Universiteit Leiden

ICT in Business and the Public Sector

Analyzing the NIST Cyber Security framework through a blockchain lens

Name: Prabdeep Singh
Student-no:s1968254

1st supervisor: Dr. W. Heijstek
2nd supervisor: Eng. Mohamed Atef Ibrahim | MSc

MASTER'S THESIS

Leiden Institute of Advanced Computer Science (LIACS)
Leiden University
Niels Bohrweg 1
2333 CA Leiden
The Netherlands

Master's Thesis
Analyzing the NIST Cyber Security framework through a blockchain lens
by
Prabdeep Singh

Thesis submitted in partial fulfillment of the requirements for the degree of
Master of Science
in
ICT in Business and the Public Sector

Date of defense: May 6, 2020

University:
Leiden University
Rapenburg 70
2311 EZ Leiden
The Netherlands

Author contact information:
Singhprabdeep10@gmail.com

Abstract

Blockchain is a relatively new technology paving its way throughout industries, and governments.

The audit industry is one of the sectors to which blockchain shows considerable potential. Research performed so far on how contemporary frameworks in the audit sector align with blockchain, is limited. Therefore, this study is of explorative nature.
The main purpose of this study is to present an understanding in the value of the NIST Cyber Security framework (NIST CSF) and a select amount of associated IT controls in the case of a risk assessment of a blockchain solution.

Six semi-structured interviews, and four expert reviews were performed to acquire data, and to analyze the framework and the IT controls. The selection of NIST SP 800-53 IT controls was established according to acquired expert information and consists of sub categories PR.DS1(Data-at-rest is protected) and PR.DS-5(Protections against data leaks are implemented), from the overarching category 'Data Security'. To finalize the research, a mapping is included of blockchain risks and the selected IT controls.

The review of the framework itself, resulted in 19 (86%) of the 22 categories from the framework, being classified as relevant for assessing a blockchain solution. However, it also showcased certain areas which do not provide an adequate match with the functioning of blockchain. The results furthermore, present a nuanced view on how IT controls are impacted, as most of the participating practitioners believe that a large part of the reviewed IT controls will require the same amount of importance in case of a risk assessment of a blockchain solution. In certain instances, IT controls can possibly lose importance. This is primarily the case for IT controls related to safeguarding the confidentiality, and integrity of information systems, and protecting information systems with cryptography. The mapping of the blockchain risks informs us on potential challenges. Blockchain risks involving smart contracts, wallet management, consensus management and permissioned ledgers consensus could not be directly addressed by the examined IT controls. Furthermore, risks involving cryptocurrency and interoperability are neither addressed by the respective IT controls nor can they be related to the category of 'Data Security'.

From the results, we conclude that the contemporary practice of the NIST Cyber Security framework can contribute substantially to the risk assessment of a blockchain solution. The framework from categorical and IT control level is perceived as generic, making it open for interpretation, and flexible to adapt it to the technicalities of blockchain. As the results also indicate mismatches it is important that practitioners stay aware that alike frameworks are not designed to complement blockchain. Especially since practitioners within (IT audit) do not possess the required blockchain-associated knowledge to uncover potential gaps related to blockchain. However, it is stressed that this study indicates the possibility for researchers and practitioners to incrementally build on already known and acknowledged frameworks and standards within the (IT) audit field.

Keywords
Blockchain, (IT) audit, IT controls, NIST, Cyber Security framework, ITGC

Table of Contents

1. Introduction

Blockchain is a digital ledger of transactions that is shared among the involved stakeholders within the network. The transactions in the blockchain are verified by the consensus of the majority of stakeholders within the network. Once a transaction is registered within the blockchain it cannot be erased. The blockchain contains a record of every transaction which can be proved (Crosby, Nachiappan, Pattanayak, Verma, & Kalyanaraman, BlockChain Technology: Beyond Bitcoin , 2016).

Industries like Finance, Real Estate and Tax & Legal are examples of industries which have invested in the technology. Shown below some figures regarding investments in the distributed ledger technology (DLT)/blockchain (World Economic Forum, August 2016).

The main drivers for financial banks and institutions to invest in the technology are mainly the opportunities that arise to save costs (Morabito, 2017). For example, a report by the European bank Santander found that blockchain is capable of cutting down on the infrastructural costs of banks by $15-20 billion a year by 2022 (Perez, 2015). Likewise, Capgemini reports that consumers can save up to $16 billion on banking and insurance by the integration of blockchain-based smart contracts (Capgemini, 2016).

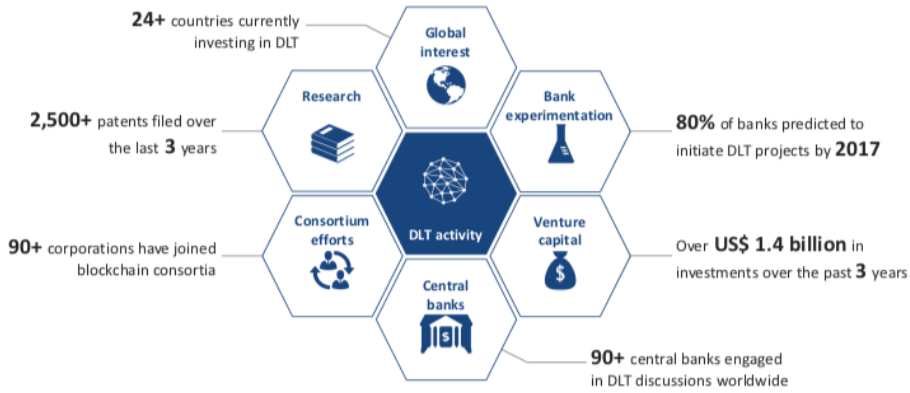

Figure 1 - Blockchain and DLT Activity (Consultancy.uk, 2017)

Other drivers which fuel the investments from Financial Services Industry (FSI) are (Morabito, 2017):

1. process automation with leveraging smart contracts,
2. and improved regulations compliance.

According to the Hype Cycle of Gartner the blockchain technology is slowly entering the 'Trough of Disillusionment' (Gartner, 2018). Gartner explains what this means: '*Interest wanes as experiments and implementations fail to deliver. Producers of the technology shake out or fail. Investments continue only if the surviving providers improve their products to the satisfaction of early adopters.* (Gartner, sd). The situation offers companies the opportunity to look how the technology has fared being implemented by early adopters, and how this knowledge can help to potentially integrate the technology in the existing or future business.
It is too early to say that the investments in blockchain have paid off, but what we can say with certainty that large firms, especially in in FSI have not withdrawn their support for the technology. In contrary, big names like JP Morgan and Goldman Sachs have shown their commitment in the future of blockchain technology (Tapscott, 2017). Some examples:

- JP Morgan launches an open source blockchain platform called Quorum (J.P. Morgan, sd)
- Goldman Sachs and Nyca Partners complete an investment of $32 million in enterprise blockchain startup Axoni (Forbes, 2018).
- Bank of America owning the most blockchain patents (Cointelegraph, 2018).

Furthermore, the 'big four'[1] are actively preparing to offer blockchain related services in the future. For example, in July 2018, the big four were involved in a trial, accompanying 20 banks for auditing temporary financial reports of public companies (Coindesk, 2018).
The same trend is observed within the public sector, where especially governments are investing in the technology of blockchain:

- European Union, using blockchain for anti-counterfeiting (EUIPO, 2019).
- Estonia, integrating blockchain within digital government (ComputerworldUK, 2019).
- China, developing a blockchain-based trade finance platform (Medium, 2018).

Blockchain opportunities are arising throughout several industries, but the feasibility and impact varies per industry. McKinsey & Company presents the following figure related to the feasibility and impact of blockchain per industry:

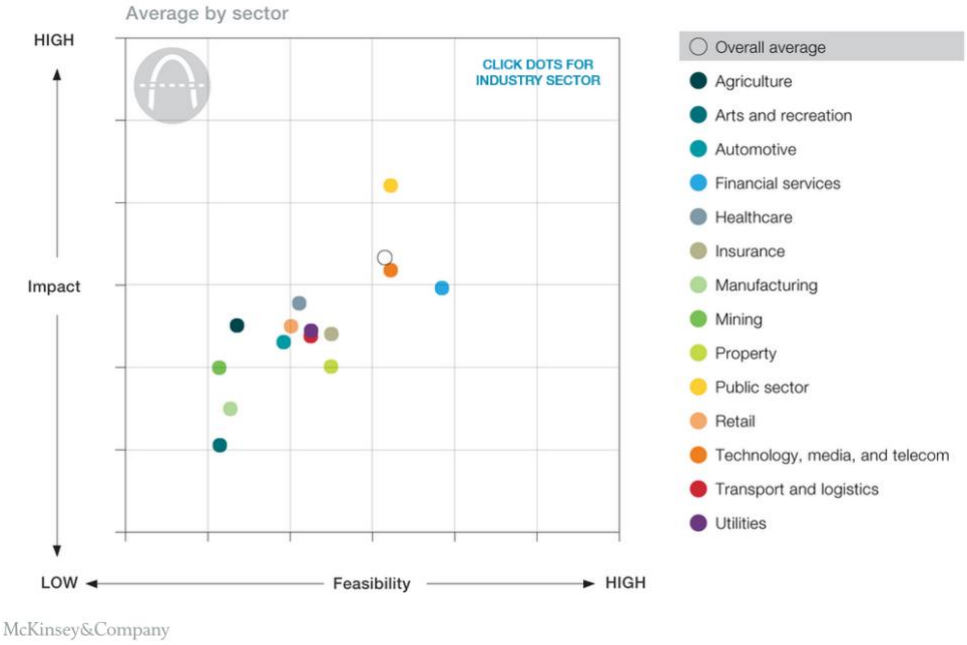

Figure 2 - Blockchain opportunities by industrial sector (McKinsey & Company, 2018)

> *'Financial services' core functions of verifying and transferring financial information and assets very closely align with blockchain's core transformative impact.'* (McKinsey & Company,

1 The 'big four' are the companies: Deloitte, PWC, EY and KPMG. These companies are the four biggest and leading organizations in consulting, and other professional services (Consulting.com, sd).

2. Literature review

The literature review discusses the existing body of knowledge with respect to the topics of blockchain and (IT) auditing. Subchapter 2.1. aims to offer an account on the emergence of blockchain, the technical concept, ending the chapter with explaining different types of blockchains. Subchapter 2.2. discusses the relevancy of blockchain to the field of (IT) audit and presents relevant research.

2.1 Defining the technology

The following definition is introduced to create a common understanding on blockchain: *'A decentralized, distributed database of signed sets of transactions which are secured by cryptographic hashing and consensus and proofing'* (Meyne, 2016).

Meyne adds, that the blockchain allows for process automation predefined by lines of code which are based on pre-determined if-else statements. Commonly referred as smart contracts, these lines of code are enforced by the code automatically without discretion (Swan M. , 2015).

The termination of the double spending problem is assured with the technology of blockchain (Pilkington, 2016). The double spend problem can indicate three different dilemmas: A dilemma induced by replicating digital goods. The notion of a dilemma that can emerge in distributed ledgers. An illustration of breaching in soundness in completely distributed ledgers (Drescher, Blockchain Basics, 2017).
Besides the dilemma of double spending, blockchain also needs to deal with the fault of individual peers having malicious intent, also referred as Byzantine failures or the Byzantine Generals problem (Baliga, 2017). The Byzantine Generals problem explains the inadequacy to reach consensus on a single truth between individuals in an unreliable network. (Lamport , Shostak, & Pease, 1982).

Brief history

Blockchain gained its mainstream-popularity trough Bitcoin. Bitcoin was introduced by Satoshi Nakamoto in the whitepaper 'Bitcoin: A Peer-to-Peer Electronic Cash System' (Nakamoto, 2008). Different elements of blockchain are not unique and trace back to decades earlier than the introduction of Bitcoin. The timestamping element for example was introduced in 1991 by Stuart Haber and W. Scott Stornetta in the paper 'How to Time-Stamp a Digital Document' (Haber & Stornetta, 1991). Furthermore, Nick Szabo introduced the notion of 'smart contracts' with the article 'Smart Contracts: Building Blocks for Digital Markets' in 1996 (Szabo, 1996).

> *'Bitcoin at its most fundamental level is a breakthrough in computer science- one that builds on 20 years of research into cryptographic currency, and 40 years of research in cryptography, by thousands of researchers around the world'* - Marc Andreessen (cofounder and general partner of the venture capital firm Andreessen Horowitz)

Blockchain and distributed ledger technology (DLT)

Blockchain and 'distributed ledger technology'(DLT) are two different concepts. Blockchain is considered a certain type or design of distributed ledger technology (Benos, Garratt, & Gurrola-Perez, 2017). Mougayar ads: '*It is deceptive to view the blockchain primarily as a distributed ledger, because it represents only one of its many dimensions. It's like describing the Internet as a network only, or as just a publishing platform'* (Mougayar, 2016).

