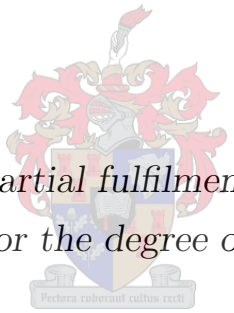
Blockchain Feasibility Assessment – A Quantitative Approach

by

Scott Spencer-Hicken



Thesis presented in partial fulfilment of the requirements for the degree of

Master of Engineering (Engineering Management)

in the Faculty of Engineering at Stellenbosch University

Supervisor: Professor C.S.L. Schutte

Co-supervisor: Professor P.J. Vlok

December 2022

Declaration

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Date: August 2022 .....

Abstract

Blockchain Feasibility Assessment – A Quantitative Approach

S. Spencer-Hicken

Department of Industrial Engineering,
University of Stellenbosch,
Private Bag X1, 7602 Matieland, South Africa.

Thesis: MEng (Engineering Management)

December 2022

This masters thesis involves the development of a blockchain assessment framework that is used to assess the technical suitability, detail design, adoption approach, economical feasibility, and business value potential of a blockchain solution within an organization for a specific process. The main aim of the study is to assess these elements using an assessment framework, while remaining generic and providing outputs that enable better decision-making regarding blockchain implementation.

Blockchain is a nascent technology that is capable of disrupting the foundations of multiple industries. Blockchain solutions possess many desirable functional characteristics such as transparency, immutability, and decentralization among others. These useful characteristics have surrounded blockchain with hype, which has consequently lead to people attempting to create blockchain solutions without fully understanding what the technology is capable of, resulting in extremely high project failure rates. Academic researchers have attempted to reduce these failure rates by creating a better understanding of blockchain and many researchers have created assessment approaches for assessing blockchain within different contexts.

However, these assessment approaches are often specific to very narrow use cases or the assessment approach is not comprehensive and only assesses one particular aspect of blockchain. This highlights the need for a comprehensive and generic blockchain assessment approach to identify whether blockchain is a viable solution for an organization within a given context.

The aim of this study is to address this need by creating an assessment framework that can be used to identify whether a blockchain solution is worth investing time, money and effort into. A literature review is completed which investigates blockchain technology, its

operation and its typical components along with other fundamental concepts required to design the necessary framework. This literature review is used to identify the relevant design requirements for the assessment framework, which is then designed in full.

The assessment framework is demonstrated with the use of a case study and is validated using expert analysis. This demonstration and validation are used to enhance the design of the framework and identify future areas of improvement. The value of the framework for the initial evaluation of blockchain solutions and for creating momentum for further blockchain exploration is proven through the validation efforts. The study concludes with the limitations of the research and recommendations for future research.

Opsomming

'n Kwantitatiewe Assesseringsbenadering vir Blokketting Gangbaarheid

S. Spencer-Hicken

Departement van Bedryfsingenieurswese
Universiteit van Stellenbosch
Privaatsak X1, 7602 Matieland, Suid Afrika

Tesis: MIng (Ingenieursbestuur)

Desember 2022

Hierdie tesis behels die ontwikkeling van 'n blokketting-assesseringsraamwerk wat gebruik kan word om die tegniese geskiktheid, detailontwerp, aanvaardingsbenadering, ekonomiese haalbaarheid en besigheidswaardepotensiaal van 'n blokkettingoplossing binne 'n organisasie vir 'n spesifieke proses te assesseer. Die hoofdoel van die studie is om hierdie elemente te assesseer deur 'n assesseringsraamwerk te gebruik, terwyl dit generies bly en uitsette verskaf wat beter besluitneming rakende blokkettingimplementering moontlik maak.

Blokkettings is ontluikende tegnologie wat in staat is om die fondamente van verskeie nywerhede te ontwrig. Blokketting-oplossings beskik oor vele gewenste funksionele eienskappe soos onder andere deursigtigheid, onveranderlikheid en desentralisasie. Hierdie nuttige eienskappe het blokkettings baie publisiteit gegee, wat gevolglik daartoe gelei het dat mense probeer het om blokketting-oplossings te skep sonder om ten volle te verstaan waartoe die tegnologie in staat is, wat tot uiters hoë projekmislukkingskoerse gelei het. Akademiese navorsers het probeer om hierdie mislukkingsyfers te verminder deur 'n beter begrip van blokketting te skep en baie navorsers het assesseringsbenaderings geskep om blokkettings binne verskillende kontekste te assesseer.

Hierdie assesseringsbenaderings is egter dikwels doelgemaak vir baie spesifieke gebruiksgevalle of die assesseringsbenadering is nie omvattend nie en assesseer slegs een spesifieke aspek van blokketting. Dit beklemtoon die behoefte aan 'n omvattende en generiese blokkettingassesseringsbenadering om te besluit of 'n blokketting 'n lewensvatbare oplossing vir 'n organisasie binne 'n gegewe konteks is.

Die doel van hierdie studie is om hierdie behoefte aan te spreek deur 'n assesseringsraamwerk te ontwikkel wat gebruik kan word om te identifiseer of 'n blokkettingoplossing die moeite werd is om tyd, geld en moeite in te belê. 'n Literatuuroorsig is gedoen wat blokkettingtegnologie, die werking daarvan en die tipiese komponente daarvan ondersoek, tesame met ander fundamentele konsepte wat nodig is om die nodige raamwerk te ontwerp. Hierdie literatuuroorsig word gebruik om die relevante ontwerpvereistes vir die assesseringsraamwerk te identifiseer, wat dan volledig ontwerp word.

Die assesseringsraamwerk word gedemonstreer met die gebruik van 'n gevallestudie en word bevestig met behulp van deskundiges. Hierdie demonstrasie en validasie word gebruik om die ontwerp van die raamwerk te verbeter en toekomstige areas van verbetering te identifiseer. Die waarde van die raamwerk vir die aanvanklike evaluering van blokkettingoplossings en vir die skep van momentum vir verdere blokkettingverkenning word bewys deur die validasie. Die studie sluit af met die beperkings van die navorsing en aanbevelings vir toekomstige navorsing.

Acknowledgements

Firstly, I would like to thank both of my supervisors, Prof Schutte and Prof Vlok for providing me with the opportunity to pursue my master's degree and for the guidance that was provided constantly throughout my studies in our weekly catch-up meetings. I appreciate the patience you had with my ever-evolving ideas and for encouraging this idea evolution to eventually arrive at the topic I ended up with. Finally, thank you for the time and effort that you put into understanding this topic that was very new to all of us and for providing guidance that was invaluable and for ultimately helping me shape the thesis I ended up with.

Furthermore, I would like to thank the company and company experts that were involved with the demonstration and validation of this study's outcome. Without your time and input, this study's outcome would not have been validated as it is.

To my girlfriend Micaela. Thank you for pushing me to pursue my master's degree. Thank you for the love, patience, and support you provided me throughout my studies and for constantly motivating me when motivation was low. Your love and motivation means the world to me and I look forward to doing the same for you next year when you pursue your own master's degree.

Finally, I would like to thank all of my family and friends for all of the support and understanding and for making my breaks fun and refreshing, allowing me to tackle my work even harder. Thank you.

Contents

List of Figures

List of Tables

Abbreviations

AML Anti-money laundering

ATOMIC Assets, Trust, Ownership, Money, Identity, and Contracts

DPoS Delegated-Proof-of-Stake

EA Enterprise Architecture

EAM Enterprise Asset Management

EAMS Enterprise Asset Management System

FMC Facility Management Corporation

GRAAL Guidelines Regarding Architecture Alignment

IS Information System

IT Information Technology

KYC Know your customer

P2P Peer-to-Peer

pBFT Practical Byzantine Fault Tolerance

PSS Product-Service System

PoA Proof-of-Authority

PoC Proof of Concept

PoET Proof-of-Elapsed-Time

PoS Proof-of-Stake

PoW Proof-of-Work

ROI Return on Investment

TPC Transactions Per CPU

TPDIO Transactions Per Disk I/O

TPMS Transactions Per Memory Second

TPND Transactions Per Network Data

tps transactions per second

USD United States Dollar

ZAR South African Rand

1 INTRODUCTION

The purpose of Chapter 1 is to create a general understanding of the research problem, the research questions required to understand the problem, the research objectives to complete, the scope of the study and the research method adopted for creating a solution to address the research problem. The chapter concludes with a brief layout description for the ensuing research study.

1.1 Background

Technology is continually becoming more vital in the success of a multitude of organizations, where it can be used to enhance the competitiveness and productivity of these organizations (Oliveira & Martins, 2011). Technology enables organizations to realize new opportunities and create more effective and efficient ways of doing typical organizational activities. However, the benefits of technology are often only realized by adopting the technology into the organization and in a lot of cases the technology may require that many organizations adopt it for maximum value due to network effects (Oliveira & Martins, 2011). There is a plethora of literature available on the adoption of a variety of technologies, ranging from telephones all the way to sophisticated databases. Furthermore, there is ample expertise available to help organizations with the adoption of these more common technologies. The problem lies where new, disruptive technologies enter the market that have the capacity to change the foundation on which many organizations operate and which leave little time to make an adoption decision.

Enter the novel blockchain technology. Blockchain is an emerging technology with the potential to disrupt the foundations of certain organizations in a variety of industries (Risius & Spohrer, 2017; Sikorski *et al.*, 2017). Many people immediately make the connection between blockchain and Bitcoin, because Bitcoin was the first and is the most well-known application of blockchain. Blockchain, however, is not limited to the financial industry and has potential in multiple industries ranging from government to energy to food (Taskinsoy, 2019; Garcia-Torres *et al.*, 2019; Brilliantova & Thurner, 2019; Bürer *et al.*, 2019; Allessie, 2017). Some have considered blockchain to be the solution to all modern-day organizational problems, but blockchain has proven to be more situational than previously expected. However, the copious beneficial characteristics of blockchain solutions have attracted many supporters and enticed them to take the risk of investing in blockchain projects.

To understand how the characteristics of blockchain are materialized, a narrow technical understanding of blockchain is required. As the name suggests, blockchain is

fundamentally a series of blocks "chained" to one another using cryptography, whereby each block contains information representing a new instance of the previous block. It is a type of distributed digital ledger that usually operates without a central authority or central repository (Yaga *et al.*, 2019). It accomplishes this by using one of a wide variety of consensus mechanisms, where Proof-of-Work (PoW) is the most well-known due to its large market capitalization within current cryptocurrencies (Gervais *et al.*, 2016). Blockchain has many definitions, without a universally agreed upon definition, which may be due to blockchain being new and hence not fully understood. However, assessing the different uses of blockchain and its key elements, an all-encompassing definition of it is proposed by Sultan *et al.* (2018) to be:

> *"A decentralized database containing sequential, cryptographically linked blocks of digitally signed asset transactions, governed by a consensus model"* – Sultan *et al.* (2018, pg. 54)

A block in a blockchain can be conceptualized as a mechanism for storing a group of transactions that occur at the same time instant and are chronologically chained to other blocks to form an immutable digital ledger (Fernández Caramés & Fraga Lamas, 2020). Each block in a blockchain typically consists of the block header and the block body (Nofer *et al.*, 2017; Zheng *et al.*, 2018*b*; Yaga *et al.*, 2019). The block header contains information on the block version, block hash, parent block hash, and timestamp, while the block body will contain the transactions the blockchain records, as well as any other necessary extras. More in-depth explanations of each component are explored in Section 2.1.3. An illustration of these block components in a typical blockchain is shown in Figure 1.1.

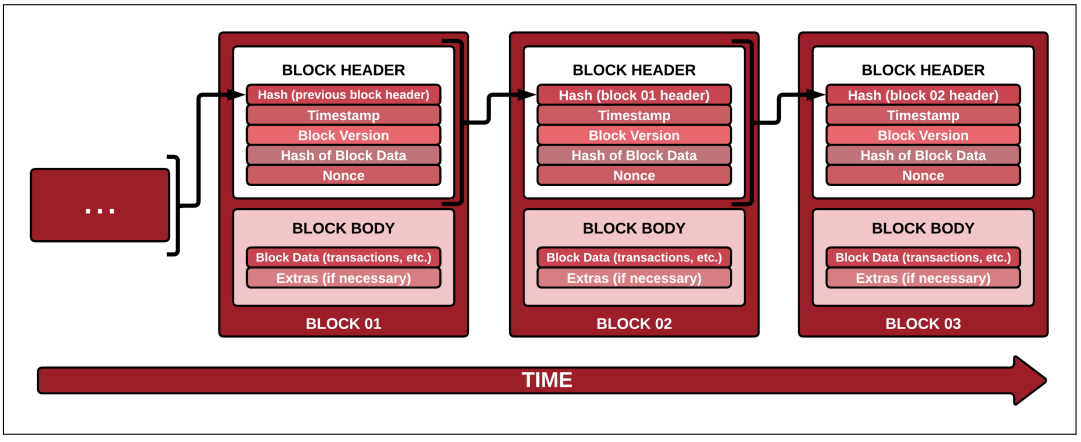


Figure 1.1: Blockchain Block Components

To understand the essence of a blockchain, only the key components of the block need to be understood. The hash (merkle tree root hash) is a 64-character hexadecimal string that is generated based on the data in the block and any change in the block data, even spacing between characters, will produce a completely new and unique hash value (Yaga *et al.*, 2019).

Forming part of the block data with which the hash value is generated, is the hash of the parent block, which is the block before the current block. This is the mechanism by which blocks in a blockchain are linked, because any change in the parent block data will change its hash value and in turn the hash value of the next block will change because the parent block's hash value is part of its data and therefore all hashes after the altered block will have to be updated, requiring immense time and effort.

