identity and participate in the economic activities of the country and can receive public sector services.” **(Dr Jane)**

Respondent were of the perspective that public sector should have a strategic focus on bringing audits to the common citizens:

> *“Proper audit trail of every single transaction, tamper proof digital identities and data associated with them, less opportunity for hackers to breach the systems.”* **(Zia)**

4.4.8 Global Framework:

Recognising the relationship of citizens with their government as a mean of delivering the right and secure solution was highlighted by most of the respondents:

> **(Eoin Connolly)** *“uPort is directly working with the canton of Zug in Switzerland to launch a pilot project of Digital Ethereum identity platform. Zug will offer a variety of services through uPort, such as e-signatures and parking fee payment, and will test out an e-vote during the first phase in spring 2018. According to the mayor of Zug, Dolfi Müller, the pilot conforms to Switzerland’s socio-technological interests. We want a single electronic identity – a kind of digital passport – for all possible applications. And we do not want this digital ID to be centralized, but on the Blockchain. Our role is not to store personal information, we only examine the identity of a person.”* (Cummings, 2017)

4.4.9 Commercial Opportunities:

The commercial impact of decentralized digital identity solutions as a transformative solution doesn't only affect the public sector but also every entity which is based on Digital identity:

> *"Every sector can be impacted by decentralization. Once the identity and money both are decentralized, every other sector is possible. Once the technology matures through the required output, even social networking sites like Facebook and Twitter can also be impacted with this."* **(Eoin Connolly)**

Dr Jane had direct involvement with the government of Indonesia to suggest Blockchain as digital identity management solution which is still under consideration. She suggested "Child Trafficking" which is already in process to bring under control using Blockchain.

> *Announced during the Humanitarian Blockchain Summit in New York on Friday, the pilot involves participation from the United Nations Office for Project Services (UNOPS) and the United Nations Office of Information and Communications Technology (UN-OICT), a press release indicates.*
>
> *Storing digital identities on a Blockchain, the release states, provides a "significantly higher chance of catching traffickers." Additionally, securing identity data on an immutable ledger will make trafficking attempts "more traceable and preventable."*
>
> *According to Dr. Mariana Dahan, co-founder and CEO of WIN, "invisible" children under the age of five and who do not possess a birth certificate are at "risk" and can fall into the hands of child traffickers. These children are often missed by social programs offered by governments or development agencies.*
>
> (Sundararajan, 2017)

Chapter 5: Discussion:

Introduction:

This section will draw insights to discuss the findings from primary research and literature review. Common themes which came as outcome of primary research findings are analysed together with ideas, themes and several common topics from the literature review.

Objective 1: Determine the impact of current identity management solution on an individual's privacy

5.1 Centralization Focus:

The literature reveals a variety of information around digital identity management solutions with which most of the organizations (public/private) are engaged to provide services. Common viewpoint from most of the scholars is the need to develop an alternative to centralized IDM solutions and the findings are fully supportive of this view with all of the respondents even Dr Jane suggesting that still there is lack of digital identities being used at all in many parts of the world.

The literature from both private and public sector specify massive utilization of centralized digital IDM as having no alternatives so far to replace. These are rooted as the first choice to consider including the usage of legacy technologies which are quite known and easy to tamper. However, the findings suggest that such solutions were ready to be replaced by any other highly secure and robust technology. It may be clear from the literature review that several IDM architects had shared principles on how to develop and maintain a digital identity from user perspective but view form findings suggest that newly designed solutions were still giving more power to the organizations rather than individuals.

Within literature there has been discussion on principles of Self-sovereign identity by Christopher Allen which defines the ideal solution for a digital identity whereas one of the respondent (Eoin) mentioned that centralized IDM solutions couldn't accommodate these principles hence giving the power back to organizations to misuse an individual's private information to earn wealth and profit.

What is clear from the literature is that central IDM create opportunities for organizations and service providers to act as "critical mass" and force individuals to act within such forces. Acting as a critical mass leads to emergence of mistrust, insecurity, inappropriate distribution of services and abuse of data. Both respondents and literature are in coherence that adopting to centralized IDM has always been the only choice unless the alternatives could be available.

Objective 2: Identify the advantages of developing decentralized identity management solutions and progress so far?

5.2 Decentralization Pathway:

Literature reveals that generating revenue, increasing economic perspectives and reducing cost are the value proposition of identity management solutions. What the real finding reveals that the current focus is to act upon lessons learnt from centralized attacks and a lot of industry experts have already started working to develop the decentralized digital identity solutions.

Literature advocates the realistic view of using digital identity and IDM should be minimization of Identity Information collection and its use with a lot researcher stressing on to let users be the owners of their identities. What the findings suggests that there is an on-going development of solutions like uPort, Blockverify, Cambridge Blockchain LLC and Evernym etc. have already developed the pilots of decentralized digital identity wallets which can used by individual on small platforms now and with its acceptance on bigger platform, they will derive the industry. Finding clearly suggests that decentralized solutions will give identity ownership back to the hands of an Individual to enhance privacy and save personal data from the hands of an organization.