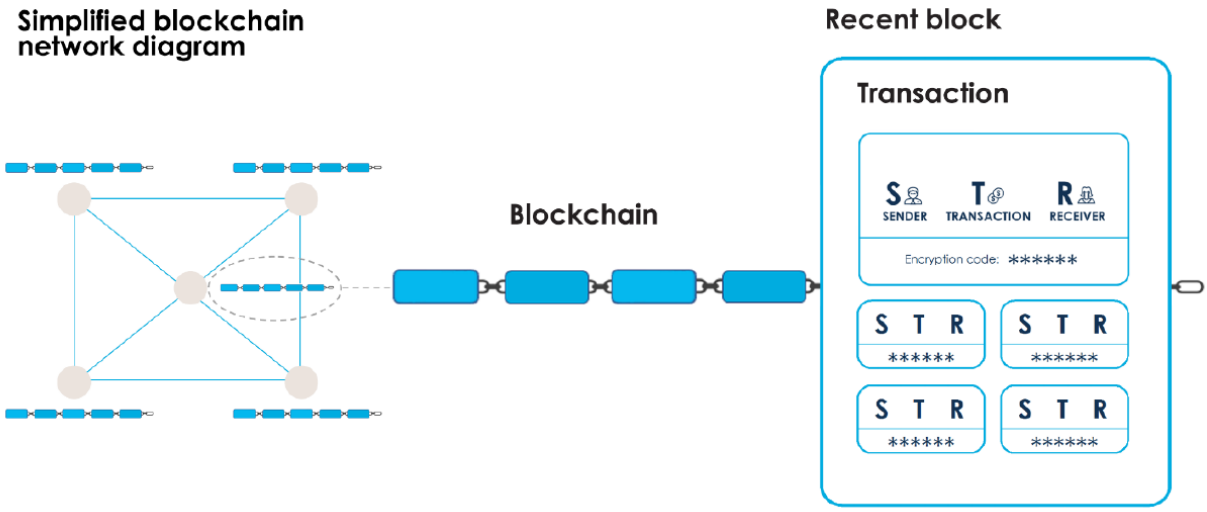

Figure 3 - Simplified Blockchain (Frøystad & Holm, 2015)

Above, an illustration of a blockchain is presented.
The blockchain consists of peers, also called nodes. Each node owns a chain of blocks.
These nodes establish a total history of transactions performed on the blockchain. A list of transactions is maintained by each block (Frøystad & Holm, 2015).

The list of transactions is continuously extended as transactions are ongoing. A new set of transactions is stored on the blockchain as a 'block'. A chain of the blocks is created, as each added block is timestamped and connected to the previous block (Dutch Blockchain Coalition, 2018).

Preceding to the chaining of the block to the blockchain, the set of transactions needs to be validated. Consensus by the majority of the nodes in the network is demanded to complete the validation. There are several consensus mechanisms that handle the validation of a blockchain. In the case of Bitcoin, this mechanism is the Proof of Work (PoW) (Frøystad & Holm, 2015). The Bitcoin blockchain being based on computation, requires an effort of computation by the node to validate the transaction, this indicates the 'proof of work' (Nakamoto, 2008).

2.1.1 Types of blockchains

Four categories of blockchains can be classified (McKinsey & Company, 2018):

- Public
- Private
- Permissioned
- Permissionless

As the name indicates, public blockchains are open to anyone (Bashir, 2018). Contrasting, private blockchains are distributed under established partners, and are not open to the public (Laurence, 2017).
A permissioned blockchain is operated by known entities, where members in a given business context operate a permissioned blockchain network. In a permissionless blockchain, anyone can join the network as a participant, anyone is able to make changes by initiating transactions, and anyone is able to engage in consensus building (Cachin & Vukolic, 2017).

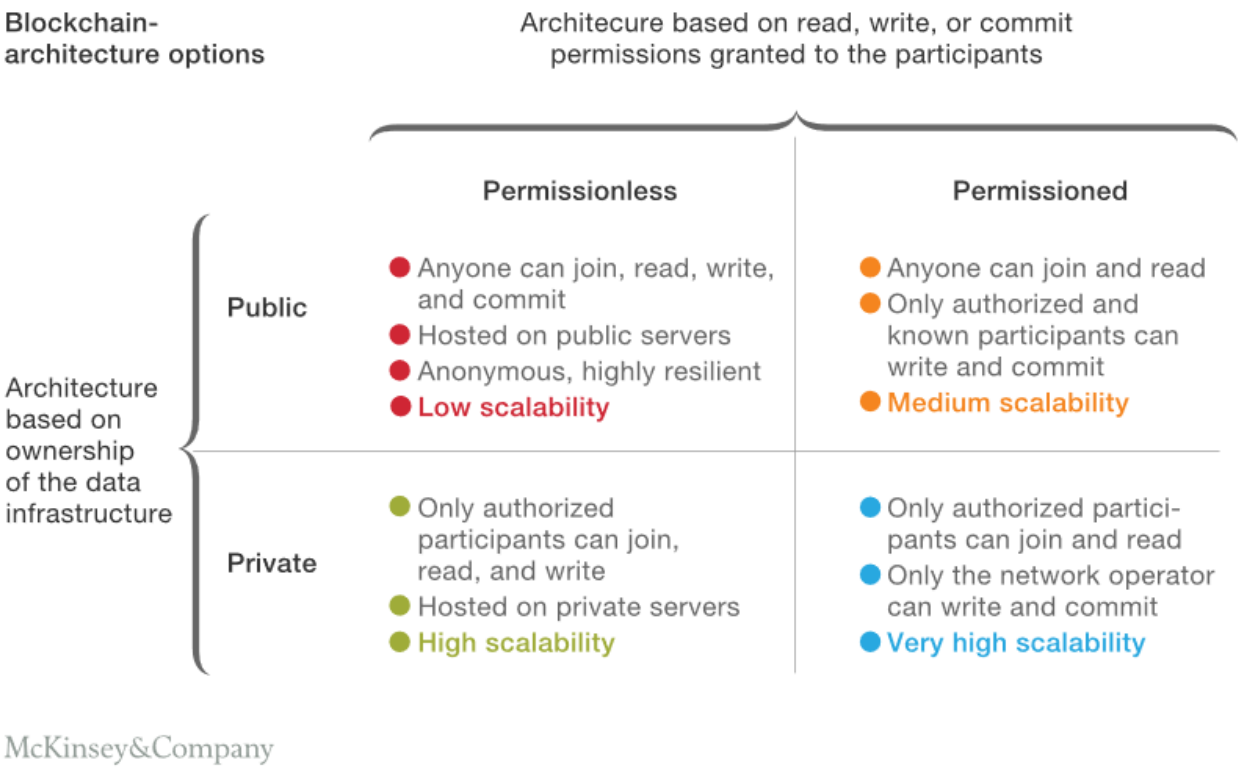

Figure 4 - Types of blockchains (McKinsey & Company, 2018)

2.1.2 Enterprise blockchains

As organizations deal with sensitive information, it is critical to choose the right type of blockchain. Considering their architectural properties, private and permissioned blockchains are inclined to being embraced earlier within enterprises (CPA Canada and AICPA, 2017).

Private blockchains have several advantages compared to public blockchains. For example, private blockchains assert more control for the company operating the blockchain, and it is cheaper as well as there are fewer nodes validating the transactions (Buterin, 2015). Another important advantage is the scalability. Permissioned and private blockchains make it easier to scale up the operations, as there is more control and fewer peers within the network (Peters & Panayi, 2015).

The Hyperledger project is an example of a private blockchain setup by the Linux Foundation, which has use cases in several enterprise sectors such as Trade Finance, Pharmacy, Supply Chain, Education and Energy Management (blockchain-council, 2019).

2.2 Blockchain and auditing

This subchapter discusses the relevance of blockchain to the audit field which also indicates the importance of this study. Reviewing existing knowledge on this topic aims to provide a valuable overview. This helps with understanding the gap which this study proposes to fill in the existing body of knowledge.

2.2.1 IT audit

Raymond Pompon in his book, IT Security Risk Control Management, defines an audit as a:
'A systematic examination by an independent expert on adherence to a well-defined standard.'
(Pompon, 2016).
From the organizations' perspective the author of this book states that audits are significant and necessary as it:

- Provides value from an outside perspective.
- Demonstrates the outgoing commitment of the organization to privacy and security.
- Can be used as a forcing function within the organization (Pompon, 2016).

Frameworks and standards are prepared by regulators like the IAASB (The International Auditing and Assurance Standards Board), which is a part of the IFAC (International Federation of Accountants) (IAASB, sd).
More IT (Information Technology) related governance frameworks are set by institutions as the Information Systems Audit and Control Association (ISACA). IT frameworks such as COBIT (Control Objectives for Information and Related Technologies) introduce IT general controls (ITGC's or IT controls), which help organizations and IT auditors with managing IT related risk(s) (Huang, Hung, Yen, Cheng Chang, & Jiang, 2010).

The process of an IT audit is conducted by the IT auditor. An IT auditor is someone who:
'Under direction of the Chief Audit Executive (CAE) and internal audit management, audits, reviews, tests, and evaluates IT-based applications and control procedures and reviews electronic security over the enterprise IT services network (Moeller, 2010).'

2.2.2 Related research

The need for this study originates from two angles. The first one already being covered in the introduction, whereas various industries and especially the Financial Services Industry, are heavily investing in blockchain. Audit and assurance firms are expected to pro-actively engage in potential disruptions within these industries as they help their clients on an operational and governance level.
Aside from this reactionary perspective, the technology itself poses interesting properties which match well with the profession of auditing as the nature of auditing is based on integrity, confidentiality and evidence-based approach[2].. Using blockchain within auditing presents the opportunity to monitor and verify transactions more efficiently and possibly to do it real-time as well (CPA Canada and AICPA, 2017); (Psaila, 2017).

Catalini and Gans explain how this is accomplished in their paper: 'Some Simple Economics of The Blockchain'. They differentiate in two main costs which are influenced by blockchain. The cost of networking describes the costs involved in the facilitation and management of a market with a centralized broker. Blockchain affects these costs as the technology facilitates the emergence of digital platforms as it radically diminishes the costs of operating decentralized networks. The costs related to authenticating information on prior transactions is indicated by the cost of verification, and the authors clarify that these costs are lowered as the authentication of the information happens on the blockchain (Catalini & Gans, 2016).

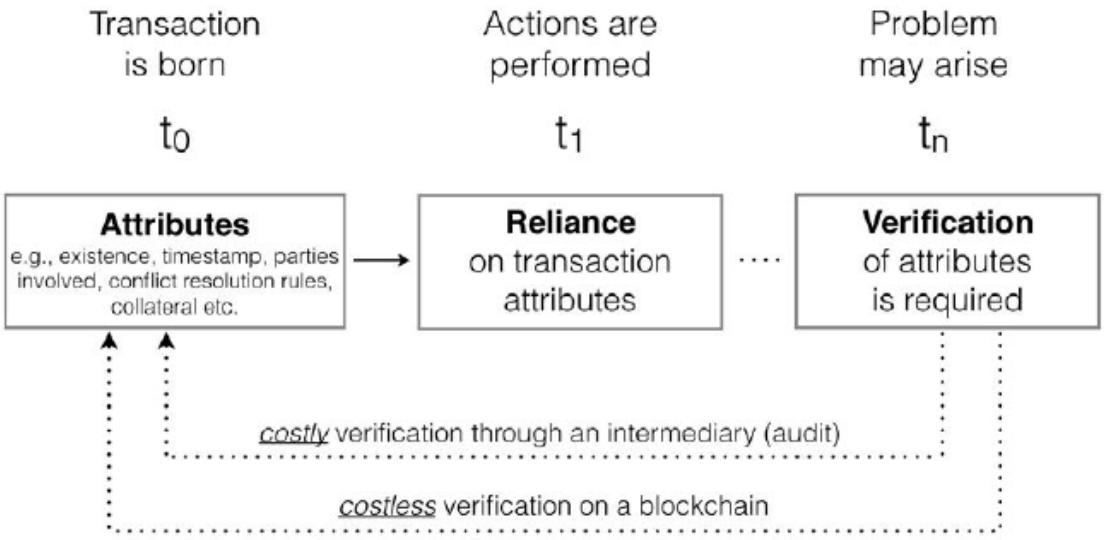

Figure 5 – traditional vs. Blockchain verification (Catalini & Gans, 2016)

Apart from driving cost efficiencies, blockchain shows promise fraud mitigation. A study in 2018 regarding transaction processing systems and blockchain found out that blockchains' properties of immutability and tamper protection are capable of being used in auditing for continuous monitoring and fraud prevention (Wang & Kogan, 2018).

2 The six audit principles are: Integrity, fair presentation, due professional care, confidentiality, independence and evidence-based approach. The characteristics of blockchain especially match with enhancing and protecting the integrity, confidentiality and evidence-based approach. These six principles are mentioned by the website of Whittington Associates, originally from ISO 19011:2011, clause 4.a through clause 4. f. (Whittington Associates, n.d.)

In the paper; Corporate Governance and Blockchains, the author highlights the term of real-time accounting which is enabled by the technology of blockchain. Envisioning the firm's business transactions on the blockchain, where involved stakeholders can attain prompt access to factual financial data. The author explains that the company itself would be capable to create its financial statements without depending on the judgement of IT auditors (Yermack, 2017) (The Institute of Chartered Accountants in England and Wales, 2018).

Jun Dai touches the topic of blockchain and audit in two essays written in October 2017: Audit 4.0 and Blockchain. The essays discuss how blockchain is capable of facilitating a real-time, trustworthy and understandable accounting ecosystem, and how the technology could possibly develop an automated assurance system (Dai, 2017). Also, the impact of the integration of blockchain along other technologies such as Internet of Things (IoT) is discussed.
Whereas Yermack explains that blockchain could reduce the role of auditing firms (Yermack, 2017), Jun Dai highlights that in consequence of the redundancy the role of IT auditors would shift from: *'Record tracing and verification to more complex analysis such as systemic evaluation, risk assessment, predictive audits, and fraud detection'* (Dai, 2017).
This conclusion is also corroborated by Cangemi & Brennan. Highlighting that, rather than removing auditors from checking transactions, blockchain is able to change how audits are conducted as it supports more forensic activities combining capabilities such as analytics, automation, artificial intelligence (AI) and machine-learning (Cangemi & Brennan, 2019).