Hashing, while appearing complicated, is a trivial task for modern day computers and thus consensus mechanisms are used to ensure that a new block being added correlates with the previous blockchain data, in an environment without trust and ensures no one can alter previous blocks without requiring immense computational power, time, or authority (Zheng *et al.*, 2018*b*). Swanson (2015) describes consensus mechanisms as "the process in which a majority (or in some cases all) of network validators come to agreement on the state of a ledger. It is a set of rules and procedures that allows maintaining a coherent set of facts between multiple participating nodes." There are many consensus mechanisms with differing characteristics and benefits and the selection of a suitable one is far from straight-forward. As mentioned previously, PoW is the most common consensus mechanism, whereby nodes, devices connected to the blockchain (Casino *et al.*, 2019), are required to expend effort in solving a computational puzzle to ensure block addition is not instantaneous (Zheng *et al.*, 2018*b*). For Bitcoin the PoW puzzle difficulty is adjusted, so that it takes roughly ten minutes to solve and add another block to the Bitcoin blockchain (Bonneau *et al.*, 2015). An in-depth analysis of the most common consensus mechanisms is presented in Section 2.1.5.

One can begin to understand how hashing and consensus mechanisms can make blockchains more secure, but a third characteristic that takes it to a new level is its shared and distributed nature. The ledger of transactions is shared among participants on the blockchain, which enables transparency among users (Yaga *et al.*, 2019). The users with access to the blockchain depends on the type of permissions the blockchain was developed with (Pilkington, 2016). As an example, Bitcoin is a public permissionless blockchain which means that anyone can join and validate transactions and have access

to all of the transactions on the blockchain (Underwood, 2016). Furthermore, the nodes of a blockchain solution are able to be distributed and thus allow anyone to join from anywhere with an internet connection and thus creates a system in which there is no single point of failure.

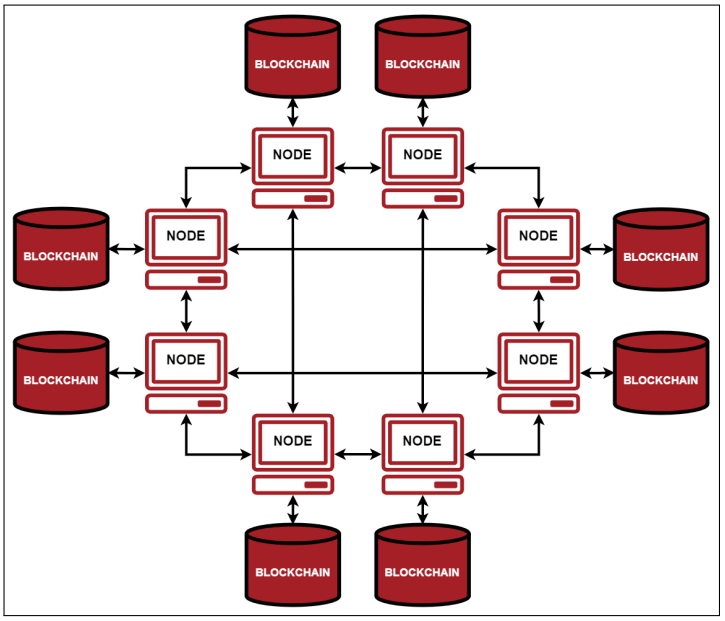


Figure 1.2: Blockchain Distributed Network

With a basic understanding of the fundamentals of blockchain, one can begin to understand the benefits that employing a blockchain solution may have. Firstly, blockchains are near immutable because of the vast amount of effort that would have to be expended to tamper with an existing block (Yaga *et al.*, 2019). However vast and unreasonable the amount of effort needed, it is still possible to tamper with a blockchain. To successfully tamper with a Bitcoin transaction block, you would be required to do the PoW for every block after the tampered block because of the hashing connections between blocks and furthermore you would have to take control of more than 50% of the nodes to accept the tampered block (Bastiaan, 2015). This is known as a 51% attack and clearly, the more nodes there are and the further back the transaction block, the harder an attack will be, because the amount of devices one would need and the amount of data one would have to change increases as the blockchain grows.

Before the introduction of blockchain, distrusting parties would rely on mutually trusted intermediary parties to facilitate transactions. This gives the control of transactions to one party, who will in turn charge for their services and could be subject to fraudulent activities. Perhaps the greatest benefit of blockchain is its ability to not have to rely on an

intermediary party to create trust between two distrusting parties (Pilkington, 2016). This trust is facilitated through its distributed nature and the consensus mechanism validating new additions to the blockchain by verifying that the new data is in line with previous transactions. Therefore, blockchain requires users to trust the system, rather than having to trust other parties that may have different interests and thus allows these parties to interact in a meaningful way without the need for an intermediary.

Furthermore, the shared and distributed nature of blockchain allows an elevated level of transparency that is not easy to achieve. This level of transparency is facilitated through blockchain's distributed and shared nature, allowing anyone on the network access to the entire transaction history of the blockchain. With this transparency and the immutability of blockchain, it allows auditing of transactions to be completed extremely effectively because transactions can be traced back to their origin and no data can be manipulated without immense effort or the knowledge of the users (Zheng *et al.*, 2018*b*).

Unfortunately even with these benefits, it still has its drawbacks and blockchain is certainly not suitable for all cases, with some sources claiming blockchain project failure rates as high as 92% (Bellini *et al.*, 2019). Blockchain has been hyped up to a point where expectations are far exceeding the capabilities of it and this leads to blockchain projects where the technology is neither necessary nor beneficial. This tends to occur with nascent technologies that are not fully understood, where misconceptions are born out of excessive fanfare and the fear of missing out pushes forward projects that would never be successful and thus leads to high project failure rates (Yaga *et al.*, 2019).

1.2 Research Opportunity

Blockchain has the potential to disrupt the foundations of certain industries and change the way in which business is done, but it is far from the be-all-end-all. The excessive fanfare surrounding blockchain, coupled with a general misunderstanding of its true capabilities, could eventually lead to a point where blockchain is seen as a technology that never quite lived up to its expectations and consequently becomes an overhyped technology without any business value. All this without ever actually appreciating what blockchain can offer and what it can do to potentially solve many modern-day business problems, from solving big data challenges to enabling more transparent supply chains (Karafiloski *&* Mishev, 2017; Singhal *et al.*, 2018).

However, academics have realized the value of blockchain and have consequently sought to address the general misunderstanding of it. Accordingly, a library of extant resources

that help to understand and realize the true potential of blockchain technology has accumulated since the release of Bitcoin's white paper by Nakamoto (2008). The literature has explored various topics on blockchain with varying depths, ranging from general overviews of the technology to comprehensive research on a particular aspect such as consensus mechanisms to in-depth case study evaluations.

To address the high project failure rates, a large portion of blockchain research has gone into the assessment of the technical suitability, economical feasibility, and business value potential of a blockchain solution for different use cases. However, blockchain is a complicated technology with many design considerations and assessing these aspects is a challenging undertaking, with the potential subsequent adoption being equally challenging (Singhal *et al.*, 2018; Yang *et al.*, 2021). Consequently, most blockchain assessment studies addressing technical suitability, adoption approaches, economical feasibility, and business value potential (simply referred to as blockchain assessment from here on out) have concentrated on specific, focused cases rather than attempting to create generic approaches, because of the many variables involved in the process of assessing blockchain for varying use cases.

While the scope of many of these studies are limited to very specific uses cases, there is still insight that can be gained from such studies to be applied to a generic blockchain assessment approach. However, a generic blockchain assessment approach stands to produce more value than concentrating on specific, focused use cases because of the amount of organizations that are able to gain insight from the use of such an approach, as opposed to just a handful of organizations with specific use cases.

Regardless of the complexity of creating a generic blockchain assessment approach, there have been multiple attempts at creating it in the hopes of harbouring a better understanding of blockchain and where it belongs. These generic approaches have assessed various aspects of blockchain assessment, including – but not limited to – blockchain technical suitability, blockchain economical feasibility, blockchain detail design, adoption approach, and business value. Intuitively, a complete assessment of blockchain would include all of these aspects to a certain extent, so that a complete picture of a blockchain solutions can be formed and can be adequately compared to a more traditional solution to allow better decision making. All of these aspects are present to some degree in the current literature.

There have been multiple, in-depth attempts at certain aspects, while other aspects have been only briefly researched. Blockchain literature has a plethora of technical suitability

analyses, from simple yes/no questions to in-depth fit scores determined through a variety of questions. The main approach of these analyses look at whether blockchain is technically suitable for a particular use case based on fundamental questions and a brave few venture into determining how suitable it is using more varied and in-depth questions.

Blockchain detail design is addressed less than the technical suitability analyses, but there is still plenty literature to help with the design decisions of blockchain development, such as consensus mechanisms, scalability, performance, permissions, and storage along with others. This aspect of blockchain assessment is more scattered, with certain decisions addressed in some studies but not in others. Currently, many studies fail to encompass all blockchain detail design decisions and the effect they have on one another or they neglect to translate these design decisions into meaningful outcomes to help with blockchain assessment for a particular use case. Furthermore, these design decisions are often left up to the subjective views and biases of the user, rather than attempting to make it as objective as possible.

Unfortunately, this is where blockchain literature starts to dwindle. Adoption approaches, economical feasibility, and blockchain business value potential are present but to a much lesser degree than the above aspects. The studies are either very focused or are simply not detailed enough to help organizations with blockchain assessment. However, the literature is not completely useless and still provides insight that can be coupled with empirical data to provide an approach that can help organizations with these blockchain assessment aspects.

Studies in blockchain literature rarely address all aspects of blockchain assessment mentioned above and hence all these blockchain assessment aspects are scattered, making it a challenging and time-consuming task for organizations to utilize generic approaches to assess blockchain solutions for their specific use case. An alternative approach to assessing blockchain, rather than using academic literature, would be to hire a blockchain professional and/or researcher that can determine the benefits of blockchain for the organization, but this would be a lengthy and expensive process. All of this highlights the opportunity within current academic blockchain literature, allowing the problem statement to be defined below.

PROBLEM STATEMENT

Literature on the assessment of fundamental blockchain aspects within organizations – technical suitability, detail design, adoption approach, economical feasibility, business value potential – is scattered and often lacks either generality or thoroughness. Consequently, blockchain assessment is a tedious process and often yields subpar results.

The above problem statement summarizes the current situation in blockchain assessment research. Armed with background knowledge and the problem statement, the introduction can now proceed with a research method for addressing the problem statement, by identifying the necessary objectives, the research questions which address the objectives and the methodology required to answer each research question.

1.3 Research Method

This section identifies the main objective of this study and the sub-objectives required to realize this main objective, along with the research questions needed to address the sub-objectives. This is followed by identifying the methods that are used to answer the research questions and concludes with the relevant scope of this study.

1.3.1 Research Objectives

The objective of this study is summarized with the main objective, which is supported by sub-objectives required to realize the main objective. The main objective, with the accompanying sub-objectives, were determined by intending to address the problem statement identified in Section 1.2 above. The main objective is presented below, with the ensuing sub-objectives presented in Table 1.1 thereafter.

MAIN OBJECTIVE

Create a comprehensive, generic, and quantitative blockchain assessment approach to assess the technical suitability, detail design, adoption approach, economical feasibility, and business value potential of a blockchain solution for a specific process within a certain organization.

Table 1.1: Research Sub-Objectives

Key	Sub-Objectives
SO1	Investigate blockchain technology and create a general understanding of fundamental concepts and aspects.
SO2	Identify, describe and compare the different types, use cases, and elements of a blockchain solution.
SO3	Investigate how blockchain solutions compare to more traditional solutions.
SO4	Identify and compare relevant blockchain assessment aspects in literature.
SO5	Identify the strengths in current blockchain assessment aspects and combine them into a single approach.
SO6	Identify the shortcomings in the single combined approach and address these shortcomings.
SO7	Finalize the approach to help organizations with assessing the technical suitability, detail design, adoption approach, economical feasibility, and business value potential of a blockchain solution.
SO8	Test the validity of the approach with a case study and expert opinion.

1.3.2 Research Questions

The methods required for achieving the sub-objectives can be made more obvious by identifying research questions that will need to be answered to successfully achieve each sub-objective. These research questions, along with the sub-objectives they are linked to, are presented in Table 1.2 below.

Table 1.2: Research Questions

Sub-Objective	Research Questions
SO1	1.What is blockchain technology?
	2.What are the fundamentals of blockchain technology?
SO2	1.What are the different types of blockchain and how do they differ?
	2.What is currently known about the potential of blockchain within organizations?
	3.How can blockchain enable organizations to create value within their processes?
	4.What are the different elements of blockchain, what choices do they present and how do they differ?

Continued on next page

Continued from previous page

Sub-Objective	Research Questions
SO3	1.How does blockchain compare against traditional solutions?
SO4	1.What are the aspects of blockchain assessment that need to be incorporated into the design of a generic blockchain assessment approach for organizations?
	2.What are the strengths and weaknesses of the currently available blockchain assessment approaches of these relevant aspects?
	3.Which of these aspects can be quantified and how can they be measured?
SO5	1.What are the strengths that can be taken from each blockchain assessment approach for each element to be used in a single, cohesive blockchain assessment approach?
SO6	1.What are the shortcomings present in the created blockchain assessment approach and how can they be identified?
	2.How can the shortcomings of the framework be addressed?
SO7	1.What are the required outcomes of a blockchain assessment approach that supports decision-making regarding blockchain implementation in organizations?
	2.What does a blockchain assessment approach for organizations look like?
	3.Are the outcomes insightful results that clearly indicate the suitability, feasibility and impact of a blockchain solution?
	4.Does the tool meet its requirements?
SO8	1.What are the scope and limitations of this approach based on the data it was created from?
	2.How can the feasibility and validity of the blockchain assessment approach be demonstrated and validated?
	3.Will this approach help with a complete assessment of blockchain implementation for organizations within the scope?
	4.Is the approach able to support decision-making in organizations considering blockchain implementation?

These research questions will be used to guide the study and the research method used will concentrate on identifying methods to answer each research question, as will be shown in Section 1.3.3. The research questions will be referenced throughout the

paper by the sub-objective that they are attached to, for example "1.What is blockchain technology?" will be referenced as SO1.1 in the paper.

1.3.3 Research Design

This section is aimed at constructing the overall research design by identifying the methodologies being used to answer each of the above research questions and as a result achieve the relevant research objectives and successfully complete the study. A mixed methods approach is being adopted, with both quantitative and qualitative methodologies being used throughout the study. The research methodologies being used to answer each research question is outlined in Table 1.3 below.