Currently, the literature reveals that most of the organisation have no alternative than to use centralized digital IDM which makes the user to register at multiple places with repletion of same steps. One of the respondent (Stan) while starting up his venture suggested that they did a lot of research before designing the product and concluded to utilize the decentralized identities to give more power back to customers.

All respondents shared in detail on the changes that came after adopting decentralized version of identities and there was a common understanding which was learnt with experience that decentralization can make a huge impact on whole value chain of the business and individuals who have been the victim of identity data loss.

Objective 3: Describe the fundamental technological advantage of using Blockchain technology to develop decentralized digital identity management solutions.

5.3 Blockchain - Technology Effect & Alternative:

Literature identifies that Blockchain technology in itself is very young and at early stages being utilized mainly for cryptocurrencies. All respondents had the common view that Blockchain will not only just supply technology advantages rather defining the industry, deriving adoption and bringing the era of www 3.0.

Literature reveals a variety of technological attributes of Blockchain technology to develop decentralized IDM solutions and the findings suggests that there has been more development on technological barriers to develop scalable solutions.

- **Interoperability:** Current literature doesn't mention the attribute of connecting different Blockchains to communicate/share the data with each other on secured network. Samrat one of the respondent mentioned and suggested to review the part of Interoperability. There are different networks within Blockchain ecosystem e.g. national governments, specific financial institution, and certain healthcare institution and required data on individual chains couldn't be shared or transferred which made it warehouse of individual chains running on separate Blockchains. Interchain communication could lead to scaling solution for the overall ecosystem. This led to the development of products like Blocknet, cosmos, aion, lamden, ICON etc. are few projects who are developing and few have already released the beta version successfully.

- **Ecosystems:** Literature suggests that Bitcoin and Ethereum are the two Blockchains being used for transactions. Both of which have technical challenges like capacity limited to 7 & 25 transactions per second. Several respondents were not in favour of these facts and shared their insights on the emergence of new ecosystems like evernym (thousands of Transactions per second), Ternio (claiming to make 1 Million transactions per second) fully decentralized and on-chain which means thousands of decentralized digital identities can utilize these platforms.

- **Maturity**: The concept of decentralized identities on Blockchain due to its properties like (immutability, decentralization) is very interesting since research claims it is tamper-free but there are barriers to achieve the overall maturity. Blockchain in itself will take long to prove its attributes and as discussed in literature review it requires further improvements such as scalability and performance. However, maturity doesn't confine within technical aspect rather grows with business aspect as well. According to PwC, globally only 24% financial institutions are aware of this technology and are working to link decentralized digital identity with daily activities of consumers such as KYC, stock trading, online payments etc.

- **Regulatory consideration:**

Government regulators and policy makers are striving to find measurements to consider and implement new disruptive technologies to make sure that safety criteria, availability and usability are up to industry standard. Blockchain to be considered for decentralized digital identity requires research and mechanisms to control the impact on those criteria. Currently, there is no standard regulatory for Blockchain implementation for e.g. there are regulations on big data in several countries but none for Blockchain.

Decentralized identity is yet a concept and future reality. Researcher tried to explore the alternative technologies from industry experts who are working to develop these solutions. All of the respondent were of the same view that attributes of Blockchain only meet the requirements of decentralized world and with the emergence of quantum computing, the capabilities of Blockchain based solution will upscale.

Objective 4: Describe the usage and impact of decentralized digital identities in Public Sector.

5.4 Public Sector implication:

Literature clearly defines that public sectors are maximum utilizers of centralized digital identity management solutions and always prone to attack and information loss. Entitlement of first and life-long identity to citizens is provided by public sector all over the world e.g. Passport, driving license etc.

World's largest biometric ID system 'Aadhaar' which has 90% enrolment of India's population was compromised due to cyber-attack. Reports suggest that "in a few years, attacking UIDAI data can potentially cripple Indian businesses and administration in ways that were inconceivable a few years ago. The loss to the economy and citizens in case of such an attack is bound to be incalculable."

76% of local government organisations suffered a cyber-attack in the 2017 itself. Although all of the organisations surveyed stated no data was stolen and no ransoms were paid, it's vital that local government seeks to adopt robust solutions to mitigate cyber security risks both before and after impact but citizens Confidence in security is lacking (Kezia, 2018)

Findings suggest that in today's era only Blockchain based decentralized identities can transform the public sector. Global Blockchain networks are being already utilized to develop decentralized identities which will give more power in the hands of citizens. Innovation of Smart IDs which is already in progress will bring the next level of governance by making the system more transparent.

Blockchain based decentralized digital identities can hold the record of personal information on a shared distributed ledge which means the control of digital public services identity will come in the hands of individual rather than the government 'a required transition in data ownership'.

Based on discussion with respondents and findings, here are few opportunities and challenges:

Opportunities	**Summary**
Transparency	Visibility of data. Transaction conducted by any public servants remain within nodes and are visible to citizens with complete overview
Controlling fraud and manipulation	Changes within ledgers will be difficult to make as blocks are unalterable and information is stored within multiple ledgers and attempt to change will be noticed promptly
Reducing corruption	Storage in distributed ledgers allows for preventing corruption. For example by storing landownership in a BT and having clear rules for changing ownership which cannot be manipulated.
Trust emergence	Immutable records and verification of transactions at several nodes increases the trust in citizens.
Transparency and auditability	Being able to track transaction history and create an audit trail. Also by having multiple ledger which can be accessed for consistency.
Increased control	Consensus mechanism to conduct transactions increases the control.