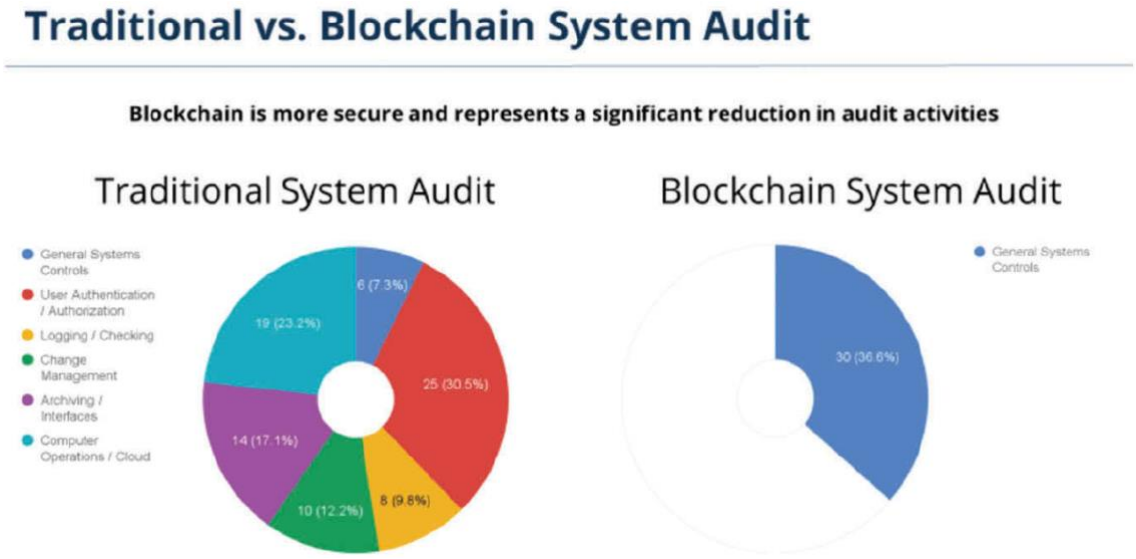

Figure 6 – Blockchain system audit vs traditional system audit (Cangemi & Brennan, 2019)

As highlighted in the image above a properly designed blockchain results in a more efficient audit.

3. Research objective

This chapter presents the problem statement. Furthermore, the main objectives and research questions are discussed.

3.1 Problem statement

Catalini & Gans and Sheldon offered a balanced view arguing that blockchain can change the nature of the work of intermediaries rather than entirely replacing these intermediaries (Catalini & Gans, 2016); (Sheldon M. D., 2018). This being in line with the conclusions of Jun Dai, Cangemi & Brennan and others as they highlight the changing role of an IT auditor surrounded by a dynamic environment of tailored technologies which allow the IT auditor to focus more on high-level questions (Dai, 2017); (Cangemi & Brennan, 2019); (The Institute of Chartered Accountants in England and Wales, 2018); (Nathalie, Marion, Jean-Henry, & Arber, 2019).

Considering the ongoing investments in blockchain from firms and governments as well, it is recognized that there is a demand for blockchain innovation especially in the Financial Services Industry. Although the need is there, organizations can still be reluctant towards the technology. One of the barriers feeding this reluctance is the regulatory uncertainty (Deloitte, 2018); (The Institute of Chartered Accountants in England and Wales, 2018). This is also supported by the findings of Jun Dai as the notion of investigating new controls with the emergence of new technologies/systems is discussed as future research possibilities (Dai, 2017).

Coherent with this thinking, are the findings in a more recent study about implications of blockchain on the audit profession. This study states that due to the lack of regulation and acceptance of the technology it is vulnerable to malicious intent. Not only is this in line with the assertion of regulatory uncertainty but it also indicates the importance of doing further research on regulatory frameworks (Jackson, 2018).

Concluding that regulatory uncertainty forms a barrier for organizations to further intensify or even start with their blockchain journey, organizations are rightfully reluctant as incomplete or incorrect regulations can pose a significant risk for the security of the organization and its environment. Blockchain introduces significant new risks and thus requires new controls and audit programs, which naturally brings challenges to contemporary practices (Cangemi & Brennan, 2019).

3.2 Main objectives

This study aims to help readers with:

1. Understanding the value of the NIST Cyber Security framework in the risk assessment of a blockchain solution.
2. Understanding the impact of blockchain on the NIST SP 800-53 IT controls.
3. Understanding how blockchain risks can be mapped to the NIST SP 800-53 IT controls.
4. Providing insight in opportunities for further research.

3.3 Research questions

The following research question (RQ) is presented:
How valuable is the contemporary practice of the NIST Cyber Security framework in response to a risk assessment of a blockchain solution?

To reach a well-defined answer on this study question, several sub questions (SQ) have been defined.

*SQ1). What is the most relevant IT audit framework for the risk assessment of a blockchain solution?**
SQ2). Which risks are associated with the technology of blockchain according to literature?
SQ3). How relevant is the NIST Cyber Security framework for the risk assessment of a blockchain solution from a categorical level?
SQ4). How important are the NIST SP 800-53 IT controls from subcategories PR.DS-1 and PR.DS-5 for the risk assessment of a blockchain solution?
SQ5). How do the collected blockchain risks, map to the NIST SP 800-53 IT controls from subcategories PR.DS-1 and PR.DS-5?

Table 1- Research questions

*Sub question one is answered in order to determine a suitable framework within the sub sequential parts of the study.

3.4 Scope

To facilitate IT auditors in their work, firms like the big four have developed their own audit methodology based on industry frameworks, standards and decades of experience. This can be considered as a best practice methodology. To scope down this study in terms of feasibility, one framework is selected for further research. The selection procedure of this framework is integrated within the research questions. The framework selected for this study is the NIST Cyber Security framework. The subcategories of the NIST Cyber Security framework are linked to the NIST SP80053r4 controls, which are of supplementary guidance to the core NIST Cyber Security framework. A selection of IT controls is chosen from the subcategories PR.DS-1: 'Data-at-rest is protected' and PR.DS-5: 'Protections against data leaks are implemented'. These subcategories are part of the function 'Protect', and category 'Data Security', and amount up to fourteen controls. These subcategories are chosen as they were deemed most relevant for this study.

3.5 Environment (Deloitte)

The study is fulfilled within the organization of Deloitte Netherlands as a graduate intern. Physical and online resources are made available by the organization for the conduct of the study. Furthermore, the organization provides potential participants which can be used for the study.

4. Research methodology

The study is conducted as an exploratory research. The objective of this study corresponds with a qualitative approach. A qualitive approach resonates with going beyond research in the form of numbers and focus on data which is not in the form of numbers (Punch, 2013). It allows this study to gain a deeper comprehension on the value the present practice of IT audit frameworks with regards to blockchain. This is deemed more important considering the state of the existing body of knowledge. Within the mindset of qualitative research, it is not necessary for transferability or generalization of the results (Polit & Beck, 2010). This is underlined by Saldana as he states that some methodologists argue that qualitative inquiry is too local and too case specific for a research to assert any transferability and that other methodologists recommend that writers leave any assumptions of transfer to the reader (Saldana, 2011).

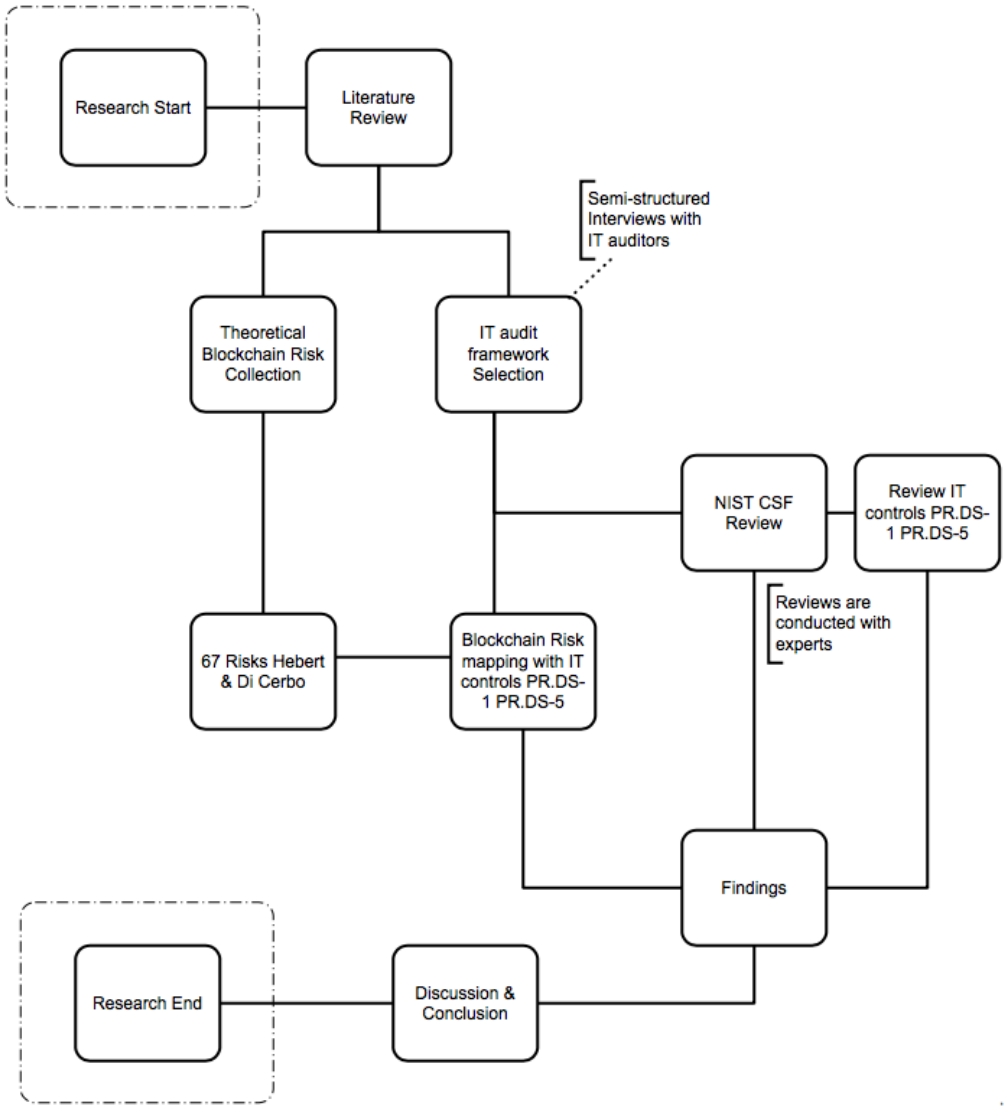

Figure 7 – Research process

4.1 Data collection and analysis

Primary and secondary data is gathered for this study.
Secondary data sources are used for the buildup of the literature review, and the collection of the theoretical blockchain risks. The secondary data sources emerge from various academic databases such as: Google Scholar, ScienceDirect, Elsevier, The Digital Library of Leiden University etc. Alongside these sources, whitepapers and reports are consulted of the big four and other organizations such as the Dutch Blockchain Coalition.
Primary data is collected by virtue of semi-structured interview and expert reviews.
Data analysis of this study is characterized by a systemic review of the NIST Cyber Security framework. The review is conducted on categorical and IT control level of the framework, and is divided in sub questions three and four.

SQ3 – Reviewing the relevancy of the NIST Cyber Security framework on categorical level
This question is answered in two parts. During the first part the actual review of the framework takes place together with a blockchain expert. The review is conducted on categorical level of the framework. The second stage involves a semi-structured interview with an IT auditor who has expertise in Cyber Security and is familiar with the selected framework. Main focus of this interview is how the participant perceives the findings arising from the review which was conducted in the first part.

SQ4– Reviewing the importance of the NIST SP 800-53 IT controls from subcategories PR.DS-1 and PR.DS-5
To answer this sub question, three expert reviews and one semi-structured interview are performed. The semi-structured interview is held with a senior manager mainly discussing the findings of the expert reviews. The purpose of this phase is to acquire findings of different experts in how they perceive the change in importance of the presented IT controls when they are used to assess a blockchain solution.

SQ5- Mapping blockchain risks to IT controls
The mapping involves three types of classifications:
1. Blockchain risks that can be associated with the respective IT control(s) (direct link).
2. Blockchain risks that cannot be associated with the respective IT control(s), but can be associated with respective risk category (indirect link).
3. Blockchain risks that cannot be mapped with neither the respective IT controls nor with the category .

The mappings are only identified with the purpose to create an understanding of potential links / mappings between blockchain risks and contemporary IT controls. The identified mappings do not imply to be the optimal link as only a selection of IT controls is used. It is possible that the blockchain risks are better linked with IT controls that are not included in the selection. The mapping is conducted without the help of any external input such as interviews, or expert reviews.

The table on the next page presents an overview of the data collection process, categorized per sub questions. The 'label' column in the table highlights a unique identifier of the interview. This identifier is used as a reference to the interview or expert review within the remainder of this document. The details of the interviews can be found in appendix A.