Table 1.3: Research Design

Research Question	Methodology
SO1.1	Content Analysis
SO1.2	Content Analysis
SO2.1	Content Analysis
SO2.2	Content Analysis, Interview
SO2.3	Content Analysis, Interview
SO2.4	Content Analysis
SO3.1	Content Analysis
SO3.2	Content Analysis, Interview
SO4.1	Content Analysis, Interview, Case Study
SO4.2	Content Analysis, Conceptual Analysis, Interview
SO4.3	Content Analysis, Secondary Analysis, Interview
SO5.1	Conceptual Analysis, Secondary Analysis
SO6.1	Case Study, Secondary Analysis, Interview, Conceptual Analysis
SO6.2	Case Study, Secondary Analysis, Conceptual Analysis
SO7.1	Content Analysis, Case Study, Interview, Conceptual Analysis
SO7.2	Content Analysis, Case Study, Interview, Conceptual Analysis
SO7.3	Conceptual Analysis, Case Study, Interview
SO7.4	Conceptual Analysis, Interview, Case Study
SO8.1	Conceptual Analysis, Content Analysis

Continued on next page

Continued from previous page

Research Question	Methodology
SO8.2	Content Analysis, Conceptual Analysis, Interview, Case Study
SO8.3	Case Study, Interview
SO8.4	Case Study, Interview

1.3.4 Research Scope

The final approach presented in this document does not intend to provide a step-by-step guide on how to assess every aspect of blockchain and guide the reader through every major decision and ultimately give a perfect solution. Instead, the aim is to create a comprehensive and generic approach that allows the reader to better understand the environment in which a blockchain solution thrives, by presenting the main aspects that affect how well a blockchain solution is received within an organization and making the reader aware of the multiple facets of a blockchain solution and where energy needs to be focused when considering implementing such a solution.

The approach does not claim to present the perfect solution to the reader or definitively proclaiming that blockchain is or is not the correct solution. Rather, it provides a recommendation based on the characteristics of a blockchain solution and presents a solution that will most likely suit the reader's needs and thus allows different considerations to be identified. The approach is a starting point to identify whether a blockchain solution has any merit within a certain context and acts as a guideline, instead of a design tool to develop the best solution or an approach that pinpoints the exact value of a blockchain solution.

1.4 Document Layout Structure

The layout of this thesis is aimed at promoting a systematic and logical flow of information to allow the reader to easily follow what is being done and where information comes from. Each chapter has been allocated a different symbol that will help guide the reader through the document and give context to the information being presented at any one time. The symbols allocated to each chapter, along with a brief description of the chapter, is presented below.

CHAPTER 1: INTRODUCTION

The first chapter deals with giving the study context and what it aims to achieve and how it will achieve this. The scope is identified and it ends with briefly describing the layout of the document.

CHAPTER 2: LITERATURE REVIEW

This chapter is aimed at building the fundamental base of knowledge required to design, construct and validate the final solution.

CHAPTER 3: SOLUTION APPROACH AND DESIGN

This chapter is aimed at detailing the approach taken to create the solution and presents the solution itself.

CHAPTER 4: SOLUTION EVALUATION AND VALIDATION

This chapter shows how the final solution is evaluated and validated using a case study and informal interviews.

CHAPTER 5: CONCLUSION

The last chapter offers a conclusion to the results of the research and highlights the most important aspects. Finally, further avenues of future research on this topic are identified.

2 LITERATURE REVIEW

This chapter will provide a relevant and comprehensive base of knowledge to be the cornerstone upon which the rest of the study will be based. It will both aid the development of the research problem and put it into perspective, while also providing the base for the initial iteration of an integrated solution. The chapter navigates fundamental concepts of the multiple facets of blockchain technology to reach an understanding of the relevant landscape, through a logical and structured flow of information.

2.1 Blockchain Technology

Blockchain technology, or blockchain, is a complex system with many interrelated elements, which have varying depths of complexity themselves. As this study has a very specific problem to solve, blockchain elements that will not affect the outcome of the solution, such as elements that are always present (block header, block body, etc.), will be briefly explained to give context but will not be explored in-depth. Whereas elements that will affect the outcome of the solution, such as blockchain permissions, will be explored in-depth to allow deductions and comparisons to be made that can be incorporated into the solution.

2.1.1 Operation

Blockchain is a nascent technology that is constantly evolving as new use cases, architectures and platforms are developed. Consequently, as mentioned in Section 1.1, blockchain has many definitions without a universally agreed upon definition and makes the formulation of such a definition difficult. While some definitions are application-specific and others attempt to be more general, there are underlying commonalities that tie many of these definitions together. Again, Sultan *et al.* (2018) have attempted to encompass all these commonalities to provide a clear, concise, and complete definition of blockchain as:

> *"A decentralized database containing sequential, cryptographically linked blocks of digitally signed asset transactions, governed by a consensus model"* – Sultan *et al.* (2018, pg. 54)

The first introduction of blockchain was through Bitcoin, the most well known application of blockchain, but blockchain extends far beyond the realm of cryptocurrencies. Blockchain was initially created, through Bitcoin, to allow the distributed storage of timestamped data that could not be tampered with without

detection and hence enabling trust within a system of untrusted parties (Lu & Xu, 2017). As blockchain has evolved, new architectures, operating modes, and platforms have been developed with unique objectives and characteristics, all stemming from the original blockchain underpinning the operation of Bitcoin.

Blockchain and distributed ledgers are often confused with one another, however there are distinguishable differences between the two. Blockchain is simply a type of distributed ledger, which may be characterised by four features, namely i) network members sharing a database of transactions ii) that is updated and governed by consensus, iii) with data that is timestamped by a cryptographic signature iv) and is ultimately maintained in a history of transactions which is auditable and tamper-proof (Swan, 2017). Blockchain differs from distributed ledgers in that cryptographic hashing is used, where each block's hash is linked to the previous block's hash, in conjunction with updating database transactions sequentially, effectively linking or "chaining" immutable transaction blocks.

This chain of linked and immutable transaction blocks are maintained by a distributed network of nodes, which will validate new transactions and add them to new blocks for the blockchain (Gatteschi *et al.*, 2018). An intuitive method of conceptualizing the blockchain mechanism is to consider Person A and Person B engaging in a transaction through the Bitcoin network, which is presented in Figure 2.1.

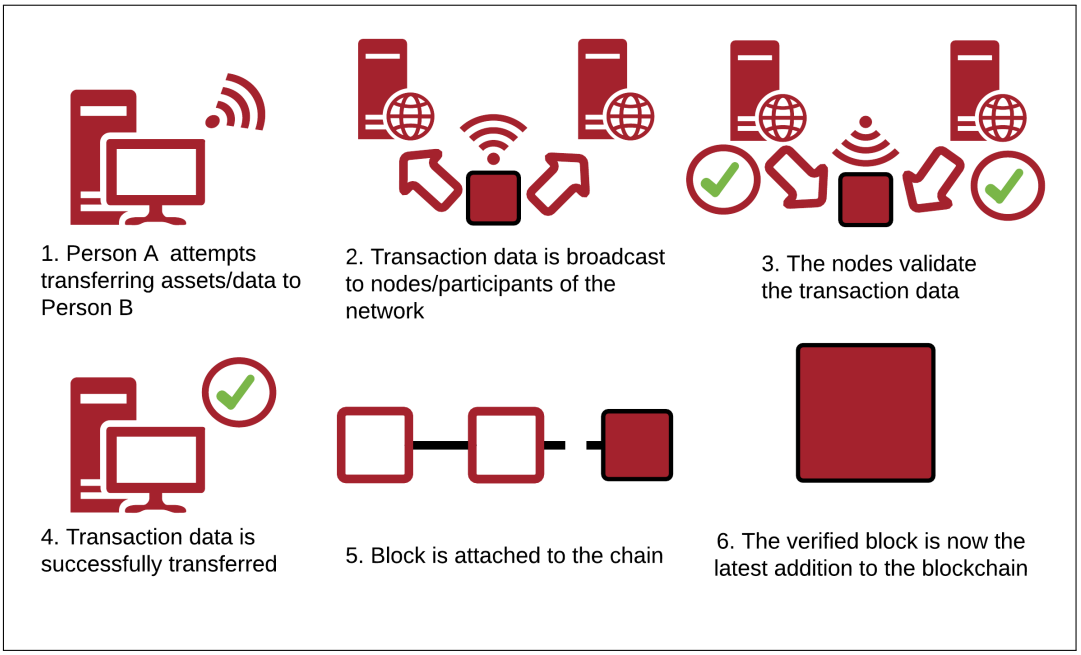


Figure 2.1: Simplistic Blockchain Overview *(adapted from Nowiński & Kozma (2017))*

The process of coming to an agreement on the state of the new block and adding it to the blockchain is facilitated by a consensus mechanism. There are a multitude of consensus mechanisms, each with their own advantages and disadvantages, where PoW is perhaps the most well known because of its affiliation with Bitcoin. The remainder of Section 2.1 will delve into the many aspects of blockchain, with a focus on the aspects that present choices that must be made.

2.1.2 Blockchain Architecture

It must be realised that for the case of blockchain being an organizational solution, it will exist within an Enterprise Architecture (EA), where the definition of architecture within the Information Technology (IT) world is defined as:

> *"Architecture is the fundamental organisation of a system embodied in its components, their relationships to each other, and to the environment, and the principle guiding its design and evolution"* - Jen *&* Lee (2000)

Then EA is the architecture at the level of the entire organization (Jonkers *et al.*, 2006). The EA provides a "blueprint" for systematically defining the current or future environment of an organization and thus helps to guide and optimise IT investments and turn the organization's strategies into technology solutions (Jonkers *et al.*, 2006). The EA can be separated into layers that represent conceptual domains (Jonkers *et al.*, 2004) which make up the basic structure of the EA model (Matthes *et al.*, 2008) by grouping related entities (Janssen, 2009).

Simon *et al.* (2013) reviewed 410 documents for which at least one EA layer was identified in order to determine the most prominent layers of an EA. They identified the prominent layers to be the business layer, application layer, information layer, and technical layer. Upon further review of relevant literature, it was found that another common layer is the process layer (Winter *&* Fischer, 2006; Braun *&* Winter, 2007; Bucher *et al.*, 2006; Janssen, 2009; Jonkers *et al.*, 2006; Kharitonov, 2017).

Different sources may use different terms for the respective EA layers, but the underlying concept of these layers remains constant. Using the above studies, the EA layers can be identified and defined as shown below.

- **Business Layer** - this layer represents the organization from a business strategy viewpoint (Bucher *et al.*, 2006; Kharitonov, 2017), decomposing the organization into arrangements of different responsibilities centred on critical value-creating

activities and ensuring coherence among these various responsibilities (Janssen, 2009; Versteeg & Bouwman, 2006). Common artifacts found in this layer are organizational goals, strategic projects, targeted market segments, value networks, relationships to customer and supplier processes, core competencies, and how these artifacts will interact (Hedman & Kalling, 2003; Weill & Vitale, 2001).

- **Process Layer** - this layer represents the organization of processes within the enterprise, including their development, creation, distribution and relationships (Bucher *et al.*, 2006; Janssen, 2009; Winter & Fischer, 2006). The enterprise is represented as the functional composition of process flows where the boundaries between processes are evident, as well as inputs and outputs (Janssen, 2009). The classic artifacts of this layer are the business processes, responsibilities, organizational units, performance indicators, and informational flows (Davenport, 1993).

- **Integration Layer** - this layer represents the organization of Information System (IS) components within the enterprise responsible for processing, storing, reusing, and distributing information among stakeholders (Bucher *et al.*, 2006; Janssen, 2009). This layer is focused on agility, cost efficiency, integration and speed and typically includes artifacts such as application clusters, integration systems, enterprise services, and data flows (Bucher *et al.*, 2006).

- **Software Layer** - this layer represents the organization of the software artifacts within the enterprise such as software services, data structures, applications, components, and objects and the relationships between these artifacts (Kharitonov, 2017; Janssen, 2009).

- **Technology Layer** - also known as the Infrastructure Layer, this layer represents the organization of computing/telecommunications hardware and networks used by various systems in the enterprise (Bucher *et al.*, 2006; Janssen, 2009). It contains the network infrastructure, operating systems and various generic facilities and services that provide functionality used by the various systems within the enterprise and thus provides the foundation from which many systems are built, such as those within the software layer (Janssen, 2009).

A blockchain solution will reside within these EA layers. Blockchain, being a complex technology, is better built from the ground up (Singhal *et al.*, 2018). This can be effectively conceptualized by considering a typical blockchain architecture and dividing

this into relevant layers based on its core fundamentals. These abstraction layers help to understand the technology stack better and makes the system easier to monitor and maintain (Singhal *et al.*, 2018).

Unfortunately, blockchain does not have global standards and thus lacks distinct layers segregating blockchain components. However, this has not stopped authors from attempting to identify blockchain layers to be able to better understand and explain the technology and create a comparison mechanism for many different blockchain variants. Comparing the literature and different layers presented throughout, the most common blockchain layers can be identified and defined as shown below.

- **Application Layer** - this is the layer that is responsible for coding the desired functionalities, typically in the form of an application that the end users will interact with (Singhal *et al.*, 2018). These applications are created to enable interaction with the blockchain system (Rehmani, 2021) and thus acts as the interface between the end user and the blockchain system.
- **Execution Layer** - this is the layer that executes all compilers needed for the application layer and any smart contracts, scripts, or algorithms that form the basis of blockchain programmable features (Rehmani, 2021; Yu *et al.*, 2018). It is responsible for the execution of any instructions received from the application layer and takes place on all nodes in the blockchain network, where these instructions may be straightforward or many complex instructions compiled into a smart contract (Singhal *et al.*, 2018).
- **Consensus Layer** - this is the layer that ensures all nodes in a Peer-to-Peer (P2P) network agree on a consistent and valid state of the ledger, typically through a consensus mechanism (Singhal *et al.*, 2018; Zhai *et al.*, 2019). This layer defines which consensus protocols need to be executed and the relevant rules for achieving consensus through this protocol to ensure security and safety (Rehmani, 2021; Singhal *et al.*, 2018). This layer operates at the level of the network layer (Rehmani, 2021).
- **Network Layer** - this layer is responsible for the management and operation of the communication mechanism of the network through a P2P protocol, allowing nodes to discover, communicate, and sync with one another regarding the current network state (Bains, 2022; Singhal *et al.*, 2018; Rehmani, 2021). Transaction/block

propagation and verification between network nodes are defined in this layer (Singhal *et al.*, 2018)(Yu *et al.*, 2018)

- **Data Layer** - this layer defines the data structure, data storage mechanism, and the linking of blocks of data to one another to ensure data integrity (Zhai *et al.*, 2019; Yu *et al.*, 2018). Thus, validated transactions that pass through the network layer are logically organized into blocks within this layer (Singhal *et al.*, 2018). This layer includes hashing, cryptographic algorithms, chain structure, time stamp, scalability techniques, data ordering, and so on.
- **Hardware Layer** - this layer represents the underlying hardware that is required for the successful operation of the blockchain nodes (Rehmani, 2021). The performance of the blockchain network is closely related with this layer and depends on the hardware architecture employed (Rehmani, 2021).