Clear ownerships reduced costs	Ownership will move from single authority to citizens involved in the network and the cost of providing services to citizens will decrease since less manpower will be involved.
Increased resilience to spam and Sybil attacks	Technology design itself will prevent attacks saving funds being given for ransom now a days.
Integrity and quality of data	This result in higher data quality. Information saved on network is the result of consensus voting in real time which leads to higher quality of data.
control on human errors	Verification and access grants will be automatic which can reduce the human errors.
Availability of information	multiple storage of data and direct access to entitled digital IDs makes the information easily available,
Privacy	Users have the ability to transact without interacting and only using the combination of public/private key to maintain their privacy.
Reliability	When all the parties agree, consensus mechanism will alter the data placed at multiple nodes.
Resilience	Resilient to malicious attacks
Security	Encrypting the data and strong it at multiple nodes makes it impossible to hack.
immutability	since the data is stored at multiple places it becomes hard to edit or make changes on the data without making changes in all the nodes.

Challenges	**Summary**
Knowledge	Public sectors lack knowledge about latest innovations and implementation time frame is very long.
Adoption	Adoption of such new identity management solutions is barrier since such solutions are yet not widely accepted.

Maturity	Developers need to realise such system would cater the citizens of a country not organization. Pilot phases have to successful before final rollouts.
Personal Intent	Intent of corrupted officials can hinder to accept such innovative solutions.
Developed Nations	Developed countries already have stabilized processes and sudden change might not be accepted whereas developing countries can choose decentralized identities as first choice.

Chapter 6: Conclusion and Future work:

6.1 Summary:

Blockchain technology is an innovative approach to structure and manage data for auditing, tracking and tracing. Blockchain architecture is well defined to develop solutions to track the ownership of digital, physical and virtual assets using the combination of public and private key infrastructure. Blockchain features are being utilized to develop decentralized digital identities for the collaborative environment where individuals can own the data, personal information linked with their identity. This work attempts to discuss a new identity management solution type since today's world is highly dependent on centralized authorities. This study evaluates the existing identity management systems & their principles and how can new technologies be utilized to develop decentralized identity management systems. With this new solution, citizens/individual can define their digital identities on their own terms, share only limited and required information with governing bodies. This identity management system differentiates from traditional identity management system in following ways:

- All transactions linked to decentralized digital identities are distributed to participants within a defined network and this network will not accept any kind of falsification or data modification even the owner of the databased (DBAs) can't amend the data once recorded. When compared with traditional system, system administrators have full control of the database and personal information is out in their hands. However, with decentralized systems the data within networks is completely decentralised and immutable.

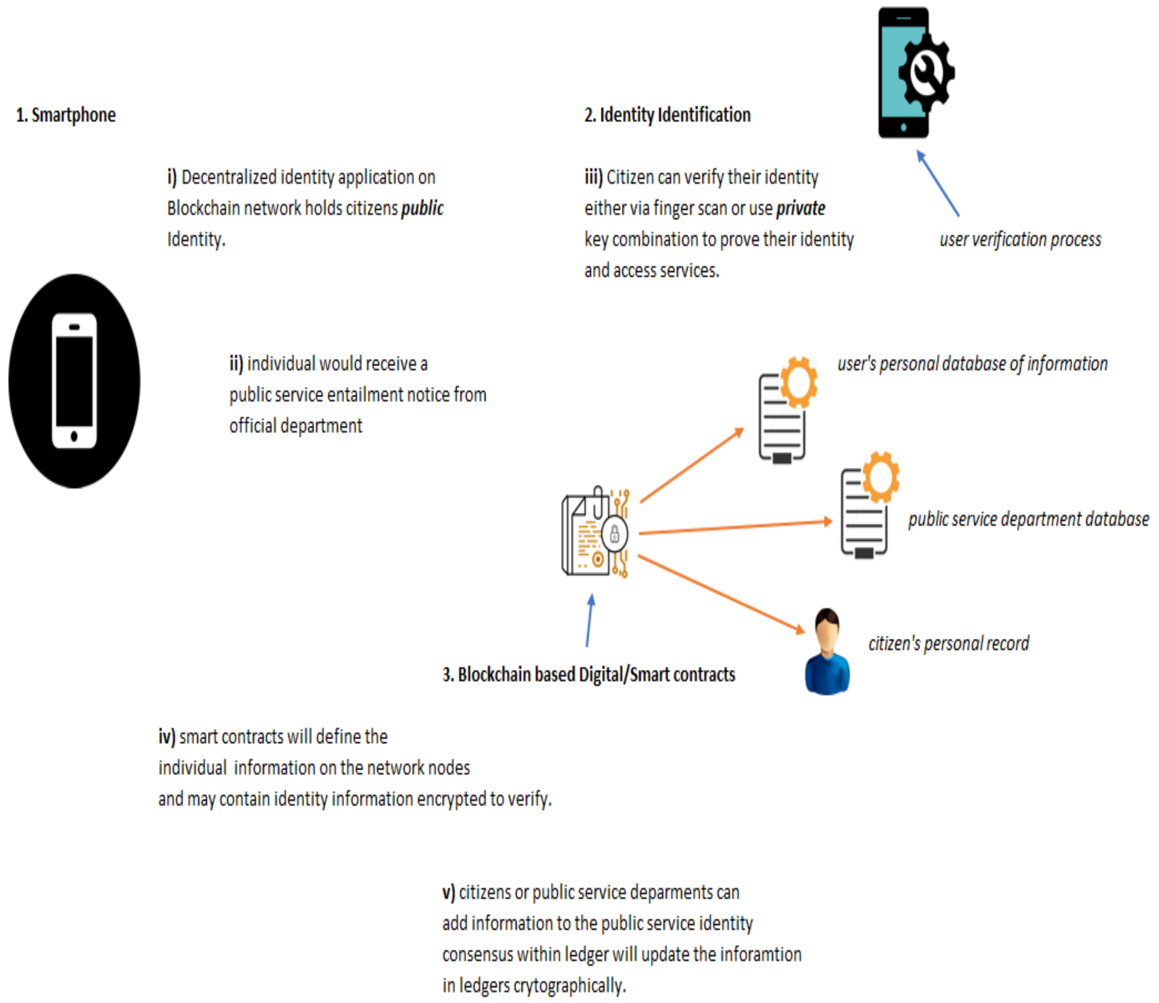
- Organisations and service providers will use an individual’s identity only to prove their presence. No single authority will have the power to manage Blockchain cluster where all such Ids are transacting. As it is said, equality is fundamental. Otherwise, central authorities can access and manipulate the data without the permission and knowledge of individuals.
- Decentralization and distributed are the fundamental attributes of Blockchain which makes will let all digital identities publically access and participate to create transparency.