Phase	Sub question	Method	Pre-determined criterions	# Participants	Expertise / Background	Seniority level	Label
Phase 1	SQ1- Determining the most relevant IT audit framework	Semi-structured interviews	1. > three participants 2. Seniority level of the participants is manager or up 3. Participants have different backgrounds	4	IT Audit Cyber Security	Manager	SQ1M1
					IT Audit General	Manager	SQ1M2
					IT Audit General	Manager	SQ1M3
					IT Audit FSI	Senior Manager	SQ1M4
Phase 2	SQ2- Collecting theoretical blockchain risks	Literature review					
Phase 3	SQ3- Reviewing the NIST Cyber Security framework (categorical level)	Expert Review and semi-structured interview	1. => one participant 2. Participant has expertise in the selected framework or expertise in blockchain 3. Seniority level is manager or up	2	Blockchain	Manager	SQ3M1
					IT Audit Cyber Security	Manager	SQ3M2
Phase 4	SQ4 – Reviewing NIST SP 800-53 IT controls from subcategories PR.DS-1 and PR.DS-5	Expert review and semi-structured interview	1. => four participants with blockchain expertise 2. Seniority level is consultant or up	4	Blockchain	Consultant	SQ4C1
					Blockchain	Consultant	SQ4C2
					Blockchain	Junior Manager	SQ4JM1
					Blockchain	Senior Manager	SQ4M2
Phase 5	SQ5 – Mapping the risks to IT controls	No specified method Mapping is conducted per risk	-	-	-	-	-

Table 2 – Data collection overview

4.2 Research validity

Several measures are incorporated to ensure the validity of this study.

Triangulation
'The idea behind triangulation is that one can be more confident in a result if the use of different methods or sources leads to the same results' (Sekaran & Bougie, 2009), (Patton, Qualitative Research and Evaluation Methods, 2002).
The triangulation technique is used on two occasions:

1. Deciding the most relevant IT audit framework: multiple IT auditors are interviewed to decide which framework is used for further research.
2. Review of the IT controls: multiple blockchain experts are asked to review the selected IT controls.

Discrepant information
During this study discrepant information has come up. Interviews with IT auditors for the selection of a framework did not provide a clear answer. The interviewees found it difficult to answer which framework would be most compatible for the risk assessment of a blockchain solution.

Other considerations
All the interviewees being affiliated with one organization, can be regarded as a threat to the validity of the research. Furthermore, as only 14 IT controls are reviewed it can pose questions on the generalizability of the study.

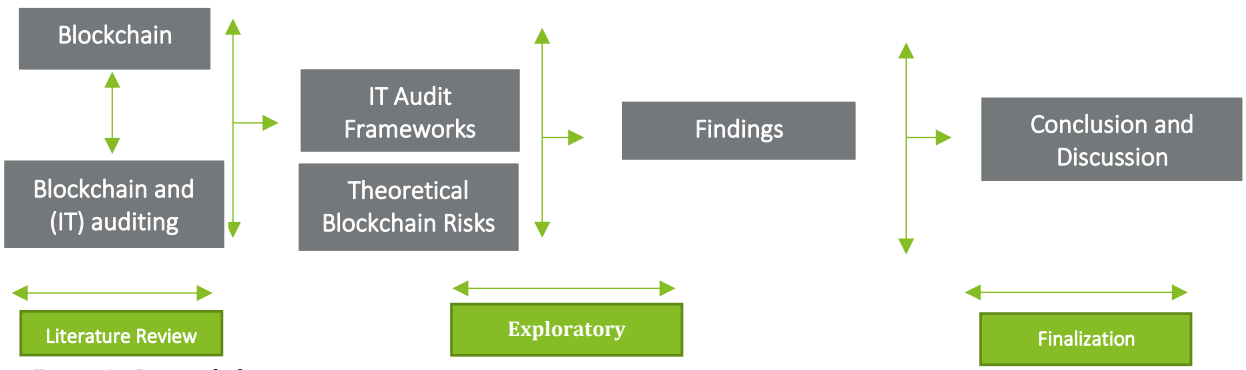

Figure 8 - Research design

5. Findings

The findings of the study are presented in this chapter. At first, an IT audit framework is selected. In subchapter 5.2, the theoretical blockchain risks are presented. Where after, the results of the review of the selected framework are highlighted. In subchapter 5.4, the findings of the IT controls review are showcased. At last, the results of the mapping are presented. The results are discussed in chapter six.

5.1 IT audit framework selection

The selection of the framework is based on single semi-structured interviews conducted with multiple IT auditors. The focus of the conducted interviews is to capture the most appropriate framework in the eyes of the interviewees in case of a risk assessment of a blockchain solution. The following questions were asked.

1.	Can you tell me your experience within IT Auditing?
2.	How do you perceive the findings of ISACA (figure 8 and 9 on page 25) presented in the tables? Do you acknowledge these findings?
3.	How familiar are you with the technology of blockchain? (If interviewee was not familiar with the technology, the concept of the technology was explained)
4.	Which framework according to you would be most appropriate for a risk assessment when the client has a blockchain solution in place, and why this framework?

Table 3 – Interview questions phase one

As a result of the interviews, the NIST Cybersecurity framework was selected as the most appropriate framework for further research.

NIST CSF (National Institute of Standards and Technology Cybersecurity framework)

NIST CSF is a set of best practices, standards, and recommendations to help organizations managing and reducing cybersecurity-related risk (National Institute of Standards and Technology, 2014). The framework originates from 2014 and came into existence after a Presidential Executive Order[3] (ObamaWhitehouse, 2013). The NIST CSF framework consists of five separate functions (National Institute of Standards and Technology, 2014):

- Identify
- Protect
- Detect
- Respond
- Recovery

The complete framework (function and categories) can be seen in sub chapter 5.3.

[3] On February 12, 2013 an executive order (13636) was issued regarding the improvement of critical infrastructure cybersecurity (ObamaWhitehouse, 2013). ca

It is of importance to mention that the terms IT or Information Security and Cyber Security are quite often used interchangeably (van Niekerk & von Solms, 2012). Rather, they are quite different from each other, despite having an overlap. Van Niekerk & Solms present the image beneath to differentiate the two.

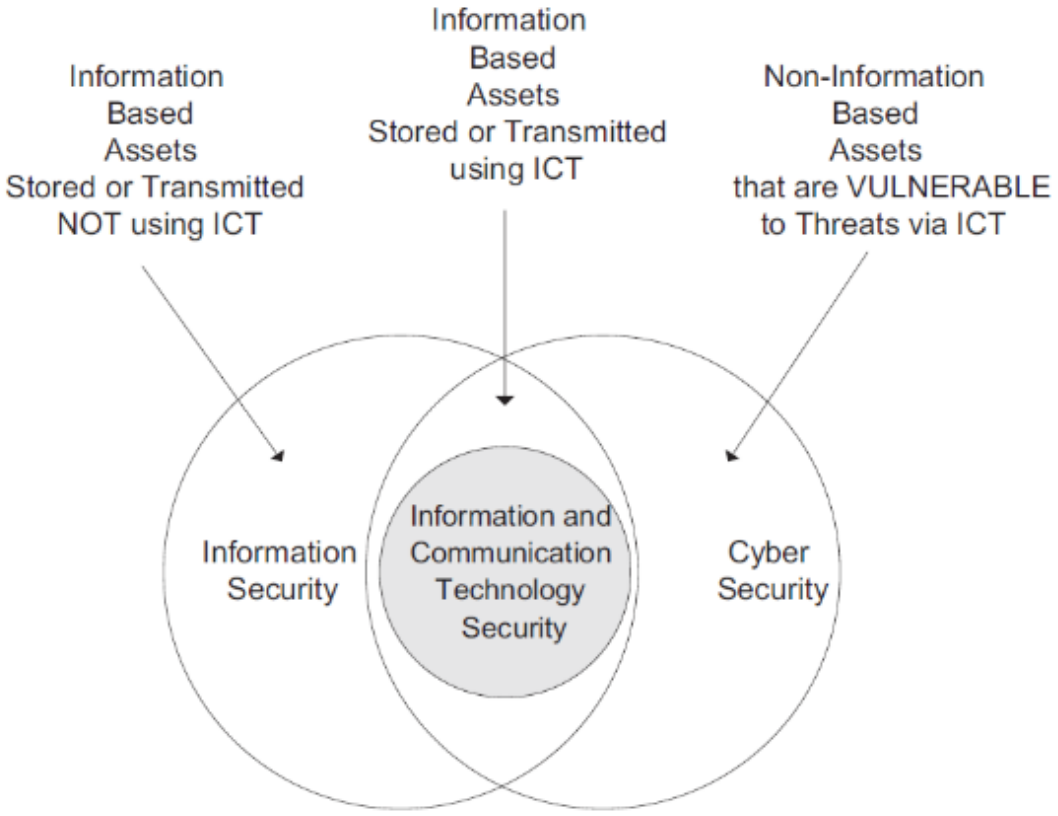

Figure 9 – Cyber vs Information Security

Overview of IT audit frameworks

Before selecting a framework, research has been conducted on the available frameworks. The following table is used as a base as it presents a comprehensive overview of the frameworks. The data in the table is collected by ISACA and Protiviti in 2017 during their global survey on IT audit benchmarking. More than 1300 participants joined the survey, from which 26% of the total participants were employed in FSI. (ISACA - Protiviti, 2018).

On which of the following accepted industry framework(s) is the IT audit risk assessment based? (Multiple responses permitted)

Region

	Africa	Asia	Europe	Latin America/ South America	Middle East	North America	Oceania
COBIT	61%	62%	68%	94%	52%	63%	63%
COSO	32%	37%	31%	53%	28%	47%	22%
ISO	68%	44%	34%	44%	52%	15%	41%
NIST CSF	10%	12%	13%	9%	8%	39%	15%
ITIL	32%	33%	31%	34%	32%	15%	33%
Basel III	6%	4%	10%	6%	16%	1%	0%

Figure 10 - Frameworks in performing IT audit risk assessments (ISACA - Protiviti, 2018)
Note: Percentages total more than 100 percent because respondents could submit more than one answer

Furthermore, from the same survey the following table is presented:

Which of the following frameworks does the audit function use in performing assessments of the organization's cyber security posture/maturity? (Multiple responses permitted)

NIST Cybersecurity Framework	59%
COBIT	53%
ISO 27000	44%
NIST 800-53	24%
CIS Top 20	14%
FFIEC Cybersecurity Assessment Tool	13%
AICPA Trust Service Criteria	5%

Figure 11- - Frameworks in performing Cyber Security assessments (ISACA - Protiviti, 2018)
Note: Percentages total more than 100 percent because respondents could submit more than one answer.

It showcases which IT audit frameworks are used in performing assessments of the organization's Cyber Security posture/maturity.
Based on the information in the table, the frameworks with the biggest footprint are explained below. Although the banking industry has its own regulatory framework in Basel III, this framework is not relevant for the scope of this study.

COSO (Committee of Sponsoring Organizations of the Treadway Commission)
COSO was established in 1985 as an independent private-sector initiative, aiming for the study of factors that can lead to fraud in financial reporting (COSO).

Figure 12 - COSO framework

The framework is also called the COSO-ERM framework, ERM standing for Enterprise Risk Management. In short, the COSO-ERM framework enables organizations to manage risks and establishes alignment with strategic objectives.

COBIT (Control Objectives for Information and Related Technologies)
As opposed to COSO, COBIT is the widely accepted internal control framework for IT. It is developed by ISACA. ISACA has released the newest version of the COBIT framework:

Figure 13 - COBIT framework

As it is noticeable from the image above, COBIT 2019 contains five domains which are subdivided in 40 management objectives. COBIT is used by organizations for IT management and governance, helping them by reducing the gap between business risks, technical problems and control requirements (ISACA).

ISO27001/2 (International Organization of Standardization)
ISO 27001 is part of the ISO 27000 family of standards which is related to Information Security (27000.org). ISO 27001 was first published in 2005 and is an international standard providing policies to secure IT assets. The purpose of the standard being: *'To provide requirements for establishing, implementing, maintaining and continuously improving an Information Security Management System (ISMS)'* (27000.org). ISO27002 is a complementing standard for the 27001-version offering more detailed information on the controls.

5.2 Theoretical blockchain security risks

In this subchapter the theoretical blockchain security risks are presented.
An aggregated table is presented beneath, with the risk category and the number of risks per category. The detailed list is attached to this document, as annex A.

Risk Category	Sub Category	Number of Risks
Basic Blockchain Risks (BAS) #26 Risks	Key Management	4
	Cryptography	2
	Data Protection and Privacy	2
	Exploitable vulnerabilities in blockchain code	1
	Consensus Management	3
	Wallet Management	4
	Scalability	4
	Regulatory, antifraud and anti-money laundering techniques and mechanisms	6
Generic data Risks #6 Risks	Capability of nodes to store arbitrary data onto the blockchain	4
	Personal Data Protection Regulations	2
Permissioned ledgers Risks #6 Risks	Permissioned Ledgers Consensus Risks	4
	Other Permissioned Ledgers Risks *	2
Permissionless ledgers Risks #8 Risks	Denial -of-Service Attacks	2
	Smart Contracts in permissionless ledgers	1
	Financial Regulations Noncompliance	2
	Scalability Risk	1
	Other Permissionless Ledgers Risks *	2
Other (situational) Risks #8 Risks	Interoperability	2
	Wallet Technologies	1
	Non-Categorical Situational Risks *	5
Crypto-currency Risks - #4 Risks	Crypto-Currency Risks *	4
Hash data Risks - #1 Risk	Hash Data Risks *	1
Smart Contract Risks - #8 Risks	Smart Contract Risks *	8
Total: #67 Risks		

Table 4 – Blockchain risks

The theoretical blockchain risks have been acquired after a thorough review of available literature. The final list originates from the paper 'Secure blockchain in the enterprise: A methodology', published by Elsevier. The risks presented by this paper have been selected as they present the most detailed version across other sources which have been investigated as well. The risks are grouped according to the information available in the paper. The subcategories highlighted with a '*' are grouped according to own insight as the paper did not provide enough information to group these as the other subcategories. The blockchain risks of other sources are retrievable in the detailed document.
The selected risks will be used in a mapping with the NIST Cyber Security framework. The results of this mapping are highlighted in sub chapter 5.5.