It can be noted, from the EA layers and blockchain architecture layers, that there is overlap between the two and that certain blockchain architecture layers will coincide with certain EA layers. It can be seen that the "Integration Layer" of the EA correlates well with the "Application Layer" in the blockchain architecture. Similarly, the "Technology Layer" correlates well with the "Hardware Layer". Finally, the remaining layers of the blockchain architecture, which can be aptly named the "Blockchain Layer", correlate well with the "Software Layer" of the EA.

2.1.3 Block Structure

The blocks that are linked to one another to form the blockchain are all comprised of certain elements that are present in every block of the blockchain. While a block can be defined during development to contain any desirable elements, there are certain elements that are commonly utilized within blockchain solutions (Yaga *et al.*, 2019). These elements are split into the block header and block body (or block data). The block header contains the metadata of the block, which includes (Zheng *et al.*, 2018*b*; Dattani *&* Sheth, 2019; Yaga *et al.*, 2019):

- ***Block Version:*** a number indicating the current version of the block and consequently which block protocol to implement.
- ***Block Hash:*** a 256-bit hexadecimal hash value calculated based on the block data (typically determined using a Merkle tree root as shown in Figure 2.2).

- ***Parent Block Hash:*** a hash pointer indicating the previous block's hash value, effectively linking the blocks to one another.
- ***Timestamp:*** the time the block was created.

These are the type of block header elements that will be found in most blockchain blocks. More elements can be added (or removed) depending on what the developer sees fit for the architecture of the blockchain. For example, blockchains running using PoW usually include a nonce, an adjustable value allowing nodes to solve a mathematical puzzle involved with PoW (Yaga *et al.*, 2019).

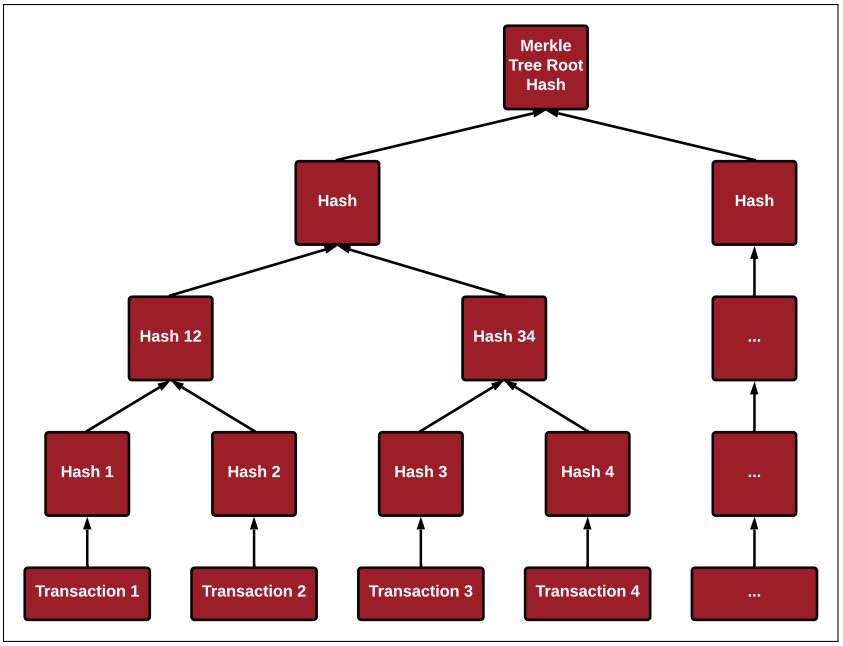


Figure 2.2: Merkle Tree Root Hash

The block body is simply a list of asset transactions (digital ledger) that are stored on the blockchain (Zheng *et al.*, 2018*b*). Typically, blocks are not continuously created, but rather created after a set time period of a few minutes so that transactions during this period are grouped together into one block, thus preventing multiple blocks being created at the same time (Singhal *et al.*, 2018). There is a pool of current transactions and during block creation, the publishing node will select and verify transactions from the pool until the block's memory limit has been reached and the remaining transactions in the pool will be added to the proceeding block (Zhang *et al.*, 2020; Singhal *et al.*, 2018). More elements can be added, such as a transaction counter, but this is up to the blockchain developer's discretion. Furthermore, the content of the transaction data depends on the purpose of the blockchain and differs from blockchain to blockchain.

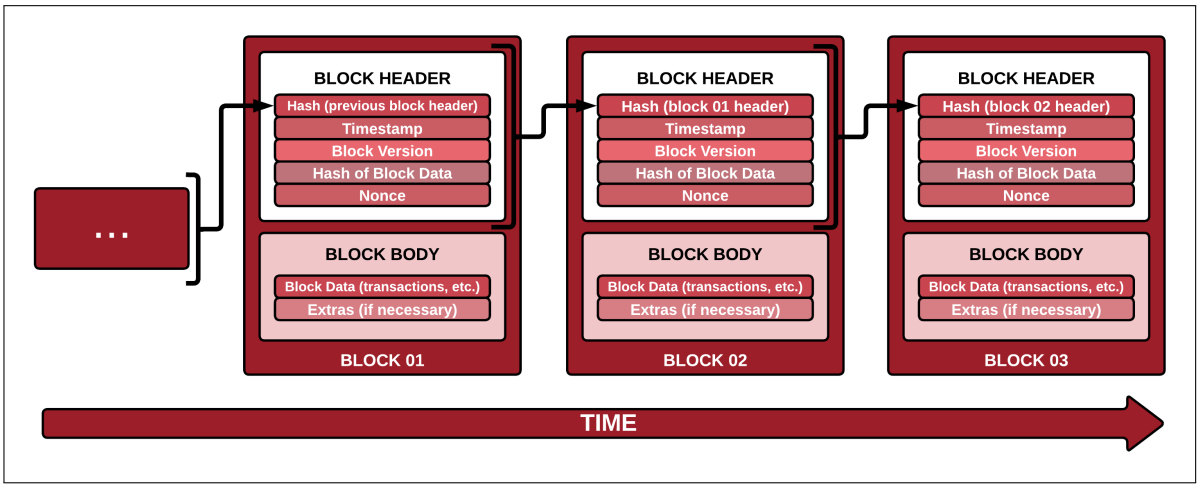


Figure 2.3: Blockchain Block Components

The elements of the block structure are not design decisions, but rather consequences of design decisions. It is simply an indication of the necessary data required for operation of the blockchain and does not require direct attention during the design of a blockchain solution.

2.1.4 Cryptography

Cryptography is one of the mechanisms that characterize blockchain and provide much of its utility, from the identity of participants to the privacy and authenticity of transactions, which both contribute to the integrity of the digital ledger that is blockchain. This section will briefly explore the main uses of cryptography within blockchain.

2.1.4.1 Cryptographic Hash Functions

Hashing is the process by which a hash function takes an input of any size (text, images, file, etc.) and creates a unique, fixed-length value output, known as a *digest* (Zhai *et al.*, 2019; Yaga *et al.*, 2019). Any alteration in the original input, no matter the size, will output a completely different digest. Hashing functions have three important properties that ensure data integrity (Yaga *et al.*, 2019):

1. **Preimage Resistance** – it is not possible to extract data using the hash value, rather the hashing function generates a hash value based off of known data.

2. **Collision Resistance** – there are no two inputs that would produce the same hash value digest.

3. **Second Preimage Resistance** – given an input, it is impossible to find another input that would produce the same hash value as the given input.

The usefulness of legitimate hash functions that uphold the above properties is unmistakable, clearly highlighting the data integrity it will be able to accommodate. The most common hash function algorithms used in blockchains are SHA-256 and Scrypt, because of their ease to validate and difficulty to forge (Fernández Caramés & Fraga Lamas, 2020). The specifics of the workings of hash functions is not important to the potential blockchain owner, it is rather a consideration for the blockchain developer to ensure that it meets all the requirements of hash functions, while performing as efficiently as possible.

Blockchains primarily use hash functions for ensuring the integrity of the blocks and the transaction data within the blocks (Zhai *et al.*, 2019). As mentioned in Section 1.1, one of the fundamental ways in which hash functions are used to ensure data integrity is by creating a digest of all information in the block, which is then referenced in the next block's header and will consequently affect that block's digest as shown in Figure 2.4. When using block digests to connect them to one another, the digests are known as hash pointers (Zhai *et al.*, 2019). The integrity of blocks is therefore ensured because changing a block will require all subsequent digests to be recalculated, otherwise there will be a mismatch of digest values.

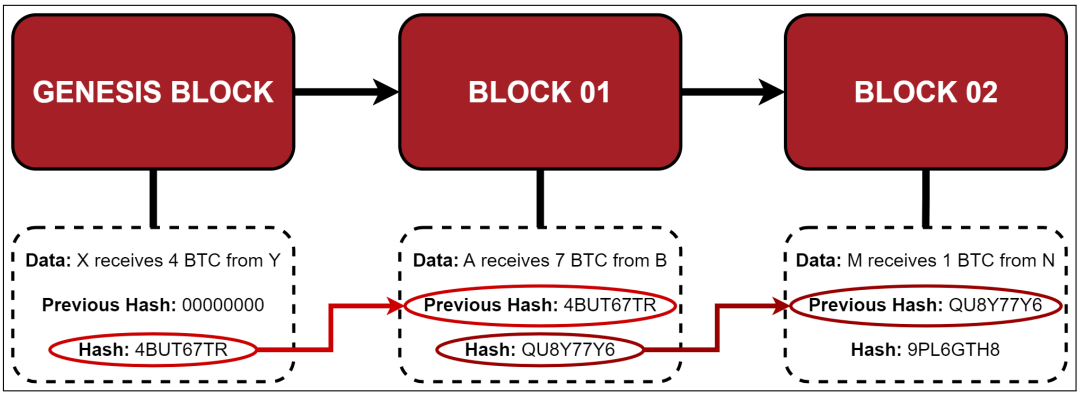


Figure 2.4: Blockchain Hash Pointers

2.1.4.2 Public-Key Cryptography

Along with ensuring the integrity of blocks and transactions, hashing is used to create unique identifiers and addresses through public-key cryptography, also known as asymmetric-key cryptography (Yaga *et al.*, 2019). Each blockchain network user has

a pair of mathematically related keys: a public and private key. The public key, as the name suggests, is made public to all users of the network and is analogous to an email address, while the private key should not be shared with other users and is analogous to a password (Yaga *et al.*, 2019).

These keys are used to encrypt and decrypt data on the blockchain to enable trust between mistrusting parties by facilitating transaction authenticity and integrity, while allowing transactions to remain public (Yaga *et al.*, 2019). This is accomplished in blockchains through the use of digital signatures (Yaga *et al.*, 2019). A private key can be used to encrypt data and anyone with the corresponding public key can decrypt it, proving that the signer of the transaction has access to the private key linked with the freely available public key. Alternatively, and perhaps more intuitively, data can be encrypted with a user's public key so that only the private key linked with it can decrypt the data. The use of asymmetric-key cryptography can thus be summarized:

- Transactions are digitally signed using private keys.
- Addresses are derived using public keys.
- Digital signatures generated with private keys are verified using the corresponding public key.
- Asymmetric-key cryptography enables users to verify that the user transferring assets or value to another user has possession over the private key needed to digitally sign the transaction.

The verification process using digital signatures has two phases: signing phase and verification phase (Zhai *et al.*, 2019). Figure 2.5 shows the typical verification process in a blockchain solution. Person A begins the transaction by generating a hash value based on the transaction's data. This hash value is then encrypted using Person A's private key and this encrypted hash is then sent to Person B along with the original transaction data. Person B is then able to decrypt the hash value by using Person A's freely available public key and compares this with the hash value generated from the original data by the same hash function that Person A used. If the hash values match, it can be verified that the transaction data is indeed from Person A and that it is valid.