6.2 Decentralized identities on Blockchain in Public Sector:

Blockchain technology can be utilized to conduct any sort of transaction or exchange of information within public sector. The fundamental characteristics of this disruptive technology open the path for public sector to implement wide range of solutions like information, inventory, asset registry and inventory and intangible assets like health data, reputation, ideas and intention etc. The basic logic behind Blockchain technology is that several public sector departments can jointly create one single *ledger* and keep track of this ledger to immutable transactions. Some researchers argue that Blockchain is “an institutional technology of governance that competes with other economic institutions of capitalism, namely firms, markets, networks, and even governments” and even stated that BC can be viewed as technology that competes with the role of government in society. Technology competing with an institution might be considered as a technology-push, far-fetched and naive, but nevertheless such propositions should not be ignored and research is needed to position this in a more realistic view which takes into account both technical and institutional elements.

The potential technical advantages of Blockchain technology for Digital Identity management systems makes it attractive for the public sector to bring overall transformation. Since the traditional identity management system utilized are relatively straightforward to control by the single authority but decentralized and distributed nature of the Blockchain technology would bring tremendous changes in responsibilities and put forward new models of governance. Implementing Blockchain based identity management solutions without required design changes might not bring derived benefits.

Researcher has devised a potential solution case for implementing decentralized identity in public sector utilizing Blockchain based smart contracts, identity management solution and smartphone.



1. Smartphone
2. Identity Identification
i) Decentralized identity application on Blockchain network holds citizens ***public*** Identity.
iii) Citizen can verify their identity either via finger scan or use ***private*** key combination to prove their identity and access services.
user verification process
ii) individual would receive a public service entailment notice from official department
user's personal database of information
public service department database
citizen's personal record
3. Blockchain based Digital/Smart contracts
iv) smart contracts will define the individual information on the network nodes and may contain identity information encrypted to verify.
v) citizens or public service deparments can add information to the public service identity consensus within ledger will update the inforamtion in ledgers crytographically.

6.3 Contributions of the Study:

As the research shows Blockchain and decentralized identities are both relatively new concepts and both are still under development phase. The overall literature review will provide the standard guideline for readers who are unfamiliar with identity management solutions and Blockchain technology.

Blockchain as a field of research is fairly new and its adoption in reality cannot be seen or experienced so far other than cryptocurrencies and few developments in financial institutions. This research provides an overview of how Blockchain an why Blockchain can be utilized for other than cryptocurrencies. With the help of this study, researcher could find some technological as well conceptual challenges and findings suggests how to approach them.

The study further explained and revealed why there is need for identity and personal information ownership and which sectors can adopt these alternatives to bring transparency and trust. Blockchain is not the ultimate mean to bring transparency but research suggests that earlier attempts to bring transparency and independence extensively have failed and the decentralized solutions which are under development on Blockchain should be able to achieve this. These solutions needs to be further studied and investigated post implementation.