5.3 NIST Cyber Security Framework review

The following table showcases the results of the assessment of the NIST CSF.
Explaining the results:

- Categories that are deemed relevant are highlighted with a '✓' sign (green).
- Categories that are scored to not being relevant for blockchain are highlighted with a '✗' sign (red).

The assessment of NIST CSF is based on the input acquired during the expert interview (SQ3M1). Elaborate details of this assessment can be found in the document 'Findings per SQ', within appendix A.

Function	Category	Result
Identify	Asset Management (ID.AM)	✓
	Business Environment (ID.BE)	✗
	Governance (ID.GV)	✓
	Risk Assessment (ID.RA)	✗
	Risk Management Strategy (ID.RM)	✗
Protect	Access Control (PR.AC)	✓
	Awareness and Training (PR.AT)	✓
	Data Security (PR.DS)	✓
	Information Protection Processes and Procedures (PR.IP)	✓
	Maintenance (PR.MA)	✓
	Protective Technology (PR.PT)	✓
Detect	Anomalies and Events (DE.AE)	✓
	Security Continuous Monitoring (DE.CM)	✓
	Detection Processes (DE.DP)	✓
Response	Response Planning (RS.RP)	✓
	Communications (RS.CO)	✓
	Analysis (RS.AN)	✓
	Mitigation (RS.MI):	✓
	Improvements (RS.IM):	✓
Recover	Recovery Planning (RC.RP)	✓
	Improvements (RC.IM)	✓
	Communications (RC.CO)	✓

Table 5 – NIST CSF review results

86% (19 out of 22) of the categories from the framework were deemed relevant for assessing a blockchain solution according to the expert. Other results and observations associated with this sub question are discussed in sub chapter 6.1.

5.4 IT controls review

This part of the study includes a review of the IT controls, concerning sub question four. The answers of the experts have been classified as one of the following:

1. The IT control stays the same, it requires the same amount of importance (green).
2. The IT control could gain importance (light blue).
3. The IT control could lose importance (dark blue).
4. None of the three above (no classification), because the expert was not able to give a comment. Either caused by the expert not understanding the control or the expert did not see a link with blockchain (grey).

The results of the assessment are presented and summarized in the table, and charts beneath. Elaborate details of this review can be found in the document 'Findings per SQ', in tab 'IT Controls Findings SQ4.

IT Control Identifier	IT Control NIST SP80053r4	SQ4C1	SQ4JM1	SQ4C2
MP-8	Media Downgrading	No classification	Control stays the same, same amount of importance	Control stays the same, same amount of importance
SC-12	Cryptographic Key Establishment and Management	Control could become more important	Control could become more important	Control could become more important
SC-28	Protection of Information at Rest	No classification	Control stays the same, same amount of importance	Control could become less important
AC-4	Information Flow Enforcement	Control stays the same, same amount of importance	Control could become more important	Control stays the same, same amount of importance
AC-5	Separation of Duties	No classification	Control could become more important	No classification
AC-6	Least Privilege	No classification	Control could become more important	Control stays the same, same amount of importance
PE-19	Information Leakage	Control could become less important	Control stays the same, same amount of importance	Control could become more important
PS-3	Personnel Screening	No classification	Control stays the same, same amount of importance	Control could become less important
PS-6	Access Agreements	No classification	Control could become more important	Control stays the same, same amount of importance
SC-7	Boundary Protection	No classification	Control stays the same, same amount of importance	Control stays the same, same amount of importance
SC-8	Transmission Confidentiality and Integrity	Control could become less important	Control could become less important	Control could become less important*
SC-13	Cryptographic Protection	Control stays the same, same amount of importance	Control could become less important	Control could become less important
SC-31	Covert Channel Analysis	Control stays the same, same amount of importance	No classification	Control stays the same, same amount of importance
SI-4	Information System Monitoring	Control stays the same, same amount of importance	Control stays the same, same amount of importance*	Control stays the same, same amount of importance*

Table 6 – IT controls review results

5.5 Mapping blockchain risks to IT controls

As mentioned before, the mapping involves three types of classifications:

1. Blockchain risks that can be associated with the respective IT control(s) (direct link).*
2. Blockchain risks that cannot be associated with the respective IT control(s), but can be associated with the overarching category of 'Data Security' (indirect link). **
3. Blockchain risks that cannot be mapped with neither the respective IT controls nor with the category.

*Although level one shows a direct relevance with the IT control, it still needs to be adjusted to the technicalities of blockchain, and the associated risk(s).

** The category 'Data Security' according to the NIST framework, is defined as: *'Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information*' (National Institute of Standards and Technology, 2014).

The results provide that 58 out of the 67 risks(86%) can either be associated with the IT controls or the 'Data Security' category, as also showcased in the pie chart below.
Nine risks cannot be linked on either of the levels.

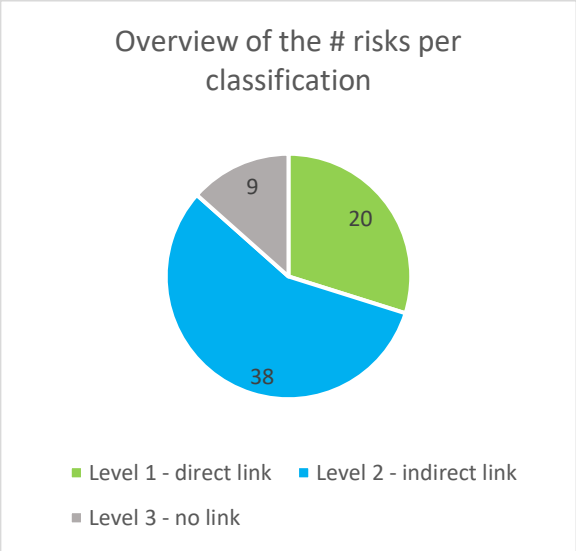

Figure 14 – Pie chart mapping

On the following page a bar chart is presented, containing an overview of the number of risks which are mapped ordered per risk sub category.

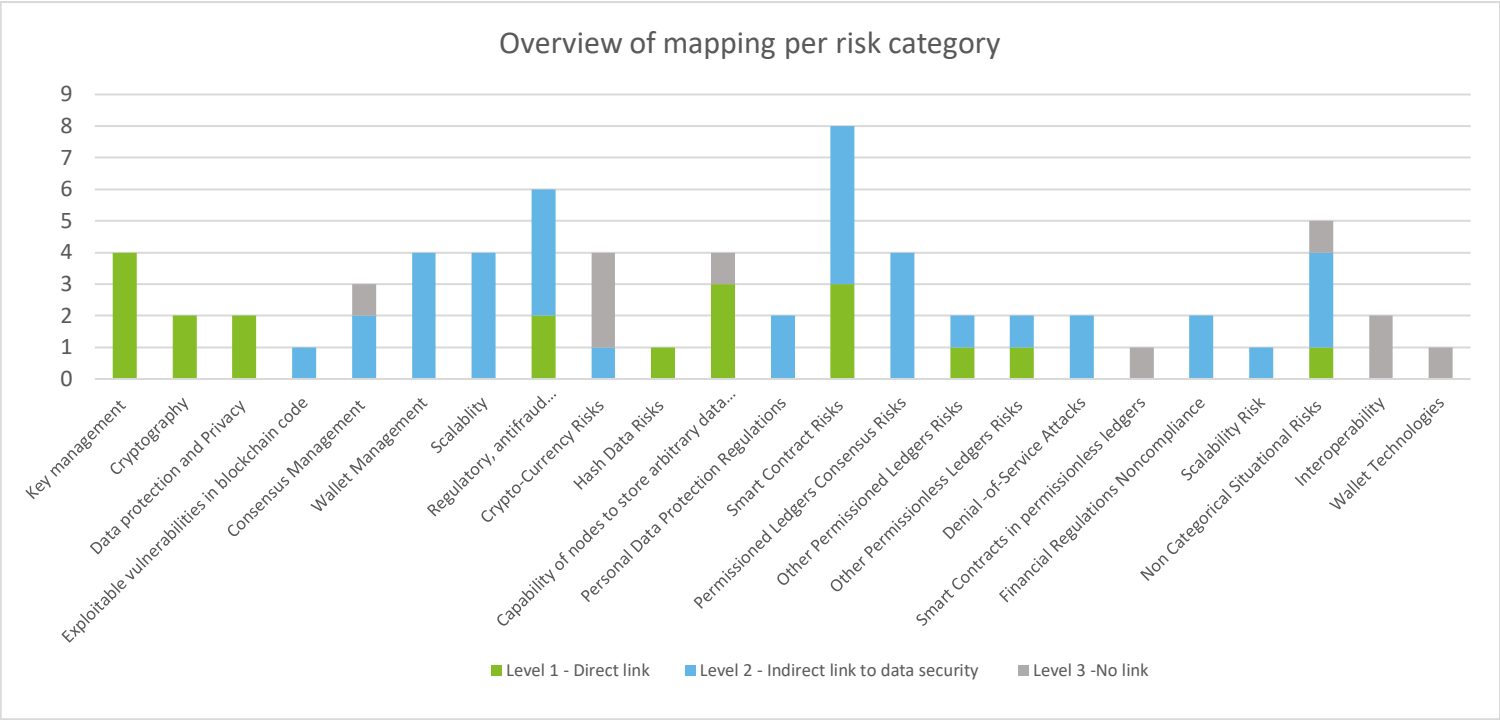

Figure 15 – Bar chart mapping per risk category

As seen in the bar chart, almost all sub categories contain risks which either contain a direct link or an indirect link. Beneath an overview is showcased of the number of risks mapped per IT control(only level one mappings).

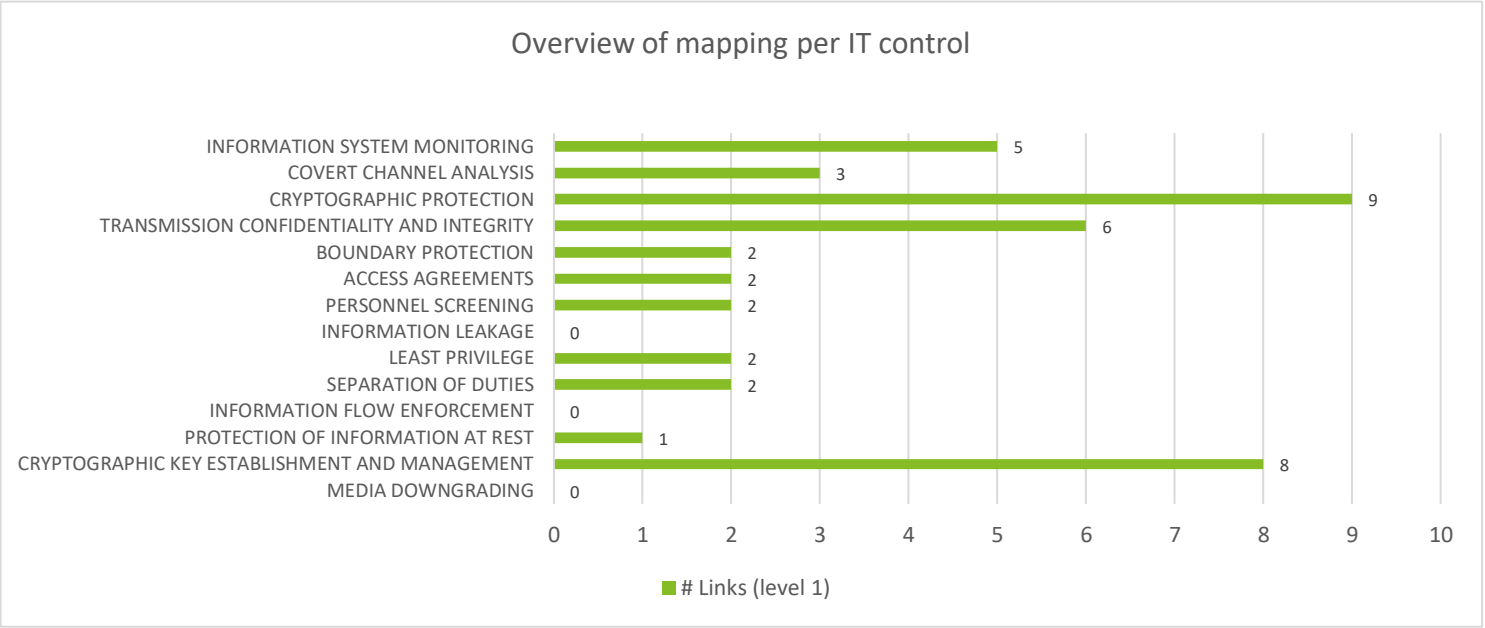

Figure 16 – Bar chart mapping per IT control

All IT controls except for the control of 'Information Leakage', Information Flow Enforcement' and 'Media Downgrading', can be linked to the risks.
Detailed information on the mapping can be found in the document 'Findings per SQ', within appendix A.