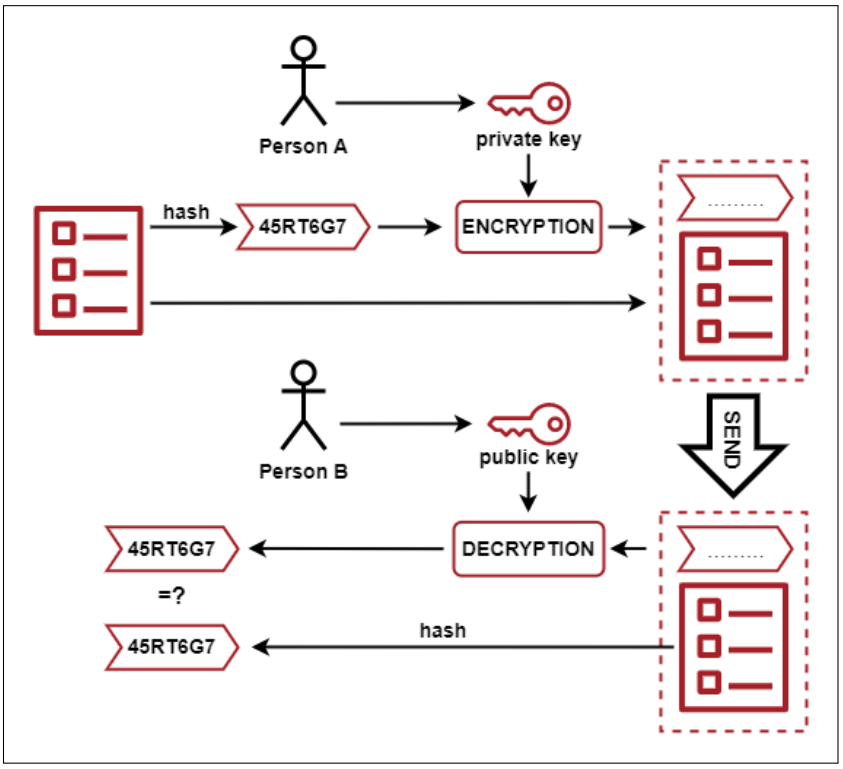


Figure 2.5: Digital Signatures in Blockchain *(adapted from Zheng* et al. *(2018*b*))*

Private keys need to be securely managed and stored, because it is not feasible to regenerate one if it is lost and thus all digital assets linked with that private key are lost too (Yaga *et al.*, 2019). Furthermore, if a private key is stolen, the thief will have access to all of the digital assets controlled by that stolen private key. It is evident that securely storing private keys is essential and many users make use of key escrow services to do so (Yaga *et al.*, 2019).

2.1.5 Consensus Mechanisms

An advantage to using blockchain is its decentralized nature, removing the need for a centralized authority to facilitate transactions between parties because every user has access to the entire blockchain and can therefore verify its integrity. However, removing this centralized authority creates a trustless environment and reaching consensus on the state of the blockchain in such an environment poses a challenge. Furthermore, the distributed nature of blockchain further complicates this challenge.

Consensus mechanisms are used to ensure that the ledgers on the distributed nodes of the blockchain agree with one another (Zheng *et al.*, 2018*b*). It's the protocol which determines how transactions will be validated (Allessie, 2017). The simplified purpose

of consensus mechanisms is to perform secure and frequent updates of the distributed ledger, resulting in a shared state throughout the blockchain network (Lashkari *&* Musilek, 2021). Through the use of such a mechanism, nodes are not required to trust other nodes but to rather trust the protocol used to ensure consistency between nodes. Consensus mechanisms are one of the key contributions of blockchain, enabling high trust in a decentralized and distributed environment (Nguyen *&* Kim, 2018).

If a node publishes a block and all other nodes agree with it, the block is then added to each node's respective blockchain (Singhal *et al.*, 2018). While majority of the nodes (or all in some cases) will have to confirm the validity of the new block, there is only one node that will publish the block and will thus be the first to ensure the validity of the proposed block. The consensus mechanism determines which node in the blockchain network will be the one to publish a given block and consequently confirm that the transaction information is consistent with the information on the blockchain (Zhai *et al.*, 2019). Seibold *&* Samman (2016) presented a formal definition:

> *"A consensus mechanism is the way in which the majority (or, in some mechanisms, all) of the network members agree on the value of a piece of data or a proposed transaction, which then updates the ledger"* – Seibold *&* Samman (2016, pg. 3)

The consensus mechanisms that blockchain uses can be categorized into two primary groups: proof-based consensus and voting-based consensus (Nguyen *&* Kim, 2018). Proof-based consensus mechanisms allow the node that performs sufficient proof that it is more qualified than the other nodes of the blockchain network to append a new block to the blockchain. Proof-based consensus mechanisms include PoW, Proof-of-Stake (PoS), Delegated-Proof-of-Stake (DPoS), and Proof-of-Elapsed-Time (PoET). Voting-based consensus mechanisms requires that the nodes in the blockchain network exchange their block appendage or transaction verification results to reach a consensus on the appropriate state of the blockchain. Voting-based consensus mechanisms include Practical Byzantine Fault Tolerance (pBFT). Combining the work of Nguyen *&* Kim (2018) and Yang *et al.* (2021), Table 2.1 presents a high-level comparison of these typical consensus mechanism groups.

Table 2.1: Consensus Mechanism Group Comparison

Consensus Mechanism Group	Vote-Based	Proof-Based
Agreement Making	Majority decision	Performing enough proof
Freely Joining Nodes	No	Mostly
Number of Executing Nodes	Limited	Mostly unlimited
Decentralization	Low	Mostly high
Trust	More trust required	Less trust required
Node Identity Management	Yes	No
Security Threats	Less serious	More serious
Incentive Reward	Mostly no	Yes
Processing Speed	Higher	Lower
Deployment Cost Benefits	Lower	Higher
Fault Tolerance	Higher	Lower

The remainder of this section will investigate the different consensus mechanisms that are most commonly associated with blockchain. While there are many options available for consensus mechanisms, only the most common will be explored due to the practical experience and subsequent deductions that can be made on them. The basic workings, advantages and disadvantages of each will be explored, completing the section with a comparison of the relevant mechanisms.

2.1.5.1 Proof-of-Work (PoW)

Perhaps the most well-known consensus mechanism because of its association with Bitcoin, PoW requires the block publisher to be the first node to solve a computationally intensive puzzle (Yaga *et al.*, 2019). This solves the confusion of having multiple nodes simultaneously verifying transactions and broadcasting them on the network, resulting in duplicated transactions and rendering the ledger useless. The computationally intensive puzzle requires nodes to earn the right to append a new block by solving the puzzle and showing "proof" they have done work (Nguyen & Kim, 2018).

The process is simple and logical. The node will update each element of the block,

including verifying and adding transactions from the pool of transactions to the block body until the block's memory limit is reached. The puzzle being solved is a threshold value below which the hash value for the current block must fall under (Nguyen *&* Kim, 2018; Queralta *&* Westerlund, 2021; Zheng *et al.*, 2018*b*; Yaga *et al.*, 2019). As mentioned in Section 2.1.3, a nonce value is used in the header of the block when using PoW and it is this value that is adjusted, hence giving new hash outputs until a nonce is found that gives a hash output lower than the threshold (Nguyen *&* Kim, 2018; Queralta *&* Westerlund, 2021; Zheng *et al.*, 2018*b*).

Once a node finds a suitable nonce, the block containing that nonce is broadcast to all other nodes, at which time they will stop solving the puzzle (Nguyen *&* Kim, 2018; Zheng *et al.*, 2018*b*; Yaga *et al.*, 2019). Instead they will verify the results of the broadcast block, including the added transactions and all elements of the block. Verification is rapid and uncomplicated because only a single hash needs to be computed to check the nonce against the puzzle requirements (Yaga *et al.*, 2019; Nakamoto, 2008). If all elements are correct and correlate with the previous block, the nodes append the broadcast block onto their blockchain as the latest block. Once a block has been accepted and appended to the blockchain, the miner that broadcast the block will typically receive a reward, often monetary in the form of tokens (Nakamoto, 2008; Yaga *et al.*, 2019; Singhal *et al.*, 2018).

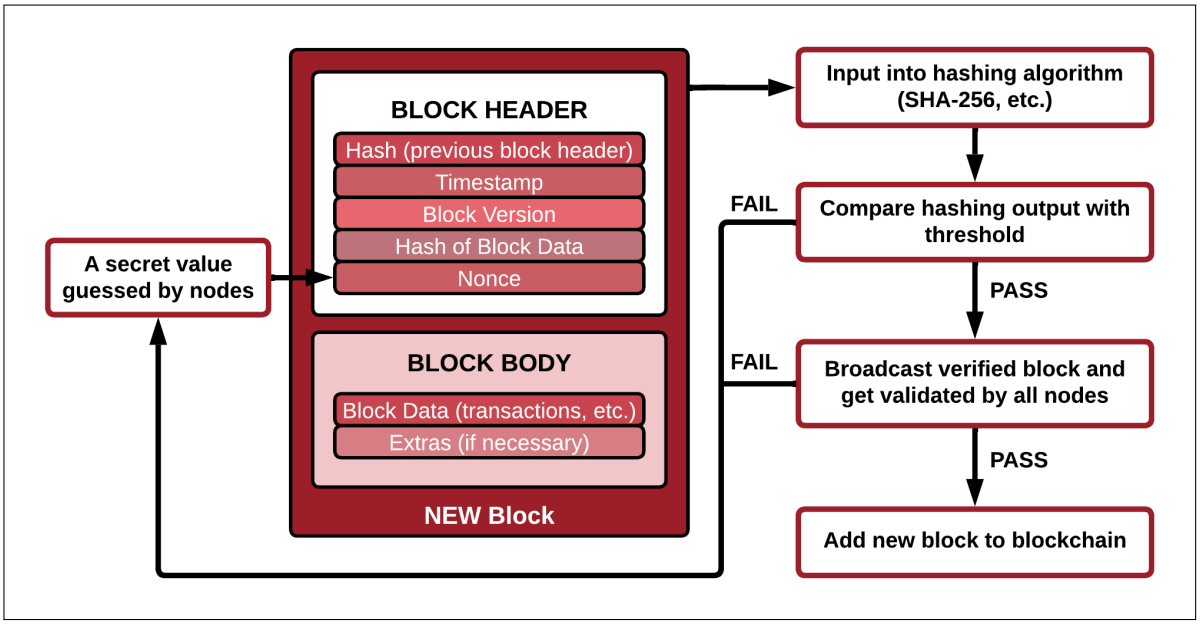


Figure 2.6: Proof of Work Process

The difficulty can be adjusted by altering the threshold requirement and thus the average speed for appending a block can be controlled (Yaga *et al.*, 2019). Bitcoin adjusts the difficulty every 2016 blocks and strive to keep block verification and appendage around 10 minutes long (Nguyen *&* Kim, 2018; Zheng *et al.*, 2018*b*; Yaga *et al.*, 2019). Also, finding a suited nonce value is called mining and the nodes appending blocks are called miners (Nguyen *&* Kim, 2018; Zheng *et al.*, 2018*b*). Unfortunately there is a case where more than one miner will find a suitable nonce and broadcast the block at the same time and the nodes only receive the first incoming block and ignore any others (Nguyen *&* Kim, 2018; Queralta *&* Westerlund, 2021; Zheng *et al.*, 2018*b*). This leads to a phenomenon known as forking, where two chains will split off of the main chain. This will be explored further in Section 2.1.12.

As the first widely adopted consensus mechanism, PoW has been the subject of many research efforts highlighting its drawbacks (Nguyen *&* Kim, 2018). Improved hardware increases appendage speed constantly and thus the difficulty of the hashing problem increases and requires miners to invest increased amounts of money into hardware, driving up costs (Nguyen *&* Kim, 2018). Another problem is the so-called 51% attack, where the attacker will attempt to make a fork, with fraudulent transactions, longer than the original, legit fork (Queralta *&* Westerlund, 2021). However, this attack requires the attacker to own over 50% of the computing power of the network, which is a highly unlikely event with larger networks such as Bitcoin (Romiti *et al.*, 2019). Pool mining, where nodes join to form a collective that splits work and rewards, could threaten to create a scenario in which 51% attacks are a more realizable threat to the network (Romiti *et al.*, 2019; Yaga *et al.*, 2019). Pool mining also greatly undermines the decentralization aspect of blockchain (Zhang *et al.*, 2020).

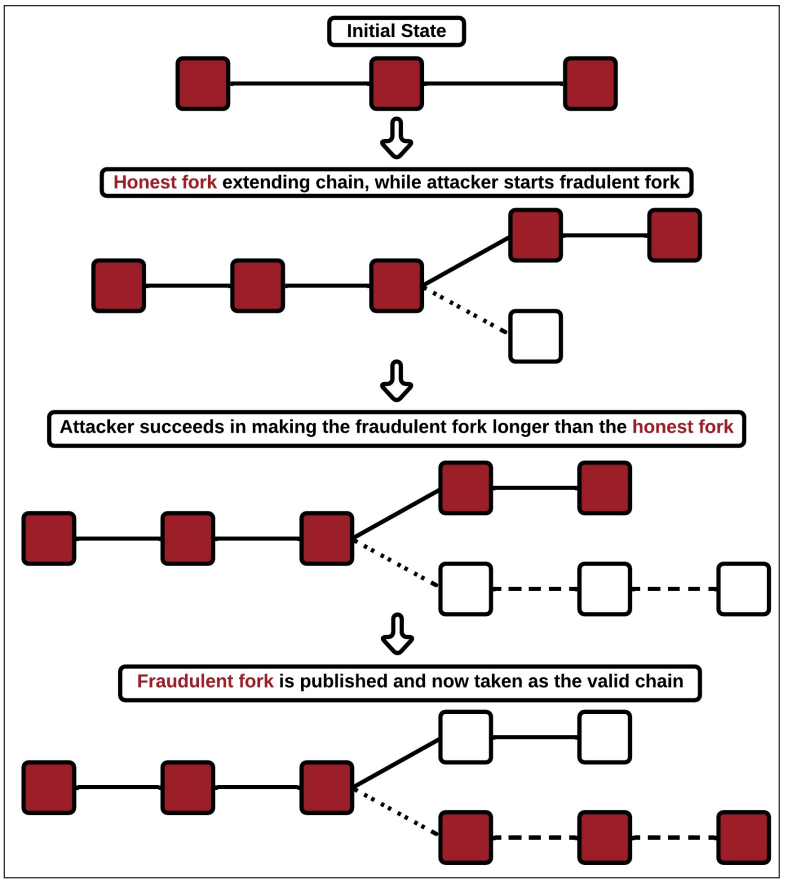


Figure 2.7: 51% Attack Mechanism

Furthermore, PoW's delayed block appendage deems it unsuitable for real-time payment systems (Eyal *et al.*, 2016; Zhang *et al.*, 2020). Also, the amount of computational power required to gain control over a network using PoW makes it extremely robust and secure, but creates an inefficient consensus mechanism as an unwanted outcome because all nodes attempt to solve the puzzle at once, while only one solution is chosen, consequently using unnecessary computational power and electric energy for solving these PoW puzzles (Queralta *&* Westerlund, 2021; Zhang *et al.*, 2020; Singhal *et al.*, 2018).