For public sector,

Chapter 7: Self-Reflection:

7.1 Introduction:

Self-reflection has been a part of my everyday life since I prefer to often take decisions in every segment of my life based on the past experiences. Reflection often strikes in our thoughts long after the incident has had occurred and it’s a natural phenomenon which occurs to let our mind think how the things could have been different. Cottrell discusses how reflection is important at a university level and that students are expected to develop into thinkers. They are expected to evaluate their own performance and draw conclusions on what went well and how to improve (Cottrell, S. 2010).

The choice of choosing to pursue MBA programme was well influenced by the discussion I have had with my colleagues, senior management within previous organizations and I personally felt that as a challenge to consider for brighter future. The choice of choosing MBA (General – Project Management, Cloud Computing & Dissertation on Blockchain) was balanced by the future prospects of my career plan and combining it my previous industrial experience.

Along with the selective subjects mentioned above, researcher had the opportunity to enhance his management experience and understand further practices of international management and financial world. MBA had always been on my mind, due to the fact it does open the path to better opportunities and provides a fair chance to involve in research on master’s level.

My personal aspiration and targets were highly inspired by the actions taken in the past and what I had planned for my future. My full time involvement in the MBA programme has let me self-reflect on my personal development, skills I had striving hard to learn with the combination of personal strength & weaknesses. I had been keenly observing the opportunities that were available in the industry and striving hard to fulfil my personal ambitions.

This MBA programme did fulfil some of the long held personal ambitions for me both professionally and personally. My personal preferences have a lot to do with how and where I grew up, what career and life choices I have made, the contexts in which these happened and the rationale and ambition accompanying my professional development to date.

Considering a personal during the course of second semester had allowed me to work upon my personal strengths & weakness and provided guidance in deciding what is important to work upon and what should be left out. This way it acted as a pivotal tool guiding me to plan and execute both my professional as well as personal development.

7.2 Planning & Preparation:

“By failing to prepare, you are preparing to fail.” — Benjamin Franklin

Planning and preparations are the basic attributes to be successful in everything we take on personally or professionally in life. Benjamin Franklin's statement couldn't be truer when it comes to conducting a research project like a dissertation. Due to limited availability of time and full time industrial internship, the whole research had to be completed within given time frame with proper planning and preparation. During the course of two semesters, professors made sure that the students were well prepared to submit their assignments on time, exams which incurred after the submissions played a vital role in preparing the students to focus on several aspects to plan in advance. Combination of such practises over a period of 8 Months helped the researcher to complete the research within time.

Overall, this led the researcher to understand the value of planning and time management when selecting the respondents for the qualitative research. Continuous efforts to plan the overall research study helped to maintain the balance with industrial internship, work life balance and submission on time.

7.3 Research Skills:

I have been continuously writing on several occasions within my previous organizations but conducting research was never a part of it. Research skill theory is completely new to me and the opportunity to conduct and become a researcher had been exciting journey so far for me.

Keeping oneself up to date with relevant information and upgrading knowledge is fundamental to present opinions, enhancing the knowledge and presenting a logical argument. Over the journey of this course, I have developed the skill to conduct primary and secondary research for this dissertation and now I can gather and formulate the information to present in a logical manner.

Since I personally found the process of research engaging and interesting, this led to utilise a large number of tools and resources available at DBS library to evaluate and develop my skills and noticed the improvement in a number of areas. Prior to this, the process of research was completely alien to me but after conducting interview with CEO's, CO-founders of organizations I understood the value of research is relevant and basic necessity in every sector of the society. Understanding the core theories of subjects like Business strategy, project management, cloud computing, international management and ethics were cerebrally challenge initially whereas with time and support from lecturers I could easily develop personal style of learning, conducting research not only to develop the understating of subjects but also to form self-opinions.

This MBA programme has also helped me to develop the writing and research skills which I have already applied at industrial internship workplace with work colleagues.

7.4 Management Skills:

I kept on exploring the different verticals of industry to grow myself professionally and took advantage of being self-starter system of autonomous learning and hard work which gave me 5+ years of diverse experience within Information technology sector in India and Germany.

My personal growth in professional world was led by utilizing attributes like technically sound, always ready to learn, self-starter, time management, respect for work, team player together with continuous industrial education and training. I have always considered myself as a pragmatic learner. This continuous development was in direct relation to my personal interests, circumstances, strength and external environment. Over the period of time, common factors like positive mind-set, ability to adapt and change as per the circumstances, problem solving attitude and giving importance to practical education have supported me to sail through unexpected situations. My current knowledge, skills and industrial experience is based on information technology sector and the development of management skills, communicating to influence, planning and decision making have come up partly through this MBA programme and the internship I had been doing so far in one of the multination consulting organizations in Dublin.

Throughout my career in India, I had been observing and learning the principles of management by looking at senior officials and implemented those practises with self-discipline while working on group assignments and presentations. I have personally worked on many projects within the capacity of project coordinator and business analyst as a part of big teams but this MBA programme gave me the opportunity to act as a conscious Group Lead and Class representative at several intervals. Within my internship, I could see myself leading the group while working for clients, submitting the overall progress reports to senior management, suggesting and implementing the new ideas.