6. Discussion

The Results chapter yields valuable data on the NIST Cyber Security framework and the IT controls. In this chapter, the results are interpreted and discussed. Furthermore, the limitations of this study and notions for future research are discussed.

6.1 Research goals and implications

The results and implications are broken down per sub question.

SQ1). What is the most relevant IT audit framework for the risk assessment of a blockchain solution?

The NIST Cyber Security framework was chosen as a response to this question.
This was based on single semi-structured interviews with four IT auditors. During the interviews it became evident that some of the IT auditors struggled to point out a framework for the possible risk assessment of a blockchain solution. This potentially caused by the IT auditors having limited knowledge about blockchain, and the fact that they are not dealing with blockchain on regular basis. Nevertheless, this observation resonates with Gartner classifying blockchain as going through the 'Trough if Disillusionment' on the Hype Cycle, as people and business do not bother as much to investigate in further opportunities with the technology.

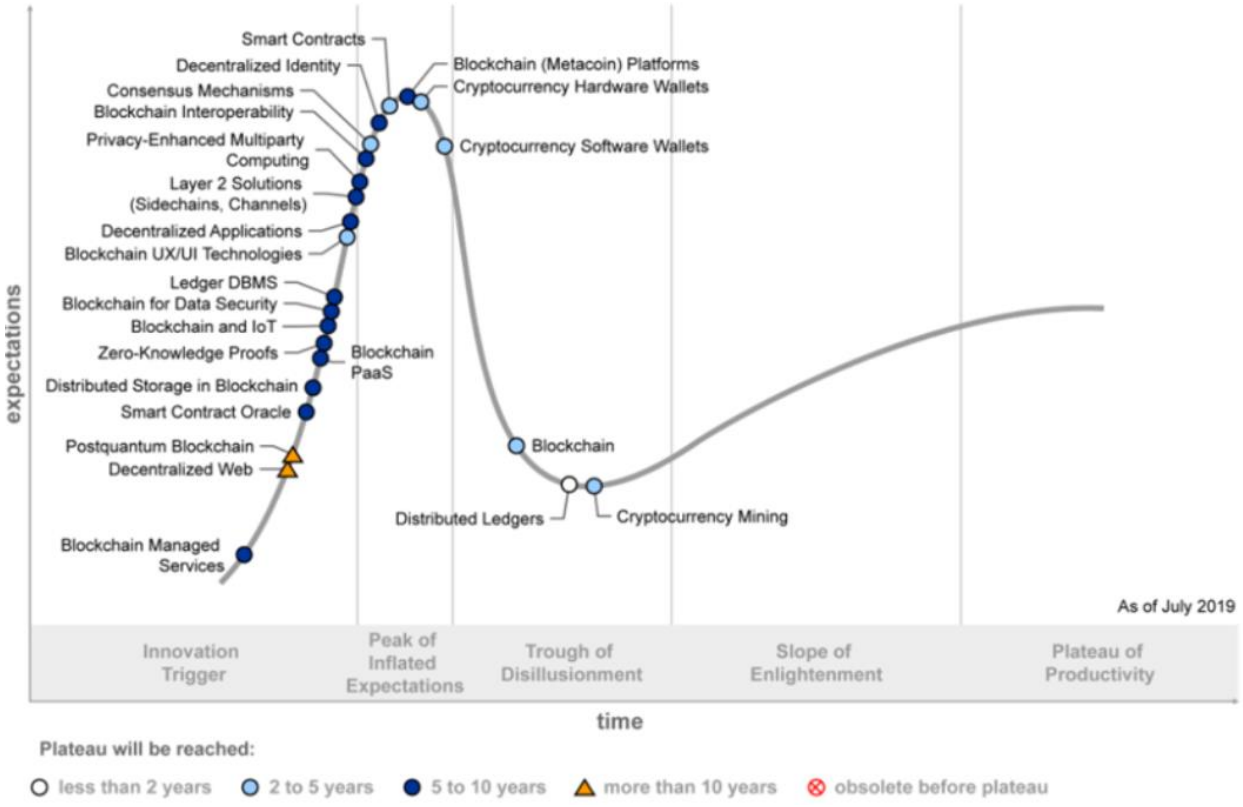

Figure 17 – Blockchain Hype Cycle (Gartner, 2019)

The stated grounds for choosing the NIST framework were, the framework being specific, albeit also flexible in approach. Based on personal experience, and also considering the use of this framework and its' IT controls by other participants who had no preceding experience with this framework, this perception is corroborated. Other discussed frameworks were termed as being more management/high-level/generic oriented.

SQ2). Which risks are associated with the technology of blockchain according to present literature?

During the process to answer this question, various sources of blockchain risks were explored and studied. Ideally, the risks were cross referenced which would have resulted in a triangulated list of blockchain risks, making it more rigid. However, this was not feasible within the constraints of the study.

After an extensive review of the collected literature, one single source was selected offering the most complete version of blockchain risks. The selected literature originated from a study on blockchain in the enterprise, published in June 2019. The research was conducted by researchers affiliated with SAP Security Research, France. The literature provided in total 67 risks. The collected blockchain risks were used in the mapping of blockchain risks to the IT controls.

On the previous page, the classification of blockchain on the Hype cycle according to Gartner is introduced('Trough of Disillusionment'). Building further on this notion, it is also observed that there is limited knowledge available within literature on the risks of blockchain from major providers such as the big four and other organizations. The literature review into these risks yielded in eight separate sources, from which two sources provided in-depth information.

SQ3). How relevant is the NIST Cyber Security framework for the risk assessment of a blockchain solution from a categorical level?

The review of the NIST Cyber Security framework produced various results and observations. The review of the framework itself, resulted in 19 out of 22(86%) of the categories from the framework being classified as relevant for assessing a blockchain solution.

From the results of the review, the following observation of a mapping is specified. The mapping concerns the risk category of 'Smart Contract risks' with 'Detect' function of the NIST Cyber Security framework. To be precise, the 'security vulnerabilities in the smart contract' risk could be detected by the category 'Anomalies and Events' within the function of 'Detect' or 'Protection'. It is crucial to note that the framework at all contains functions and categories that can be mapped to the risks of blockchain by either blockchain or IT audit practitioners.

Furthermore, there were similarities, and discrepancies between the thoughts of the two experts which were questioned during this phase. It is observed that both experts indicated the NIST CSF to being sufficient for a potential risk assessment of a blockchain solution. However, the blockchain expert explicitly stated to also consider the blockchain risks. The expert mentioned the following:

'When facing a client who has a blockchain solution for a risk assessment, then you should go with both the NIST Cyber Security framework and the blockchain risks document' SQ3M1.

These thoughts were discussed with the second expert. He pointed out to the performance of a Business Impact analysis. According to the expert, the Business Impact Analysis is incorporated in the IT audit methodology and automatically uncovers the blockchain risks in the scenario of the IT audit / risk assessment of a blockchain solution. The second expert furthermore, gave a rough estimate of 70% of blockchain risks that could be detected using the NIST CSF.

Nevertheless, the framework is also lacking in certain aspects. The results point out to the lack of a 'prevent' function within the NIST CSF.

We highlight the immutability property of blockchain, which on the contrary in many cases of a private and permissioned blockchains contain a built in 'backdoor' to prevent critical situations. The following was stated in relation to this: '*Response can be quite difficult if we are looking at an immutable blockchain. Nothing you can do, when something happens on a public chain. Unless your system is built in a certain way, enabling you to hit an emergency button. This*

is not necessarily something you would think about in response planning. Maybe a little bit, but primarily this would be in your design phase' SQ3M1.
The NIST Cyber Security framework does not directly address this functionality as it does not include a 'Prevent' category. It is believed that a 'Prevent' category would be a better match then for example the category of 'Response Planning', as it asks for a pro-active approach to plan these functionalities within its design-phase.

We can observe affiliations between the analyzed framework and blockchain.
Even though, the framework does not address the blockchain risks one on one, it does provide touch points to pose questions which will help practitioners to assess a blockchain solution to uncover potential risks.

SQ4). How relevant are the NIST SP 800-53 IT controls from subcategories PR.DS-1 and PR.DS-5 for the risk assessment of a blockchain solution?
As seen in the pie chart below, a majority of 59% of judgements indicated that the IT controls would either hold the same amount of importance or would gain importance in the situation of the risk assessment a blockchain solution.

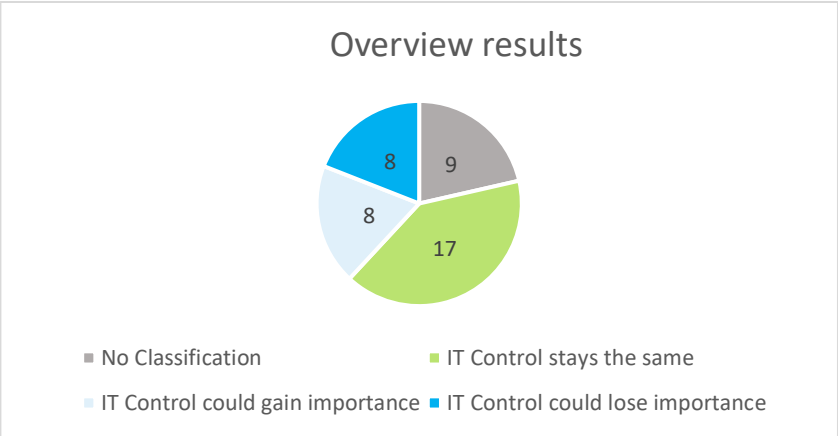

Figure 19 – Pie chart SQ4

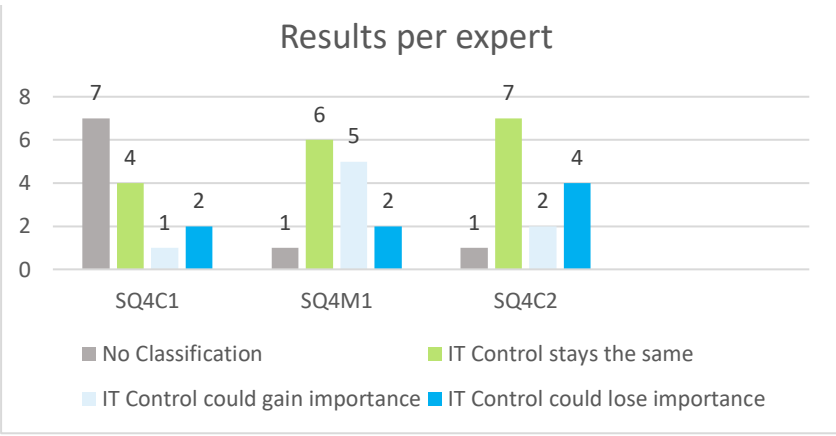

Figure 18 – Bar chart SQ4

Other observations are made:

- The experts have consensus on three out of the fourteen IT controls.
    - All three experts think that the IT control 'Cryptographic Key Establishment and Management' could become more important.
    - Furthermore, they share the same judgement on the IT control 'transmission Confidentiality and Integrity' as they consider it potentially losing importance. Hereby, it is important to note that one expert (SQ4C2) clearly mentions, that this is only true for the 'Integrity' part of the IT control.
    - At last, they agree on the IT control 'Information System Monitoring', holding the same amount of importance. Two experts (SQ4M1 and SQ4C2) note that some aspects of this IT control gain importance, and some aspects lose importance. The experts state that as blockchain is added to the IT infrastructure of the client, it is of critical nature to monitor and track attacks on the network. On the other side, as blockchain on itself is a log, adding transparency and making it easier to monitor and track attacks.

None of the experts think that the reviewed IT controls become redundant. Although, one of the experts does explicitly state that blockchain possesses the capability to cause redundancy of IT controls in the future (SQ4C2). As the experts were asked to review the IT controls with keeping in mind a general blockchain application, they made a lot of assumptions in their thought process. Therefore, they were asked to expand on the biggest factor influencing their thought process. The most important consideration that affects the application of IT controls in a blockchain setting, is the particular type of blockchain which is used, i.e., public or private blockchain. With respect to private blockchains, it is expected that potential changes will not be vast and disruptive as private blockchains are much more reminiscent of current IT environments then public blockchains. It becomes challenging, when we try to apply contemporary practices and frameworks in public blockchain settings, as it poses questions on the accountability and governance of systems. For example, unlike private or permissioned blockchains, public blockchains are open to all and do not inherently contain a 'back-door' for emergency situations. Technicalities as such, make it much more difficult to use contemporary frameworks and practices in a public blockchain setting. Consequentially, future researchers are advised to take this into account as it could pose to be a more interesting viewpoint for their research.

In sub chapter 2.2.2 we highlighted various perspectives of related research, some of those stating that blockchain was capable to reduce the role of auditing firms, and some emphasizing the changing role of IT auditors. Especially related to these views, the results of the review are also of interest as we can see how they reflect the results of this sub question.
From the results of the review of the IT controls and the included in-depth interview within this phase, we recognize that the experts do not think that blockchain would make the reviewed IT controls redundant. However, it is identified that blockchain has the capability to influence the IT controls in such a way that they can lose importance. Out of the 42 separate judgements, eight of the judgements indicated this classification(19%). This is particularly the case for IT controls related safeguarding the confidentiality, and integrity of information systems, and protecting information systems with cryptography.
Additionally, the results explain that blockchain also indicates that certain IT controls could require more emphasis, especially IT controls related to 'Key Management'.
As seen in the results, the majority of the judgments of the review indicated that the respective IT controls would require the same amount of importance. With regards to these IT controls the blockchain experts believe not much will change.