This high computational dependency leads to scalability issues because as the network grows, transactions will take longer and require more power and so the network will eventually reach a limit (Nguyen *et al.*, 2019). Lastly is a phenomenon known as selfish mining whereby selfish miners will force honest miners to waste their resources on shorter forks by mining blocks and not publishing them and creating a longer private chain than the current public chain, and only broadcasting their private chain when certain requirements are reached and thus receiving more revenue because there was

no competition on the private chain that has now become the main chain (Eyal & Sirer, 2014). With selfish mining, adversaries require as little as 25% of the network's computational power (Eyal & Sirer, 2014).

2.1.5.2 Proof-of-Stake (PoS)

PoS was proposed to deal with the inherent inequality of PoW, where miners with better equipment or pool miners can more easily find nonces in comparison to others with slower equipment (Nguyen & Kim, 2018). Additionally, it addresses the computational complexity of PoW and in turn the resource inefficiency, low scalability, and transaction validation latency (Queralta & Westerlund, 2021). The core idea of the mechanism is that nodes' stakes in the network will dictate who mines the next block (Nguyen & Kim, 2018). Buterin *et al.* (2020) described it as nodes earning the right to append blocks only after staking part of the digital tokens they own on the blockchain network. The belief being that those with more stake will want to uphold the integrity of the blockchain and refrain from performing fraudulent transactions (Zheng *et al.*, 2018*b*; Yaga *et al.*, 2019). Furthermore, a 51% attack would require a single node to own over 50% of all the digital tokens of the network, which is, in theory, a lot more challenging than gaining half the computing power (Nguyen & Kim, 2018).

The premise is that the more stake a node has in the network, the higher probability it has to mine a new block and receive a reward for doing so (Nguyen & Kim, 2018). The reward is not usually a newly issued coin because less resources are required for PoS mining, instead the miner will receive a reward through the transaction fees paid by users (Yaga *et al.*, 2019; Singhal *et al.*, 2018). Presume node N has x staked coins of a total of y staked coins on the network, then the chance for node N being the chosen node to mine the next block is x/y.

The validating nodes will put something, usually the digital tokens it owns, at stake instead of computational power to get selected to do the mining of the new block (Queralta & Westerlund, 2021; Singhal *et al.*, 2018). The digital tokens at stake are usually "locked in" by a special transaction, either by holding it in a specific wallet or sending it to a special address (Yaga *et al.*, 2019). Once this selection has been made, the node will update elements of the block header, as well as verify and add transactions from the pool of transactions to the block body until the block's memory limit is reached and then broadcast the new block to the rest of the nodes (Nguyen & Kim, 2018). If the node attempts any fraudulent actions, they are at risk of losing the total value of their stake (Queralta & Westerlund, 2021).

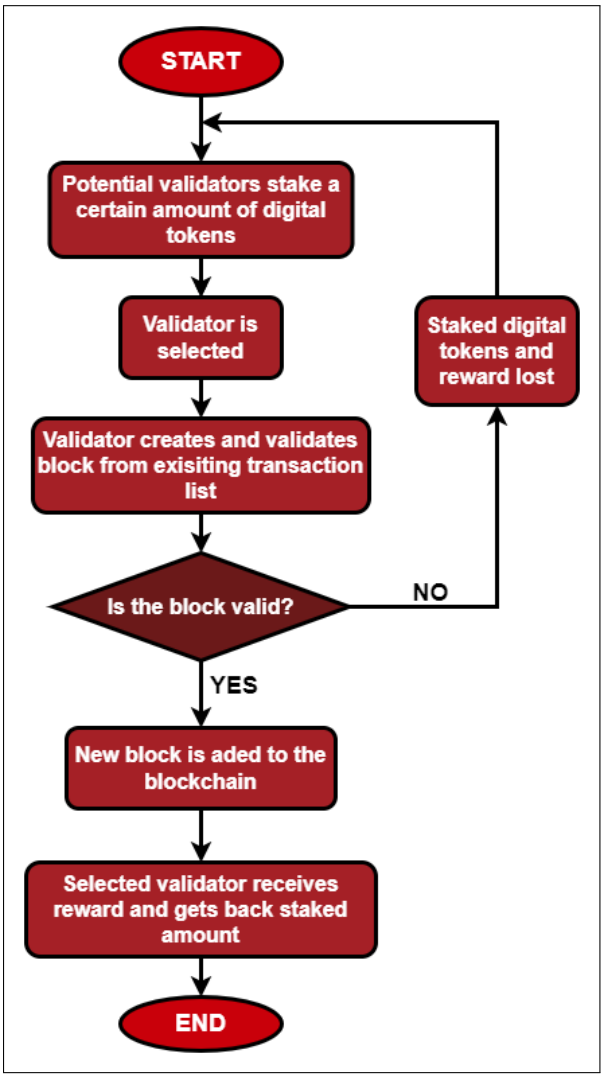


Figure 2.8: Proof of Stake Process

From the onset it is obvious that this consensus mechanism is unfair because the wealthier nodes will get better chances of appending blocks and receiving rewards and hence the rich get richer. As a result, there are a few common variations of PoS that use a combination of stake size and alternative elements to determine who will append the next block (Zheng *et al.*, 2018*b*). Regardless of the chosen variation, appendage rights are still proportional to stake size.

Naturally, the pure form of PoS is determining appendage rights through the random selection of staked users based on their stake size. The pure form of PoS is not widely used and most blockchain solutions using PoS use a PoS variant (Zhang *et al.*, 2020). One variation of PoS uses multi-round voting, where a number of staked users are chosen by the blockchain network to append new blocks and all staked users will verify and cast

a vote on a proposed block, which may extend over a few rounds of voting (Yaga *et al.*, 2019). This variation allows all staked users to participate in block appendage regardless of their stake size.

Another popular system is the coin age system, wherein the staked tokens only count towards the owner's stake after a certain predetermined period (Yaga *et al.*, 2019). If the owner was selected for block appendage, the staked tokens have their age reset and will hence not count towards the owner's stake until after the predetermined period. This cooldown enables wealthier nodes to participate but not dominate. Older tokens and large groups of tokens have a higher probability of getting chosen for block appendage. Another variation using coin age is making the stake of a user equal to their stake multiplied by the tokens age, which is the time since its last transaction (Zhang *et al.*, 2020; Wang *et al.*, 2019). This makes it easier for less wealthy users to get a chance to publish a block by allowing their stake to sit for longer periods.

Lastly is the delegate system in which users vote for randomly selected nodes to be one of the limited publishing nodes, as well as voting to remove nodes from this set of publishing nodes (Yaga *et al.*, 2019). This variant is popular and is known as Delegated-Proof-of-Stake (DPoS). Voting power is proportional to stake in this instance. The voting is a continuous process, and to remain a publishing node and receive rewards the nodes have to act benevolently. The nodes voted in will verify transactions and publish blocks to the blockchain (Nguyen *&* Kim, 2018). The validating nodes are rewarded after successfully participating in block appendage and the validating nodes' voters also receive rewards proportional to their stake size (Veinović *et al.*, 2021). This voting extends to the voting of delegates that will govern the blockchain and voting on proposed changes to the blockchain (Yaga *et al.*, 2019). With less validating nodes, transactions can be processed faster and the network can be scaled bigger, but it centralizes power more than PoS (Zheng *et al.*, 2018*b*).

PoS addresses the resource inefficiency, transaction latency, and low scalability of PoW, but due to its faster speeds, it is also prone to forking within high-latency networks (Zhang *et al.*, 2020). Of course 51% attacks are still a plausible issue and pools of stakeholders could be formed to centralize power (Yaga *et al.*, 2019). For the remainder of this study, PoS and all its variants will be assumed to be a single consensus mechanism unless otherwise stated, while DPoS will be treated as a separate consensus mechanism due to its popularity.

2.1.5.3 Proof-of-Elapsed-Time (PoET)

PoET was first proposed by Intel and is executed in a specific environment called the trusted execution environment (Nguyen & Kim, 2018). All miners will request and receive a wait-time generated from a secure hardware time source from within the node's system (Yaga *et al.*, 2019). Once a miner's wait-time has elapsed, and no one else has finished waiting, it will get a chance to create and append a block, publishing the block to the rest of the nodes. The rest of the waiting nodes will cease waiting, verify the new block, add it to their blockchain and the process will then begin anew.

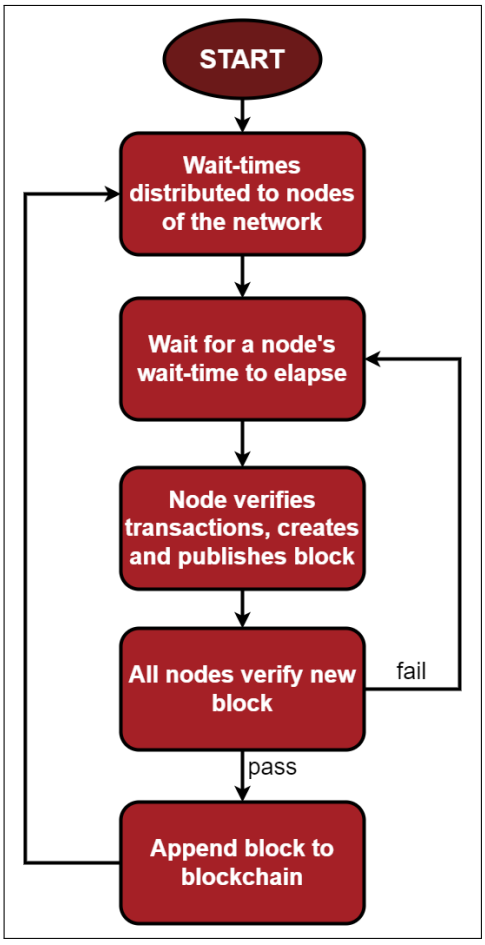


Figure 2.9: Proof of Elapsed Time Process

This mechanism requires that random times are assigned so that malicious nodes are not able to predict and take advantage of the system (Yaga *et al.*, 2019). Another requirement is ensuring that the publishing node waited their specific wait-time. These are solved by running specialised software in the trusted execution environment. This software cannot be altered by external programs when in this trusted execution

environment. The software provides a certificate to the node after it has waited its given wait-time, whereupon the node will publish this certificate with the block it is appending.

PoET reduces resource utilization, including staked tokens. PoET was developed with a permissioned blockchain in mind, but is scalable and therefore has the potential to extend to permissionless networks (Bains, 2022). Unfortunately, Sybil attacks, attacks where forged identities are used to subvert the system, are a concern in permissionless settings (Bains, 2022). Additionally, the centralization aspect of blockchain is undermined because of the use of third party software and hardware, requiring you to trust them as you would a bank.

2.1.5.4 Practical Byzantine Fault Tolerance (pBFT)

pBFT is the consensus mechanism for the well-known Hyperledger Fabric, which is Hyperledger Foundation's underlying blockchain protocol that runs on the IBM Blockchain Platform according to Hyperledger's website (http://hyperledger.org/). While pBFT can be used in a permissionless setting, it was created with the permissioned setting in mind where participants are obligated to act appropriately (Castro & Liskov, 2002). It is assumed when using this mechanism that less than a third of the nodes are faulty (f) and so the network should consist of at least $n = 3f + 1$ nodes (Castro & Liskov, 2002).

The process that pBFT adopts can be seen in Figure 2.10. pBFT has two types of nodes: validating and non-validating nodes (Castro *et al.*, 1999). The validating nodes can be further broken into a leader node (which can change every round) and validating peers (Sukhwani *et al.*, 2017). A user or client will send a transaction request to non-validating nodes that act as a proxy between users/clients and validating nodes (Androulaki *et al.*, 2018). The receiving validating node validates the transaction and broadcasts it to the rest of the validators (Sukhwani *et al.*, 2017). After a predefined number of transactions (*batch size*) or interval (*batch timeout*) has been reached, the leader sorts the pending transactions by their timestamp and puts them into a new block.

Thereafter, the three-phases of pBFT commence (Nguyen & Kim, 2018). The first phase is the pre-prepare phase, where the leader will broadcast the prospective block to the validating peers who receive, validate and store the prospective block locally. Secondly is the prepare phase, in which all validating nodes broadcast the block to all other validating nodes. After the broadcasting, the nodes will ensure they have received the same block that they broadcast from more than 2/3 of the validating nodes,

whereupon they will continue with the commit phase. The commit phase has the same procedure as the prepare phase. Once more than 2/3 of the validating nodes agree in the commit phase, all validating nodes will execute the requested transactions and append the new block to their respective blockchains, as well as broadcasting the new block to non-validating nodes for them to append to their copy of the blockchain.