7.5 New Career Direction:

The researcher has accomplished his aim to gain profound knowledge about one of the disruptive technology Blockchain and each respondent had agreed that the subject of the dissertation was at most important for the coming future. During the interview process, researcher could find that there is hardly any research on Decentralized identity management solution based on Blockchain other than few report writings and solution design. Each respondent has requested a copy of dissertation post official marking since they have similar opinion about the decentralized digital identity. Researcher has completed his industrial internship and already started exploring the opportunities in the field of Blockchain as a major interest. This has to be the most fulfilling part of the overall process, realising what you planned and achieved in terms of personal and professional growth.

7.6 Conclusion:

During the process of pursuing MBA, researcher has become more conscious about his personal and professional life and admired the people who helped to shape this perspective. As a strength I have developed focused thinking and decisive nature. I might even suggest others to consider academic process (if not full-time, enrol for part-time) to refresh their experience and establish new achievements. It has been overall a roller coaster ride but now I am ready occupy myself in full time work to apply the learnings.

I think of myself as fortunate enough to plan and execute my ambitions with the help of individuals who influenced in the beginning to do so. At this stage of my life, I have achieved the objectives, goals set before leaving my home country and dedicate this victory to my family for their unconditional support and love.

Bibliography

1. Accenture. (2018). *Accenture.* Retrieved from Accenture: https://www.accenture.com/t20180418T064019Z__w__/ie-en/_acnmedia/Accenture/Designlogic/16-3360/documents/Accenture-2017-Top-10-Challenges-10-Distributed-Ledgers-Blockchain.pdfla=en#zoom=50

2. Ahmed Alketbi, D. Q. (2018). Blockchain for Government Services – Use Cases, Security Benefits and Challenges. *IEEE*.

3. Alexandre, A. (2018, Aug 28). *cointelegraph.* Retrieved from cointelegraph.: https://cointelegraph.com/news/pwc-regulatory-uncertainty-and-lack-of-user-trust-inhibit-blockchain-adoption

4. Ali Ahmad Malik, H. A. (2015). Federated Identity Management Challenges and Opportunities . *IEEE*.

5. Ali Alkhalifah, J. D. (2012). The Role of Identity Management Systems in Enhancing Protection of User Privacy . *IEEE*.

6. Allen, C. (2016, April). *lifewithalacrity*. Retrieved from lifewithalacrity: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

7. Alliance, S. I. (2018, June 19). *secureidentityalliance*. Retrieved from secureidentityalliance.org: https://secureidentityalliance.org/public-resources/152-strong-identity-strong-borders-an-sia-paper-june-2017/file

8. Andrew Tobin, D. R. (2017). The Inevitable Rise of Self-Sovereign Identity. *Sovrin Foundation*.

9. Antipova, T. (2018). Using Blockchain Technology for Government Auditing. *IEEE*.

10. Asia, N. (2018, Nov). *Networks Asia.* Retrieved from Networks Asia: https://www.networksasia.net/article/blockchain-adoption-and-deployment-massively-hyped-study.1525919030

11. Ayed, G. B. (2011). Digital Identity Metadata Scheme. *IEEE*.

12. Bernd Zwattendorfer, T. Z. (2014). An Overview of Cloud Identity Management-Models. *Institute for Applied Information Processing and Communications*.

13. BOJANA KOTESKA, E. K. (2017). Blockchain Implementation Quality Challenges: A Literature Review. *Proceedings of the SQAMIA 2017.* Belgrade.

14. Breckenridge, G. (2018, June 4). *medium*. Retrieved from medium.com: https://medium.com/humanizing-the-singularity/a-brief-history-of-digital-identity-9d6a773bf9f5

15. Burns, R. B. (2008). *Business research methods and statistics using SPSS. .* London.

16. Cummings, D. (2017, July). *ethnews*. Retrieved from ethnews.com: https://www.ethnews.com/uport-announces-zug-digital-ethereum-id-pilot

17. Deloitte. (2018). *Deloitte.* Retrieved from Deloitte: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-2018-global-blockchain-survey-report.pdf

18. Deloitte. (2018, January). *Deloitte.* Retrieved from Deloitte: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/public-sector/in-ps-blockchain-noexp.pdf

19. Di Battista G, D. D. (2015). Bitconeview: visualization of flows in the bitcoin transaction graph. In: Visualization for Cyber Security (VizSec),. *IEEE*, 1-8.

20. ERCIM. (2017). *Blockchain Engineering.* July.

21. Erik, J. (2018, Aug). *EEMA*. Retrieved from EEMA: https://www.eema.org/identityblog/the-problem-of-self-sovereign-identity-we-cant-trust-people-john-erik-setsaas/

22. Erik, J. (2018, August 10). *EEMA.ORG*. Retrieved from EEMA: https://www.eema.org/identityblog/the-problem-of-self-sovereign-identity-we-cant-trust-people-john-erik-setsaas/

23. Eve Maler, D. R. (2008). The Venn of Identity. *IEEE*.

24. Fearon, J. D. (1999). *WHAT IS IDENTITY (AS WE NOW USE THE WORD)?* Stanford: Stanford University.

25. Ferreira, M. B. (2014). Identity management for the requirements of the information security. *IEEE International Conference on Industrial Engineering and Engineering Management*, 53-57.