SQ5). How do the collected blockchain risks, map to the NIST SP 800-53 IT controls from subcategories PR.DS-1 and PR.DS-5?

From the results of the mapping we observe that 58 out of the 67 risks(86%) can either be associated with the IT controls or the overarching 'Data Security' category. However only 20 out of the 67(30%) blockchain risks can directly be mapped with the examined IT controls. The fact that larger part of the blockchain risks can be linked with the category does not come as a surprise, as blockchain after all is a digital ledger which contains data and is distributed via the internet.

From the direct mappings we point out several observations. For comprehension purposes a table is included on the next page highlighting which risks can directly be inked with which respective IT controls. The risks are abbreviated, the complete risk name can be seen below.

Abbreviation	Complete Risk	Blockchain Category
BAS-1	BAS-1 Wallet credential theft	Basic Blockchain Risks
BAS-2	BAS-2 Private key theft	
BAS-3	BAS-3 Private key forging	
BAS-4	BAS-4 Signature of rogue transaction	
BAS-5	BAS-5 Weak key generation software	
BAS-6	BAS-6 Resilience of asymmetric keys to 0-days/quantum computing	
BAS-7	BAS-7 Data protection & privacy violation (header data)	
BAS-8	BAS-8 Lack of forward secrecy	
BAS-23	BAS-23 Untrusted end-user computer (hacked account)	
BAS-25	BAS-25 Exploitation of the transaction protocol (hacked key)	
H-1	H-1 Hash collision	Hash Data Risks
GEN-1	GEN-1 Decryption of encrypted data	Generic Data Risks
GEN-3	GEN-3 Resilience of encryption scheme (confidential data)	
GEN-6	GEN-6 Storage of malicious data	
SC-1	SC-1 Privacy breach through vulnerability in smart contract	Smart Contract Risks
SC-2	SC-2 Security vulnerability in the smart contract	
SC-3	SC-3 Smart contract-powered denial of service	
PERM-6	PERM-6 Disclosure of internal processes	Permissioned Ledger Risks
PLESS-1	PLESS-1 User re-identification via transaction analysis	Permissionless Ledger Risks
OTH-1	OTH-1 Security vulnerability in the platform code (node-hosting cloud platform)	Other (Situational) Risks

Table 7 – Blockchain risk names

IT Controls **Risk sub categories**	SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	SC-28 PROTECTION OF INFORMATION AT REST	AC-5 SEPARATION OF DUTIES	AC-6 LEAST PRIVILEGE	PS-3 PERSONNEL SCREENING	PS-6 ACCESS AGREEMENTS	SC-7 BOUNDARY PROTECTION	SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY	SC-13 CRYPTOGRAPHIC PROTECTION	SI-4 INFORMATION SYSTEM MONITORING
Key management	BAS 1-4								BAS 1-4	
Cryptography	BAS-5 BAS-6								BAS-5 BAS-6	
Data protection and Privacy	BAS-8									BAS-8
Regulatory, antifraud and anti-money laundering techniques and mechanisms										BAS-23 BAS-25
Hash Data Risks										H-1
Capability of nodes to store arbitrary data onto the blockchain	GEN-3		GEN-1 GEN-6	GEN-1 GEN-6	GEN-1 GEN-6	GEN-1 GEN-6		GEN-3	GEN-3	GEN-1 GEN-6
Smart Contract Risks							SC-3	SC-1 SC-2		
Other Permissioned Ledgers Risks								PERM-6		
Other Permissionless Ledgers Risks		PLESS-1						PLESS-1		
Non-Categorical Situational Risks							OTH-1			

Table 8 – Level one links

From the table we observe that Gen-1(Decryption of encrypted data), and Gen-6(Storage of malicious data) can be mapped to a majority of the respective IT controls. This is the case as they discuss unauthorized access and abuse within the infrastructure which possibly can be mitigated by the affiliated IT controls(AC-5, AC-6, PS-3, PS-6 and SC-4). Furthermore, we observe that the blockchain risks regarding cryptographic key management and cryptographic protection (BAS1-6) are mapped with the IT controls with respect to cryptographic key establishment and management, and cryptographic protection(SC-12, SC-13).

Related to all the direct mappings it holds true that adjustments need to be made to the technicalities of blockchain. As blockchain proposes a unique concept, it is anticipated that contemporary IT controls are not a perfect fit. Therefore a 'plug-and-play' approach cannot be adopted. Illustrating, the IT control of SI-4 broadly dictates the organization to:

1. Firstly, to detect attacks, potential attacks and unauthorized access through the information system.
2. Secondly, deploys monitoring devices to collect and protect essential information (NIST, 2013).

As showcased in the table various blockchain risks which are particularly associated with attacks, hacked accounts or keys and malicious use, can be affiliated with this IT control. However, it is required for the organization to be informed about all the blockchain risks that either directly or indirectly can lead up to attacks and malicious use through unapproved access. This observation however, also demonstrates a strong suit of the reviewed IT controls: that of being flexible in approach and generically written to align it to your own interpretation.

Moving on to the indirect risks, and the risks that could not be mapped with either the IT controls or with the category of 'Data Security', we observe that a lot of these risks involve terms uniquely known to blockchain. These terms primarily involve smart contracts, wallet management, scalability, consensus management, permissioned ledgers consensus risks, cryptocurrency and the interoperability between different ledgers.
As only a selective number of IT controls were examined for this study, it is possible that IT controls from other sections are more related to one of these concepts. However, it is argued that some of the concepts are so unique it instills the notion that it requires supplemental attention.

7. Conclusion

This study aspired to analyze a contemporary framework within the IT audit sector for its' use in a risks assessment of a blockchain solution. The NIST Cyber Security framework was eventually chosen, and it can be concluded from the gathered information and results, that the framework on categorical and IT control level presents substantial value whilst also showing room for improvements. The framework from categorical and IT control level is perceived as generic, making it open for interpretation, and flexible to adapt it to the technicalities of blockchain. While the results prove the value of the framework, they also highlight certain aspects in which the framework lacks. As explained in the Discussion section, certain categories like 'Response Planning' within the framework, are not considered an adequate match with the functioning of blockchain.

The mapping of the blockchain risks also informs us about potential challenges. Blockchain risks involving smart contracts, wallet management, consensus management and permissioned ledgers consensus could not be directly addressed by the examined IT controls. Furthermore, risks involving cryptocurrency and interoperability are neither addressed by the respective IT controls nor can they be related to the category of 'Data Security'. These results indicate the significance of future IT control and blockchain related research.

For practitioners within (IT audit) it is difficult to uncover potential gaps related to blockchain, since they do not possess the required blockchain-associated knowledge. As blockchain becomes more integrated within businesses it is paramount to minimalize this weakness. Even with flexible frameworks and standards such as the NIST framework, additional knowledge on blockchain is advised to be incorporated within the process of a risk assessment. This could be accomplished by major firms such as the big four, by conducting regular trainings, and finetuning their audit methodologies. Audit methodologies are heavily influenced by international standardization organizations such as ISO, ISACA, COSO etc. It is necessary that this type of organizations take initiative to align their standards with technologies such as blockchain.

The study also questioned how practitioners perceived the importance of IT controls in response to a blockchain solution. The results present a nuanced view on how IT controls are impacted, as participants believe that a large part of the reviewed IT controls will require the same amount of importance. In certain instances, IT controls can possibly lose importance in response to a blockchain solution. This is primarily the case for IT controls related to safeguarding the confidentiality, and integrity of information systems, and protecting information systems with cryptography. The IT controls that were used for the review and the mapping are related to sub categories PR.DS1(Data-at-rest is protected) and PR.DS-5(Protections against data leaks are implemented), from the 'Data Security' category. Since they only account to a select amount of IT controls from the total framework, it limits the generalizability of these results. To create a better understanding of the results and simultaneously offer more value, future studies could address specific enterprise blockchain contexts in which corresponding IT controls are tested.

Blockchain prevails to be a topic that raises questions. It is crucial that practitioners and researchers stay ahead of the curve and keep innovating. Related to the (IT) audit sector, it is contemplated that innovation will occur incrementally as control frameworks and standards form a baseline. The study indicates that this does not necessarily has to be a restraining factor on the further integration of blockchain in our businesses.

7.1 Research limitations

This study is limited in several ways. As mentioned in chapter three, the scope of this study is limited to the NIST Cyber Security framework. NIST itself has other standards such as NIST SP800-175B standard which is a guideline for cryptographic standards and, NIST SP800-57 which is related to for key management. These standards were not included in this study as it exceeded the premises of the study. Furthermore, the generalizability of this study is limited. This being the consequence of focusing on one framework, and taking a selection of IT controls for the review. The results identified particular areas of improvement within the analyzed framework. However, since it was not a main purpose of the study to conduct a comprehensive gap-analysis it reveals a limit of this study.

7.2 Future research

From the research limitations we can derive opportunities for future research. As this study particularly focused on qualitative data, it would be of interest to see what the implications are of a study of quantitative nature. This could be incorporated with the potential mapping of the blockchain risks to not only one framework, but several frameworks. Consequently, it could inspire to the operationalization of an industry framework for blockchain risks.. At last, future researchers are stimulated to work from a more blockchain-oriented perspective, as this could extensively help with identifying gaps within contemporary audit frameworks.

Acknowledgements

Without the help of others my efforts to write this thesis would have been futile. I would like to use this section to express my gratitude to everyone who helped me along the way. First of all, I would like to thank my university supervisors dr. Werner. Heijstek and Eng. Mohamed Atef Ibrahim | MSc. Werner's supervision and extensive knowledge on research methodology, contributed significantly to the structure of my thesis.
Mohamed's expert feedback and guidance proved essential. As the result of his critical but thorough feedback, I was able to steer towards relevant aspects and ask myself critical questions. Both supervisors helped me with embracing critical perspectives which elevated the quality of my thesis.

Furthermore, I would like to thank my in-house supervisor Muhammad Khurshid. His guidance helped me immensely with finding my place within Deloitte. Muhammad fulfilled his responsibility as a coach exceptionally well, and I am very thankful for this. Moreover, I would like to thank Deloitte for giving me the opportunity to fulfill my graduation in-company. At last, I would like to thank everyone who participated in my thesis.

LIST OF FIGURES

LIST OF TABLES

Bibliography

27000.org. (n.d.). An Introduction To ISO 27001 (ISO27001). Retrieved from http://www.27000.org: http://www.27000.org/iso-27001.htm

Adams, R., Parry, G., Godsiff, P., & Ward, P. (2017). The future of money and further applications. Wiley. ontr

Andreessen, M. (2014, January 21). Why Bitcoin Matters. Retrieved from https://dealbook.nytimes.com: https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/?_php=true&_type=blogs&_r=0

Antonopoulos, A. M. (2017). Mastering Bitcoin. In A. M. Antonopoulos, Mastering Bitcoin (pp. 18-19). O'Reilly.

Baliga, A. (2017). Understanding Blockchain Consensus Models. Persistent Systems.

Baran, P. (1962). On Distributed Communication Networks. Santa Monica: The RAND Corporation.

Bashir, I. (2018). Mastering Blockchain. Birmingham: Packt Publishing.

Bauerle, N. (n.d.). What is Blockchain Technology? Retrieved from Coindesk: https://www.coindesk.com/information/what-is-blockchain-technology

Benos, E., Garratt, R., & Gurrola-Perez, P. (2017). The economics of distributed ledger technology for securities settlement. Bank of England.

Bis.org. (n.d.). Basel III: international regulatory framework for banks. Retrieved from https://www.bis.org: https://www.bis.org/bcbs/basel3.htm

blockchain-council. (2019, November 25). https://www.blockchain-council.org. Retrieved from HYPERLEDGER FABRIC – TOP USE CASES: https://www.blockchain-council.org/blockchain/hyperledger-fabric-top-use-cases/

Brink, H. (1993). VALIDITY AND RELIABILITY IN QUALITATIVE RESEARCH. Curationis.

Buterin, V. (2015, August 6). On Public and Private Blockchains. Retrieved from https://blog.ethereum.org: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

Cachin, C., & Vukolic, M. (2017). Blockchain Consensus Protocols in the Wild. zURICH: IBM Research.

Cangemi, M., & Brennan, G. (2019). BLOCKCHAIN AUDITING – ACCELERATING THE NEED FOR AUTOMATED! EDPACS, 59:4,, 1-11.

Capgemini. (2016, October). Consumers set to save up to sixteen billion dollars on banking and insurance fees thanks to blockchain-based smart contracts says Capgemini report. Retrieved from https://www.capgemini.com/news: https://www.capgemini.com/news/consumers-set-to-save-up-to-sixteen-billion-dollars-on-banking-and-insurance-fees-thanks-to/

Catalini, C., & Gans, J. (2016). SOME SIMPLE ECONOMICS OF THE BLOCKCHAIN. Cambridge: NATIONAL BUREAU OF ECONOMIC RESEARCH.

Coindesk. (2018, July 19). All 'big four' auditors to trial blockchain platform for financial reporting. Retrieved from https://www.coindesk.com: https://www.coindesk.com/all-big-four-auditors-trial-blockchain-platform-for-financial-reporting

Cointelegraph. (2018, November). Bank of America Has the Most Blockchain Patents, But Is It Actually Going to Use Them? Retrieved from https://cointelegraph.com: https://cointelegraph.com/news/bank-of-america-has-the-most-blockchain-patents-but-is-it-actually-going-to-use-them

ComputerworldUK. (2019, February 7). How governments around the world are using blockchain . Retrieved from https://www.computerworlduk.com.