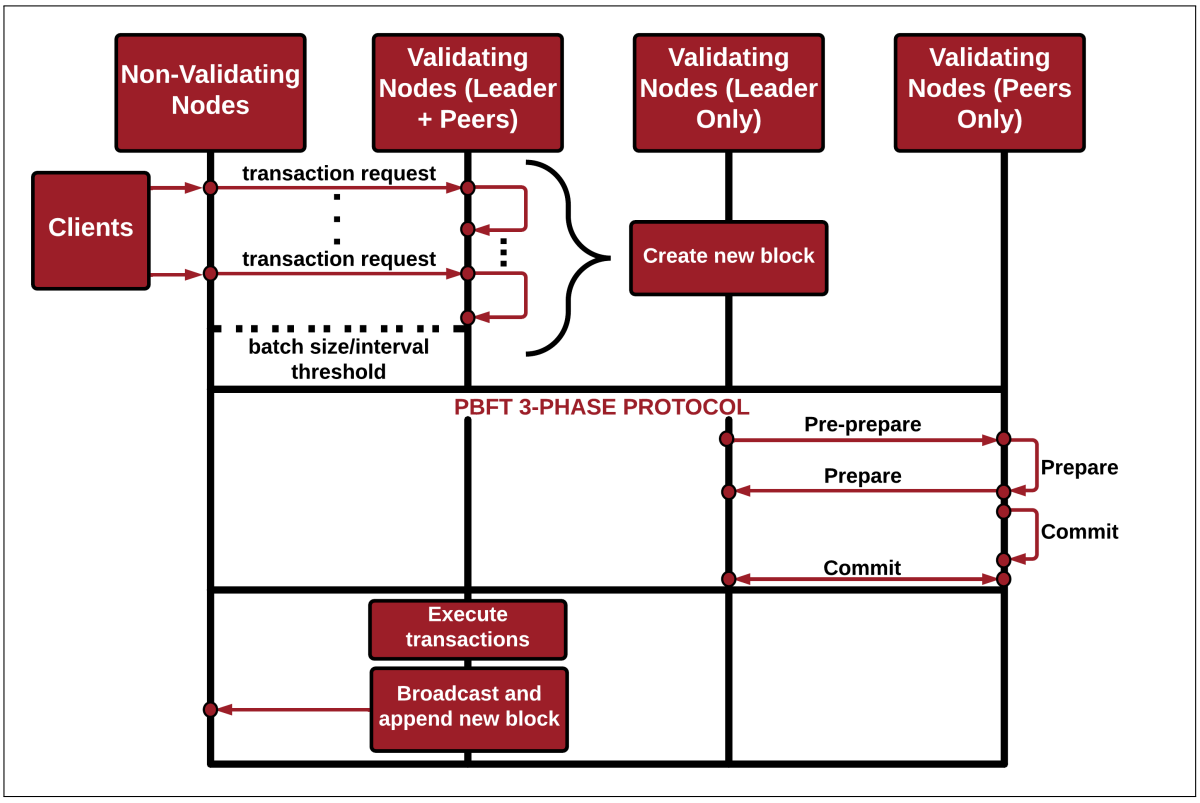


Figure 2.10: Practical Byzantine Fault Tolerance Process adapted from Sukhwani *et al.* (2017)

pBFT works well as a permissioned consensus mechanism because it is network-intensive to ensure security with the three-phase protocol and it therefore struggles to scale up to larger networks of validating nodes (Lashkari & Musilek, 2021). pBFT requires less resources than PoW, but this opens it up to Sybil attacks, which poses a problem in permissionless settings (Queralta & Westerlund, 2021). Validating nodes typically need to be known to reduce malicious intent and thus jeopardizes the anonymity of these nodes (Singhal *et al.*, 2018). While pBFT enables fast and efficient networks, increasing network size decreases this speed and efficiency (Bains, 2022). Forking is not an issue with this mechanism because only the leader node is responsible for compiling the new block (Zhang *et al.*, 2020). Thus, this mechanism works best with smaller networks

of validating nodes, while the client/non-validating nodes are able to be much larger networks. Furthermore, transaction settlement is immediate and final because of the constant communication between validating nodes (Bains, 2022).

2.1.5.6 Consensus Mechanism Comparison

Selecting a relevant consensus mechanism for a blockchain solution is crucial for its success. As will be demonstrated, there is a vast number of solution characteristics that are influenced by the choice of a consensus mechanism. There are conventional situations which will favour one consensus mechanism over another due to the inherent characteristics of that situation.

In a permissioned setting (Section 2.1.6) where access-control is typically required, the blockchain solution will typically implement a well-researched Byzantine Fault Tolerant consensus mechanism such as pBFT to reach consensus among a group of authenticated nodes (Wang *et al.*, 2019). Contrastingly, open-access or permissionless networks (Section 2.1.6) use a combination of cryptographic puzzles and an incentive mechanism to promote participation in the consensus, such as PoW (Wang *et al.*, 2019).

Vukolić (2015) addresses certain trade-offs between the typical consensus mechanisms implemented in a permissioned and permissionless setting respectively. Permissioned settings usually implement a semi-centralized consensus mechanism with higher messaging overheads to enable immediate and deterministic consensus finality, further enabling higher transaction throughput. Whereas the consensus mechanisms used in permissionless settings typically have looser control on data synchronization and thus they can only guarantee probabilistic consensus finality. However, these mechanisms typically have better support for scalability at the cost of this lower processing efficiency.

As can be deduced from the above paragraph and noted by Yaga *et al.* (2019), as the level of trust between nodes increases the need for resource intensive consensus mechanisms decrease. In these higher trust environments, the consensus mechanism extends beyond just ensuring authenticity and validity of blocks, but is also used to perform any necessary checks or validations on a transaction required by a specific setting.

Drawing upon the work of the studies cited throughout Section 2.1.5, comparisons can be made between the different consensus mechanisms, making it clearer where a particular consensus mechanism may be best suited. Table 2.2 below presents a comparison of these consensus mechanisms over a range of features and characteristics.

Table 2.2: Blockchain Consensus Mechanism Comparison

CRITERIA	Proof- of- Work	Proof- of- Stake	Delegated- Proof- of- Stake	Proof- of- Elapsed- Time	Practical Byzantine Fault Tolerance
Energy Efficiency	Low	Medium	Medium	High	High
Hardware Dependence	High	Medium	Low	High	Low
Forking	Yes	Very difficult	Very difficult	Yes	No
51% or Double Spend Attack	Yes, with 51% of network's computational power.	Yes, with 51% of network's digital tokens, but it is difficult.	Yes, with 51% of delegates and 51% of digital tokens.	No	N/A
Block Generation Speed	Slow	Medium to Fast	Fast	Fast	Fast
Pool Mining	Yes, but can be prevented.	Yes, and difficult to prevent.	Yes	No	No
Centralization	Decentralized	Partially centralized	Centralized	Partially centralized	Centralized
Scalability (# of validating nodes)	High (thousands depending on computational power)	High (thousands depending on owned stake)	High (thousands)	High (unlimited)	Low (limited)

Continued on next page

Continued from previous page

CRITERIA	Proof- of- Work	Proof- of- Stake	Delegated- Proof- of- Stake	Proof- of- Elapsed- Time	Practical Byzantine Fault Tolerance
Scalability (# of client nodes)	High (thousands)	High (thousands)	High (thousands)	High (thousands)	High (thousands)
Memory Requirement	High	High	High	High	Medium
Security	High, but 51% attack possible.	High, with reduced 51% attack chance.	High	Medium, but gets worse as network grows	Medium, with potential single point of failure.
Adversary Tolerance	<25%	<51%	<51%	Unknown	<33.3%
Typical Accessibility	Permissionless	Both, but mainly permissionless	Both	Both	Both, but mainly permissioned
Communication Model	Physical clock timestamps for block validity.	Synchronous	Synchronous	N/A	Synchronous
Settlement Finality	Probabilistic	Probabilistic	Probabilistic	Probabilistic	Deterministic

Continued on next page

Continued from previous page

CRITERIA	Proof- of- Work	Proof- of- Stake	Delegated- Proof- of- Stake	Proof- of- Elapsed- Time	Practical Byzantine Fault Tolerance
Block Publisher Selection	Based on hash rate or indirectly CPU/GPU power.	Based on stake (ownership of scarce tokens).	Based on ownership of scarce tokens and peer reputation.	Trusted random function implemented by specialised software.	Predetermined leader node or random selection of known validator nodes.
Transaction Confirmation Speed	Slow (>100s)	Medium (<100s)	Medium (<100s)	Medium (<100s)	Fast (<10s)
Validators	Entire network	Entire network	Fixed	Entire network	Predetermined known nodes
Decoupled Block Generation and Transaction Commitment	No	No	Yes	No	Yes
Node Identity	Unknown nodes	Unknown nodes	Either (typically unknown nodes)	Either	Either (typically known nodes)

Continued on next page

Continued from previous page

CRITERIA	Proof- of- Work	Proof- of- Stake	Delegated- Proof- of- Stake	Proof- of- Elapsed- Time	Practical Byzantine Fault Tolerance
Throughput Performance	Low (7 - 30 tps)	Medium (13.3 - 100 tps)	High (250 - 100 000 tps)	Medium (450 tps)	High (1000 - 2000 tps)
Latency Performance	10 minutes per block	15 - 120 seconds per block	3 - 30 seconds per block	Low latency (not measured)	Matches network latency
Contestability (barriers to entry)	High	High	High	High	Low

2.1.6 Blockchain Type and Data Access

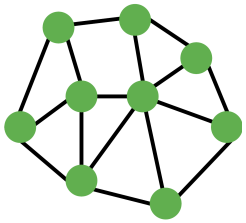
Blockchain can be broadly categorized based on two properties: data access and consensus participation. Data access can either be public or private (Garzik *et al.*, 2015). Private data access ensures that only a select number of participants may transact within the blockchain network and the digital ledger of transactions is only available for viewing to this select group. Public data access allows anyone to transact and view the digital transaction ledger on the blockchain network, but identification data is often still encrypted and thus anonymized.

Consensus participation can either be permissioned or permissionless (Garzik *et al.*, 2015). Permissioned consensus participation only allows a predefined group of nodes to participate in the validation of transactions and publishing of new blocks. Permissionless consensus participation allows anyone with the capability to participate in transaction validation and block publishing.

These parameters allow four main blockchain types to be identified, with three being useful (Allessie, 2017). These different types can be seen below, with green dots indicating nodes that can transact and participate in the consensus process, red dots indicating nodes that can transact but not participate in the consensus process, and the black ring indicating if there is a boundary within which the nodes can see the full digital transaction ledger history.

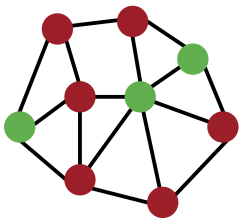
Public Permissionless Blockchains

These blockchain networks are fully accessible for transacting and viewing to anyone with a internet connection and sufficient hardware. Furthermore, anyone is able to participate in the consensus process.



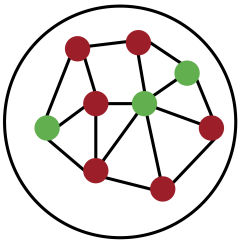
Public Permissioned Blockchains

These blockchain networks allow anyone to transact and view the digital ledger, but only a selected number of nodes are able to participate in the consensus process. This allows a slightly more controlled network.



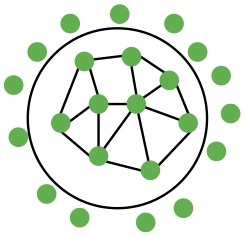
Private Permissioned Blockchains

This blockchain network restricts the ability for transacting and viewing the digital ledger, whereby only the network owners determine who may access the ledger and transact on the network. They are also responsible for determining who will participate in the consensus process.



Private Permissionless Blockchains

This blockchain network restricts who is able to view the ledger and transact, but the consensus process is open for anyone to join. Due to contradicting properties, there are no current use cases for this blockchain type (Allessie, 2017; Bauer *et al.*, 2019).



The three typical approaches to blockchain permissions are referred to as public, private and consortium blockchains (Kochhar *et al.*, 2018). Public blockchains, or public permissionless blockchains, typically offer an incentive for validation efforts. Private blockchains, or private permissioned blockchains, usually have a single organization or individual that monitors who becomes validators and who has access to what information, creating a closed ecosystem (Kochhar *et al.*, 2018).

Private blockchains reduce the risk of attacks and thus make intensive consensus mechanisms unnecessary (Casino *et al.*, 2019). The premise behind private blockchains is that all participants are known and trusted to vote honestly, making co-operation incentives mostly unnecessary (Mattila, 2016). Private blockchains tend to operate with natural disincentives to behave maliciously since everyone's identities are known and legal action can be taken for intentional malice (Yaga *et al.*, 2019). According to Swanson (2015), a private blockchain should incorporate the following aspects:

- Legally accountable validators
- Settlement finality
- Suitable for off-chain assets

A consortium blockchain has the typical benefits of a private system, such as transaction privacy and efficiency, but refrains from centralising the power to a single organization or individual and instead distributes the power between multiple organizations or

individuals who control and manage the network (Kochhar *et al.*, 2018). Thus the consortium tends to find itself in the middle ground between the two extremes of public and private blockchains.

Based on the literature of this section and the work of the cited studies, a comparison can be made between the different blockchain types over a variety of criteria. This comparison is presented in Table 2.3 below.

Table 2.3: Blockchain Type Comparison

CRITERIA	Public Permissionless	Public Permissioned	Private Permissioned	Private Permissionless
Organization Control	Very low	Low	High	Average
Actor Identities	Unknown	Unknown	Well known	Well known
External Transparency	Very high	Very high	Low	Low
Latency and Transaction Speed	Low	Medium	Medium	Low
Scalability	Low	Medium	Medium	Low
Energy Efficiency	Low	Low	High	High
Immutable	Yes	Yes	Not necessarily	Not necessarily
Data Accessibility (read)	Public	Public	Private	Private

Continued on next page

Continued from previous page

CRITERIA	Public Permissionless	Public Permissioned	Private Permissioned	Private Permissionless
Data Accessibility (write)	Public	Public	Private	Private
Consensus Participation	Permissionless	Permissioned	Permissioned	Permissionless

Data access is evidently an important factor in determining a relevant blockchain type and should thus be considered carefully when selecting an appropriate approach to deal with acess. Access is the ability a stakeholder has to use the network (Lapointe *&* Fishbane, 2019). Access is extremely important to increase data privacy and, if not handled with care, can lead to violations of privacy. There are different levels of access: write permission and read permission (Lapointe *&* Fishbane, 2019). Readers may participate in transactions and read, analyse and audit the blockchain data (Wüst *&* Gervais, 2018). Writers may participate in the consensus process and facilitate the growth of the blockchain by creating blocks and appending them to the blockchain (Wüst *&* Gervais, 2018). Establishing stakeholders' access for these particular functions depends on the chosen blockchain type and the governing body's decisions.

Private and consortium blockchains often enclose certain nodes to operate in separated, but parallel blockchains that are normally interconnected (Wüst *&* Gervais, 2018). This enables the ability to select who has access to certain transaction information based on their identity, and thus privacy is maintained because while network users can see a transaction occurred, they will not see the contents of the transaction unless they are authorised to do so (Yaga *et al.*, 2019). The use of side-chains is especially useful for this, as addressed in Section 2.1.11.2. There are many points to consider regarding blockchain access, where Figure 2.11 highlights some of the main considerations adapted from Lapointe *&* Fishbane (2019).