26. Forum, W. E. (2018). *Identity in a Digital World .* Geneva: World Economic Forum.

27. Francesco PIGNATELLI, M. S. (2018, Oct 24). *ec.europa.* Retrieved from ec.europa: https://ec.europa.eu/isa2/sites/isa/files/2018-10-18_blockchain_isa2.pdf

28. Gartner. (n.d.). *Gartner*. Retrieved from Gartner: https://www.gartner.com/it-glossary/identity-and-access-management-iam/

29. gemalto. (2018, May). *gemalto*. Retrieved from gemalto: https://www.gemalto.com/brochures-site/download-site/Documents/documentgating/fs-wp-The-Digital-Identity-Revolution.pdf?webSyncID=6c08674a-5807-7019-ed14-44430b335c3d&sessionGUID=7e0b5d19-0120-70a2-6c53-a8ec3bae6065

30. Gilbert Fridgen, F. G. (2018). Challenges and Opportunities of Blockchain-based Platformization of Digital Identities in the Public Sector. *European Conference on Information Systems*. Retrieved from European Conference on Information Systems: https://pdfs.semanticscholar.org/51ad/431bae6872b60c9f0dee4c37e7d3cdc48016.pdf?_ga=2.47114151.1086101123.1546870308-2038221706.1546870308

31. Gustav, H. H. (2017). A Blockchain-Based Approach Towards Overcoming Financial Fraud in Public Sector Services. *aisel*.

32. Hasnae L0AMRANI, B. E. (2016). Identity Management Systems: Laws of Identity for Models0 Evaluation. *IEEE*.

33. Holden, M. L. (2004). *Choosing the Appropriate Methodology: Understanding Research Philosophy.* Mark.

34. Infosys, F. L. (2017). *Blockchain Technology From Hype to Reality.* Feb.

35. Jackson, E. (2013). *Choosing a Methodology: Philosophical Underpinning.*

36. Jesse Yli-Huumo, D. K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. *PLOS ONE* .

37. Josep Lluis de la Rosa, V. T.-P. (2017). A SURVEY OF BLOCKCHAIN TECHNOLOGIES FOR OPEN INNOVATION.

38. Kezia, E. (2018). *itpro*. Retrieved from itpro: http://www.itpro.co.uk/cyber-attacks/30487/76-of-local-government-organisations-suffered-a-cyber-attack-in-the-past-year

39. Kvitnitsky, A. (2018, September 17). *Digital Identity: Crucial for the Success of Today's Mobile-First World* . Retrieved from GSMA: https://www.gsma.com/identity/digital-identity-crucial-for-the-success-of-todays-mobile-first-world

40. Maylor, H. a. (2005). *Researching Business and Management.* London : Palgrave.

41. Miriam Lips, C. P. (2008). *IDENTITY MANAGEMENT IN INFORMATION AGE GOVERNMENT .* Wellington : Victoria University of Wellington .

42. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *https://bitcoin.org/bitcoin.pdf, 2008.*

43. Nations, U. (2018). *E-GOVERNMENT SURVEY 2018.* New York: UNITED NATIONS.

44. OECD. (2011). *DIGITAL IDENTITY MANAGEMENT .* OECD.

45. OECD. (2015). *Working Party on Security and Privacy in the Digital Economy.*

46. OECD. (2018, October 10). *oecd.org.* Retrieved from oecd.org: http://www.oecd.org/parliamentarians/meetings/gpn-meeting-october-2018/OPSI-Blockchain-Presentation-for-Global-Parliamentary-Network.pdf

47. Pimenidis, E. (2010). *Digital Identity Management.* Bristol: University of the West of England, .

48. Piotr Pacyna, A. R. (2009). Trusted Identity for All: Toward Interoperable Trusted Identity Management Systems. *IEEE*.

49. Pîrlea, G. (2016, Nov). *UCL.* Retrieved from UCL: http://students.cs.ucl.ac.uk/2016/group15/reports/research.pdf

50. Preukschat, A. (2018, jan). *medium*. Retrieved from medium: https://medium.com/@AlexPreukschat/self-sovereign-identity-a-guide-to-privacy-for-your-digital-identity-5b9e95677778

51. Rachida AJHOUN, R. A. (2014). Towards a New Model of Management and Securing Digital Identities . *IEEE*.

52. Rauchs, D. G. (2017). *EY.* Retrieved from EY: https://www.ey.com/Publication/vwLUAssets/ey-global-blockchain-benchmarking-study-2017/$FILE/ey-global-blockchain-benchmarking-study-2017.pdf

53. Rick Kuhn, T. W. (2017). Can Blockchain Strengthen the Internet of Things? *IEEE*, 68-72.

54. Riley, M. C. (2004). *Researching and writing dissertations in business and management.* London: Thomson Learning.

55. Rouse, M. (2017, Nov). *Tech Target*. Retrieved from Tech Target: https://searchsecurity.techtarget.com/definition/identity-management-ID-management

56. Sachdeva, S. (2002). E-Governance Strategy in India. *Government of Department of Administrative Reforms and I-WAYS*.