Consultancy.uk. (2017, March 02). The potential of blockchain as a future financial services infrastructure. Retrieved from https://www.consultancy.uk/: https://www.consultancy.uk/news/13099/the-potential-of-blockchain-as-a-future-financial-services-infrastructure

Consulting.com. (n.d.). The Complete Guide To Big 4 Consulting. Retrieved from https://www.consulting.com: https://www.consulting.com/big-4-consulting

COSO. (n.d.). COSO About Us. Retrieved from https://www.coso.org: https://www.coso.org/Pages/aboutus.aspx
CPA Canada and AICPA. (2017). Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession. Deloitte.
Crosby, M., Nachiappan, Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). BlockChain Technology: Beyond Bitcoin. Applied Innovation Review.
Crosby, M., Nachiappan, Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). BlockChain Technology: Beyond Bitcoin . Applied Innovation Review.
Dai, J. (2017). THREE ESSAYS ON AUDIT TECHNOLOGY: AUDIT 4.0, BLOCKCHAIN, AND AUDIT APP. Newark, New Jersey: The State University of New Jersey.
Deloitte. (2018). Breaking Blockchain Open; Deloitte's 2018 global blockchain survey. Deloitte.
Drescher, D. (2017). Blockchain Basics. In D. Drescher, Blockchain Basics (pp. 98-100). Apress.
Drescher, D. (2017). Blockchain Basics. In D. Drescher, Blockchain Basics (pp. 105-108). Apress.
Drescher, D. (2017). Blockchain-basics; Non technical introduction in 25 steps. In D. Drescher, Blockchain-basics; Non technical introduction in 25 steps (pp. 70-71). Apress.
Dutch Blockchain Coalition. (2018). Blockchain Security, A Framework for Trust and Adoption.
EUIPO. (2019, February 07). Using blockchain in the fight against counterfeiting - EUIPO launches a Forum to support concrete solutions in that field. Retrieved from https://euipo.europa.eu: https://euipo.europa.eu/ohimportal/nl/news/-/action/view/4963920
Forbes. (2018, August). Goldman Sachs And J.P. Morgan Join $32M Series B In Enterprise Blockchain Startup Axoni. Retrieved from https://www.forbes.com: https://www.forbes.com/sites/michaeldelcastillo/2018/08/14/goldman-sachs-and-jp-morgan-join-32m-series-b-in-enterprise-blockchain-startup-axoni/#2da8795b6276
Frøystad, P., & Holm, J. (2015). Blockchain: Powering the Internet of Value. Evry.
Franco, P. (2015). Understanding Bitcoin - Cryptography, engineering, and economics. In P. Franco, Understanding Bitcoin - Cryptography, engineering, and economics (pp. 95-96). Chichester: Wiley.
Gartner. (2018, August). 5 Trends Emerge in the Gartner Hype Cycle for Emerging Technologies, 2018. Retrieved from https://www.gartner.com/: https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/
Gartner. (2019, October 19). Gartner 2019 Hype Cycle Shows Most Blockchain Technologies Are Still Five to 10 Years Away From Transformational Impact. Retrieved from https://www.gartner.com: https://www.gartner.com/en/newsroom/press-releases/2019-10-08-gartner-2019-hype-cycle-shows-most-blockchain-technologies-are-still-five-to-10-years-away-from-transformational-impact
Gartner. (n.d.). Gartner Hype Cycle. Retrieved from https://www.gartner.com/: https://www.gartner.com/en/research/methodologies/gartner-hype-cycle
Ghauri, P., & Grønhaug, K. (2005). Research Methods in Business Studies: A Practical Guide. In P. Ghauri, & K. Grønhaug, Research Methods in Business Studies: A Practical Guide (p. 16). Pears Education.
Golafshani, N. (2013). Understanding Reliability and Validity in. The Qualitative Report.
Grounded Theory Institute. (2016, July 20). What is Grounded Theory? Retrieved from http://www.groundedtheory.com: http://www.groundedtheory.com/what-is-gt.aspx
Haber, S., & Stornetta, W. (1991). How to time-stamp a digital document. Journal of Cruptology.
HFS Research. (2018, March 1). Who's Winning the Battle of Enterprise Blockchain Platforms? Retrieved from https://www.hfsresearch.com/: https://www.hfsresearch.com/pointsofview/whos-winning-the-battle-of-enterprise-blockchain-platforms
Huang, S.-M., Hung, W.-H., Yen, D., Cheng Chang, I., & Jiang, D. (2010). Building the evaluation model of the IT general control for CPAs under enterprise. Elsevier.

IAASB. (n.d.). International Auditing and Assurance Standards Board. Retrieved from https://www.iaasb.org: https://www.iaasb.org/about-iaasb
Infosec Institute. (2019, May 14). Guide to COBIT 2019. Retrieved from https://resources.infosecinstitute.com/: https://resources.infosecinstitute.com/guide-to-cobit-2019/#gref
Investopedia. (2019, March 03). Bootstrapping. Retrieved from Investopedia.com: https://www.investopedia.com/terms/b/bootstrapping.asp
Investopedia. (2019, April 26). Smart Contracts. Retrieved from Investopedia.com: https://www.investopedia.com/terms/s/smart-contracts.asp
ISACA. (n.d.). Retrieved from http://www.isaca.org/: http://www.isaca.org/COBIT/
ISACA - Protiviti. (2018). A Global Look At IT Audit Best Practices - Assessing the International Leaders in an Annual ISACA-Protiviti Survey. ISACA.
ISACA. (2019). Blockchain Preparation Audit Program . Retrieved from https://www.isaca.org/: https://www.isaca.org/bookstore/audit-control-and-security-essentials/wapbap
ISO. (2018). ISO/TC 307 Blockchain and distributed ledger technologies. Retrieved from https://www.iso.org/: https://www.iso.org/standard/73771.html
J.P. Morgan. (n.d.). Retrieved from https://www.jpmorgan.com/: https://www.jpmorgan.com/global/Quorum
Jackson, B. (2018). Understanding the Implication of Blockchain. Florida: STARS .
Lamport , L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem . ACM Transactions on Programming Languages and Systems, 382-401.
Laurence, T. (2017). Blockchain For Dummies. Wiley & Sons.
Mainelli, M., & Smith, M. (2015). Sharing Ledgers for Sharing Economies: exploration of mutual distributed ledgers (aka blockchain technology). EY Global Financial Services Institute.
McKinsey & Company. (2018, June). Blockchain beyond the hype: What is the strategic business value? Retrieved from https://www.mckinsey.com: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value
Medium. (2018, October 2). Blockchain: Public Sector Use Cases. Retrieved from https://medium.com: https://medium.com/crypto-oracle/blockchain-public-sector-use-cases-49a2d74ad946
Medium.com - BlockstreetHQ Team. (2018, September 6). Before Blockchain, There Was Distributed Ledger Technology. Retrieved from Medium.com: https://medium.com/blockstreethq/before-blockchain-there-was-distributed-ledger-technology-319d0295f011
Medium.com - Debraj Ghosh. (2016, April 5). How the Byzantine General Sacked the Castle: A Look Into Blockchain. Retrieved from Medium.com: https://medium.com/@DebrajG/how-the-byzantine-general-sacked-the-castle-a-look-into-blockchain-370fe637502c
Meyne, N. (Director). (2016). Blockchain: Real World Use Cases [Motion Picture].
Moeller, R. (2010). IT Audit, Control, and Security. In R. Moeller, IT Audit, Control, and Security (p. 5). Hoboken: Wiley.
Morabito, V. (2017). Business Innovation through Blockchain. In V. Morabito, Business Innovation through Blockchain. Springer.
Mougayar, W. (2016). The Business Blockchain. In W. Mougayar, The Business Blockchain. Wiley.
Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
Nathalie, B., Marion, G., Jean-Henry, M., & Arber, S. (2019). POTENTIAL IMPACT OF BLOCKCHAIN ON AUDIT PRACTICE. Journal of Strategic Innovation and Sustainability.
National Institute of Standards and Technology. (2014, February 12). Cybersecurity Framework. Retrieved from https://www.nist.gov: https://www.nist.gov/cyberframework
National Institute of Standards and Technology. (2014). Framework for Improving Critical Infrastructure Cybersecurity . National Institute of Standards and Technology.

ObamaWhitehouse. (2013, February 12). Executive Order -- Improving Critical Infrastructure Cybersecurity. Retrieved from https://obamawhitehouse.archives.gov: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
Patton, M. (1990). Qualitative evaluation and research methods. In M. Patton, Qualitative evaluation and research methods (p. 182). Beverly Hills: SAGE.
Patton, M. (2002). Qualitative Research and Evaluation Methods. In M. Patton, Qualitative Research and Evaluation Methods (pp. 230-242). SAGE.
Perez, Y. B. (2015, july). Santander: Blockchain Tech Can Save Banks $20 Billion a Year. Retrieved from https://www.coindesk.com/: https://www.coindesk.com/santander-blockchain-tech-can-save-banks-20-billion-a-year
Peters, G. W., & Panayi, E. (2015). Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money . London: Department of Statistical Science, University College London.
Pilkington, M. (2016). Blockchain Technology: Principles and Applications. University of Burgundy, France.
Polit, D., & Beck, C. (2010). Generalization in quantitative and qualitative research:. New York: Elsevier.
Pompon, R. (2016). IT Security Risk Control Management, An Audit Preperation Plan. In R. Pompon, IT Security Risk Control Management, An Audit Preperation Plan (pp. 6-7). Seattle: Apress.
Psaila, S. (2017, September 22). Blockchain: A game changer for audit processes? Retrieved from https://www2.deloitte.com: https://www2.deloitte.com/content/dam/Deloitte/mt/Documents/audit/dt_mt_article_blockchain_gamechanger-for-audit-sandro-psaila.pdf
Punch, K. (2013). Introduction to Social Research: Quantitative and Qualitative Approaches. In K. Punch, Introduction to Social Research: Quantitative and Qualitative Approaches (p. 3). SAGE.
PWC. (2018). Blockchain is here. What's your next move? Retrieved from https://www.pwc.com/: https://www.pwc.com/gx/en/issues/blockchain/blockchain-in-business.html
Saldana, J. (2011). Fundamentals Of Qualitative Research. In J. Saldana, Fundamentals Of Qualitative Research (p. 76). Oxford Unitversity Press.
Salkind, N. J. (2010). Encyclopedia of Research Design. In N. J. Salkind, Encyclopedia of Research Design (p. 1254). Sage Publications.
Sarkar, P. (2011, December 9). Hash Functions: A Gentle Introduction. Kolkata, India.
Sekaran, U., & Bougie, R. (2009). Research Methods for Business. In U. Sekaran, & R. Bougie, Research Methods for Business. Wiley.
Sheldon, M. D. (2018, December). A Primer for Information Technology General Control. University Heights, Ohio, United States.
Sheldon, M. D. (2019). A Primer for Information Technology General Control Considerations on a Private and Permissioned Blockchain Audit. American Accounting Association.
Swan, M. (2015). Blockchain - Blueprint for a new economy. O'Reilly.
Swan, M. (2015). Blockchain, Blueprint for a New Economy. In M. Swan, Blockchain, Blueprint for a New Economy (p. 92). O'Reilly.
Szabo, N. (1996). Smart Contracts: Building Blocks for Digital Markets. Retrieved from http://www.fon.hum.uva.nl/: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html
Tapscott, A. T. (2017). How Blockchain Is Changing Finance. Harvard Business Review.
Tashakkori, A., & Teddlie, C. (2003). Handbook of mixed methods in social & behavioral research. SAGE Publications.

The Institute of Chartered Accountants in England and Wales. (2018). Blockchain and the. ICAEW.
The Institute of Internal Auditors. (n.d.). Global Technology Audit Guide (GTAG) 17: Auditing IT Governance. Retrieved from https://na.theiia.org/: https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG17.aspx
TheNextWeb. (2018, July 27). Here's the difference between blockchain and distributed ledger technology. Retrieved from https://thenextweb.com: https://thenextweb.com/hardfork/2018/07/27/distributed-ledger-technology-blockchain/
U.S. General Services Administration. (n.d.). NIST Cybersecurity Framework (CSF). Retrieved from https://www.gsa.gov: https://www.gsa.gov/technology/technology-products-services/it-security/nist-cybersecurity-framework-csf
van Niekerk, J., & von Solms, R. (2012). From information security to cyber security. Port Elizabeth: Elsevier.
Walport, S. M. (2016). Distributed Ledger Technology: beyond block chain. UK Government.
Wang, Y., & Kogan, A. (2018). Designing confidentiality-preserving Blockchain-based transactionprocessing systems. Elsevier.
Whittington Associates. (n.d.). Audit Princples. Retrieved from whittingtonassociates.com: https://www.whittingtonassociates.com/2014/02/audit-principles/
World Economic Forum. (August 2016). The future of financial infrastructure An ambitious look at how blockchain can reshape financial services. World Economic Forum.
Yermack, D. (2017). Corporate Governance and Blockchains. Oxford University Press on behalf of the European Finance Association.

Appendices

Appendix A- Findings per sub question

The findings per sub question cannot be disclosed due to confidentiality reasons. This appendix is delivered separately.

Annex

Annex A – Theoretical blockchain risks

This annex is delivered separately.