57. Saunders, L. a. (2009). *"Research methods for business students".* Prentice Hall.

58. Saunders, L. P. (2012). *Research Methods for Business Students.* Essex: Pearson Education Limited.

59. Shoemaker, D. (2010). Self-exposure and exposure of the self: Informational privacy and the presentation of identity. *Ethics and Information Technology*.

60. Standford. (2018). *stanford.* Retrieved from stanford: https://www.gsb.stanford.edu/sites/gsb/files/publication-pdf/study-blockchain-impact-moving-beyond-hype.pdf

61. Sundararajan, S. (2017, Nov). *coindesk.* Retrieved from coindesk..com: https://www.coindesk.com/un-agencies-turn-to-blockchain-in-fight-against-child-trafficking/

62. Swan, M. (2015). *Blockchain: Blueprint for a New Economy.* O'Reilly Media, Inc.

63. Venkatesh, V. B. (2013). *Bridging the Qualitative-Quantitative Divide Guidelines for Conducting Mixed Methods Research in Information System.*

64. Walliman, N. (2011). *Your research project: designing and planning your work,.* London.

65. Wayne Goddard, S. M. (2004). *"Research Methodology: An Introduction".* Juta and Company Ltd.

66. WEF. (2018). *Identity in a Digital World.* Geneva: WEF.

67. Yeonjung Kang, H. P. (2008). A Digital Identity Management Service Model . *IEEE*.

68. Yuan Cao, L. Y. (2010). A Survey of Identity Management Technology. *IEEE*.

Appendix 1:

COVER LETTER FOR PARTICIPANTS

Hello Dear Participants,

My name is Sourabh Wadhwa, I am a student of MBA at Dublin Business School, Ireland. I am doing a research on the 'Decentralized Digital identity management using Blockchain and its implication on Public Sector. The main objective of the research is to understand the existing Centralized Digital Identity Management solutions, future of Blockchain based decentralized identity management solutions and how can public sector benefit from it. I want you to participate in this research, as a respondent, I (Researcher) would like to have a telephonic or video conferencing (as per your feasibility) interview regarding the above-mentioned topic, none of your personal details will be shared without your consent, All the information would remain secure and confidential, and the information will be destroyed after the completion of the module. The interview will approximately take 30-40 minutes. I would also like to put in your notice that I would like to record our conversation, if you allow me to do so, as a proof of the primary research. No personal information will be asked during the interview, and the participant can withdraw his/her participation at any time during, before or after the interview.

Kindly, have a look at the Consent form and Information Sheet as well. If you have any queries, please feel free to contact me at 10354466@mydbs.ie.

Kind Regards,

Sourabh Wadhwa

Appendix 2:

INFORMATION SHEET FOR PARTICIPANTS

PROJECT TITLE:

Decentralized Digital identity management using Blockchain and its implication on Public Sector.

You are being asked to take part in a research study on…

Blockchain based decentralized identity management solutions and the implications factors on public sector.

WHAT WILL HAPPEN:

In this study, you will be asked to answer few questions on the factors which influence identity management solutions and evolution of decentralized identity management solutions using Blockchain technology. How will newly devised decentralized identities be utilized in public sector and the overall impact?

TIME COMMITMENT:

The study typically takes 30-40 minutes.

PARTICIPANTS' RIGHTS:

You may decide to stop being a part of the research study at any time without explanation required from you. You have the right to ask that any data you have supplied to that point be withdrawn/destroyed. You have the right to omit or refuse to answer or respond to any question that is asked of you. You have the right to have your questions about the procedures answered (unless answering these questions would interfere with the study’s outcome. A full de-briefing will be given after the study). If you have any questions because of reading this information sheet, you should ask the researcher before the study begins.

CONFIDENTIALITY/ANONYMITY:

The data I collect does not contain any personal information about you except your Name, designation, industrial experience and company name, any other personal details will not be shared to anyone at any point of time.

FOR FURTHER INFORMATION:

I Sourabh Wadhwa or my supervisor Mr. ‘Harnaik Dhoot’ will be glad to answer your questions about this study at any time. You may contact me at 10354466@mydbs.ie and my supervisor at harnaik.dhoot@dbs.ie.

Appendix 3:

Research questionnaire

Q1. What's your opinion about centralized digital identity management solutions?

Q2. Will decentralization affect the future of digital identity management solutions?

Q3. How Blockchain will explicitly impact the future of Decentralized digital identity management solutions?

Q4. Is there any other disruptive technology in the market that can provide same level of technical advantage as Blockchain for considering Decentralized Identity?

Q5. Can Government institutions consider Decentralized Identity Management solutions based on Blockchain to provide services for Citizens (e.g. one identity for credit rating, pensions, social welfare etc.)?

Q.6 what factors can hinder government institutions to adopt such solutions?

Q.7 what will be the biggest advantage of implementing Decentralization based solution in public sector?

Q.8 Are you aware of any programmes already commenced by the government of any nation to adopt Blockchain based solutions and what's the progress so far?

Q.9 which other sectors can directly be impacted by decentralization?

Q.10 is there anything you want to share as valuable knowledge and thoughts for this research?