	WHO	WHAT	HOW
DESIGN	Who determines who may access the blockchain? Who should have access to validate transactions and append blocks to the blockchain? Who should have access to transact, view and read blockchain information?	What technology will be required to access to blockchain network? What depth of understanding will be required to use the network effectively?	How will users access the information relative to them? How are users prevented from accessing information not relative to them?
ASSESSMENT	Who will need access to what bits of information? Who outside of the network should have access to the network's information? Who would be financially incentivized to have access to the system?	What is the level of digital literacy that end users have and require? What are the different levels of technological access? What information do users currently have access to and what information is it useful for them to have access to?	How are users accessing the information relative to them? How are users prohibited from not viewing information not relative to them?
EVALUATE	Who might misuse the access they possess? Who profits from a more opaque network? Is there a conflict of interest due to financial incentives?	What user interface is required to make it accessible to all users? What technological choices make the network less usable for certain users and what can be done to address this?	How will users use their information the most effectively and are they aware of how to do this?

Figure 2.11: Access Considerations (adapted from Lapointe & Fishbane (2019))

2.1.7 Blockchain Governance

As with any successful system, there needs to be some level of governance to ensure the system is continuously performing as well as it is capable of. Governance refers to the creation and maintenance of rules and protocols that govern the blockchain network (Lapointe & Fishbane, 2019). Governance of a blockchain will directly affect the decentralization extent of the system and must thus be considered to ensure it correlates with the blockchain approach being adopted.

Bitcoin's governance contains two distinct governance structures: "governance *by* the infrastructure (achieved via the Bitcoin protocol) and governance *of* the infrastructure (managed by the community of developers and other stakeholders)" (De Filippi & Loveluck, 2016, pg. 1). De Filippi & Loveluck (2016) noted that while Bitcoin is an open-source project, the development and maintenance (governance) of it is accomplished via a small group of developers.

The governance structure of a system can benefit from employing open source development methods that allow modification in a collaborative fashion (Pilkington,

2016). Open source allows software to benefit from the power of distributed peer review and process transparency, which comes paired with increased flexibility, reliability and reduced costs (Pilkington, 2016). Open source blockchain projects force governance structures to remain consistent with the community's desires, because anyone can create a fork of the blockchain by copying the current version and evolving it separately to conform to the community's desires (Kroll *et al.*, 2013).

In most cases there will likely be a dedicated group to govern the development and maintenance of the blockchain. Unfortunately, there is a lack of research on blockchain governance and it is an aspect that is yet to be explored (Atzori, 2015). Consequently, there are not a lot of governance models that have been researched and the decision of governance falls into the hands of the blockchain owner or developer. Blockchain governance selection has the possibility of undermining the decentralization of the network and it is thus critical for a stable human governance structure to be in place to govern the network. Figure 2.12 highlights some of the main considerations of blockchain governance adapted from Lapointe & Fishbane (2019).

	WHO	WHAT	HOW
DESIGN	Who are the stakeholders and what would their roles be? Who will setup the governance of the blockchain solution? Who will decide on changes to the governance of the blockchain?	What will be the technical rules to govern the system? What will be the capabilities of the different nodes and stakeholders of the network?	How will stakeholders interact and communicate? How will the system manage the exit of key stakeholders? How will stakeholders be incentivized to participate in validation?
ASSESSMENT	Which stakeholders are needed to provide the required service? Which stakeholders are needed to provide the tools that end users will need to access the service?	What are the technical capabilities of the stakeholders? What level of trust exists between the stakeholders?	How do stakeholders currently interact and communicate? How dependent are users on the service and will a stakeholder exiting affect this?
EVALUATE	Which governing stakeholders pose a threat to users? Which stakeholders affect the power balance and how? Which stakeholders are made more powerful by the system?	What mechanisms are used to hold stakeholders accountable and is this enough?	How are disagreements among stakeholders resolved? How are incentives or processes used to ensure productive collaboration?

Figure 2.12: Blockchain Governance Considerations (adapted from Lapointe & Fishbane (2019))

2.1.8 Nodes

A node can be defined as an entity on the blockchain network that has certain data manipulation capabilities (Li & Zhang, 2017). Different nodes will have different permissions and capabilities within the network. The capabilities typically include:

1. ***Data transmission.*** This includes transferring data from one node to other participating nodes in the network.
2. ***Data analysis.*** This entails analysing data to ensure its integrity and consistency with previous data entries based on the chosen security algorithm or consensus mechanism.
3. ***Data storage.*** This includes storing the blockchain data as a distributed ledger, containing all blocks of the blockchain.
4. ***Data Cryptography.*** This includes data encryption and decryption based on the necessary task.

A common occurrence in permissioned blockchains (rarely in permissionless blockchains) is the presence of authority nodes, which are a set of overarching nodes with full control over certain aspects of the network, such as approving nodes to join the network, validating during transaction approval and block creation processes, and removing nodes from the network (Gourisetti *et al.*, 2019). These are the nodes that control access to the blockchain and dictate node allowances.

2.1.8.1 Cloud-based and Server-based Nodes

The nodes of a blockchain network can either be hosted on local servers, which the nodes themselves are responsible for maintaining, or they can be based in the cloud (Singhal *et al.*, 2018). Server-based nodes will require the nodes to run and maintain the blockchain network on local machines. Server-based nodes provide full ownership of the data, high security, and it is client-dedicated (Murthy *et al.*, 2020). It is more expensive to host nodes on a local server, but it enables tighter control over the network (Murthy *et al.*, 2020).

Cloud-based nodes are hosted by a third party and users are consequently not required to host nodes on a local server (Singhal *et al.*, 2018). Nodes running on the cloud will not have to pay for power or storage, such as a server-based node, but they require a third party for broadcasting their transactions, storing their data, and maintaining the nodes (Singhal *et al.*, 2018; Murthy *et al.*, 2020). This approach is cheaper but less secure because of the reliance on a third-party to handle the data.

2.1.8.2 Identity

Consideration needs to be given to what "identity" entails for the owner of the blockchain. The owner needs to decide whether the identity of nodes needs to be known or whether public and private keys are sufficient for the network's processes. This decision can be split between the reading and writing nodes and is typically dictated by the blockchain type chosen, where permissioned blockchains normally ensure that the readers and writers have known identities.

It is important to consider how identity information will be accessed, used and protected. There are a few considerations to this end (Scriber, 2018):

- who (or what) performed a certain transaction
- what was involved in a certain transaction
- how something moved through transactions (e.g. who owned something previously and who owns it now)
- who has certain access allowances

Keys are very loosely coupled with real-world identity, and thus cannot be trusted to indicate an identity. There is no facilitation that links keys to real-world identities and making this connection will require outside processes (Yaga *et al.*, 2019). Therefore, care must be taken if identities are required and consideration needs to be given to where an identity is required, such as transactions or activities like validation and how these identities will be facilitated. Some further considerations are highlighted in Figure 2.13 adapted from Lapointe *&* Fishbane (2019).

	LEVEL OF IDENTITY	WHICH IDENTIFIERS?
DESIGN	Are identities needed foundationally or transactionally? What components of identity are required for the chosen context?	Which identifiers will establish that the identity claimed is real and unique and that it rightfully belongs to the user claiming it? Are there minimally viable identifiers that can be used for the required context?
ASSESSMENT	What level of identity is required to provide the necessary service? What identity systems are currently in place that can be leveraged?	Which identifiers are currently used to establish identity? How are end users currently vulnerable and what identifiers are responsible for this vulnerability and which ones should not be collected? Which components of identity need to be legitimized? What technology can be used to establish identity?
EVALUATE	Is it necessary for the identity system to outlast the specific project?	Do any identifiers put users at risk and can they be aggregated and correlated in a dangerous way and are certain users more vulnerable to risk? How might the needs and risks of users change over time? Do the identifiers work in emergency situations?

Figure 2.13: Identity Considerations (adapted from Lapointe & Fishbane (2019))

2.1.9 Incentive Schemes

Nodes are incentivized to participate in the validation of blocks and the maintenance of the blockchain by contributing computing power, reputation, or money. The incentive received depends on multiple factors including the process complexity, power consumption, transaction fee, specialized hardware dependency, validation rewards, staked value and reputation (Bamakan *et al.*, 2020). Different blockchains employ different incentive schemes, where the incentives are used to encourage nodes to participate in the consensus process and consequently ensure the stability of the network (Kroll *et al.*, 2013).

The incentive is used to encourage honest nodes by attempting to ensure that if a malicious node were to assemble enough resources to manipulate the network it would be more beneficial to behave honestly than undermine the network (Nakamoto, 2008). This can be achieved by aligning individual and systemic incentives "for eliciting effort and the contribution of resources from people to conduct various record-keeping and verification activities for the public ledger" (Evans, 2014, pg. 3).

Presently, there are three main categories which incentive schemes fall into in P2P networks (He *et al.*, 2018). *Credit-based schemes* utilise virtual currency to stimulate participation in a distributed network, where the service requesting node will pay a virtual currency fee that the service providing node will receive (Yu *et al.*, 2018). The problem with such a scheme is that it will fail if the virtual currency is not secure or has no value associated with it (He *et al.*, 2018).

Barter-based schemes operate on the concept that service providing nodes will provide a service or supply resources and will then be able to obtain returns from other nodes based on what they supply to others (Yu *et al.*, 2018). These schemes may struggle to maintain different service requirements of its users because balancing the give and take of services is delicate. *Reputation-based schemes* rely on reputation scores, which is the probability that a node will behave honestly (He *et al.*, 2018).

Typically, public blockchains will use a credit-based scheme, while private blockchains do not typically rely on incentives because the nodes are usually known and behaving maliciously will damage their reputation and will have real-life repercussions (Yu *et al.*, 2018). Private blockchains can be said to use disincentives because of the repercussions of behaving maliciously and the fact that all actions can be tracked on the blockchain to a specific key, which is usually tied to a real-life identity on private blockchains. Ultimately, the decision of which incentive scheme to use is up to the owner of the blockchain.

2.1.10 Data Management

Data is a major part of blockchains and a lot of data is generated and transacted on them and it is thus crucial to manage this data effectively so that it is used optimally. Business blockchain networks will be composed of a group of organizations that share some common business interests, and it is likely that businesses will be a part of many blockchain networks because of the vast scope of some of them (Vo *et al.*, 2018). Thus, there will be data coming from multiple sources with different data schema and effectively managing this data will be crucial to the success of blockchain applications. Effective rules, processes, and techniques will be required to consolidate this data from the multiple blockchain networks that an organization may be involved in. As Casino *et al.* (2019) identified, there are many mechanisms that can be used to effectively manage data, but selecting the right approach will come down to the specific context of the blockchain's application. Figure 2.14 highlights a few key considerations to think about regarding data management, adapted from Lapointe *&* Fishbane (2019).

	WHO	WHAT	HOW
DESIGN	Who will have nominal ownership over what data? Who will have physical control over what data?	What effective control over data do different stakeholders have and who benefits? Where will data be stored (on the blockchain or linked to an external source)? What processes will be needed to access data?	How will users exert ownership over their data? How will users know if data is incorrect on the blockchain? How will users have incorrect data fixed? How will data be accessed?
ASSESSMENT	Who has nominal ownership over what data? Who has physical control over what data? Who would benefit from having more control over their own data?	Are stakeholders benefiting from the data? What processes are being used to currently access data?	Can users exert ownership over the data? How is incorrect data currently fixed? How is data being used? How is data currently accessed and can that be leveraged?
EVALUATE	What happens if data is used maliciously? Does owning data mean it can be sold? Does owning data mean that stakeholders can leave with it?	Will stakeholders benefit from the data? Can stakeholders use the data maliciously?	Are the information correction processes accesible? Is the information correction process burdensome for any users?

Figure 2.14: Data Management Considerations (adapted from Lapointe & Fishbane (2019))

2.1.11 Scalability

Many modern businesses work together with a host of other businesses, who all continuously create a massive flow of new and time-sensitive information that often needs to be shared amongst each other. Unfortunately, there are few shared databases between these businesses and thus data sharing is a tedious process, where blockchain presents a solution to this in the form of a distributed ledger. However, with the on-boarding of more businesses or clients, a testing challenge is found in how the system is able to scale and operate with a larger number of stakeholders and consequently more transactional data.

Blockchain networks are still currently struggling with scalability issues (Vujičić *et al.*, 2018). There are two major concerns with scalability: the growth of the digital ledger's size and the speed of transaction processing (Hon *et al.*, 2016). Due to the requirement that all nodes of the network keep a full copy of the digital ledger for transaction validation and that this ledger grows bigger with every block added, it may reach a point where it becomes an unmanageable size for the individual end-users.

Transaction processing speed will typically decrease as the blockchain grows due to higher volumes of transactions (Hon *et al.*, 2016). This is also dependent on the consensus mechanism employed, but typically the more validators there are, the slower the transaction processing speeds (Hon *et al.*, 2016).

Some blockchains require only one broadcast per block appendage, such as PoW-based networks, and thus the main impediment to growth is computational power requirements, which cannot be reduced without sacrificing security (Queralta *&* Westerlund, 2021). While with other blockchain networks, such as pBFT-based networks, the main impediment to scaling is communication costs, which again cannot be reduced without sacrificing security (Vukolić, 2015).

Private blockchains tend to suffer less from scalability issues because the owners have greater control over the validation process and can dictate node specifications, making them more computationally powerful with more bandwidth (Singhal *et al.*, 2018). No matter the blockchain categorization, it is important to understand different scaling techniques and develop the blockchain with the preferred technique in mind. The remainder of this section briefly looks at some of the main scaling techniques employed in blockchain solutions.

2.1.11.1 On-chain and Off-chain

Data can either be stored on the blockchain (on-chain) or stored separately to the blockchain (off-chain). Determining what data should be on-chain versus off-chain is dictated by two factors: performance and privacy (Lu *&* Xu, 2017). Performance can be increased by limiting blockchain usage and doing the heavy computational work off-chain and only storing outcomes on-chain, such as hash values (Singhal *et al.*, 2018). Off-chain computation may go against certain blockchain characteristics, but blockchain may not be needed for all computation and could be cleverly used for certain pain points (Singhal *et al.*, 2018).

There is no standard for off-chain computing and it is thus up to the owner's discretion (Singhal *et al.*, 2018). It could be that the computations are done on a side-chain (explored in Section 2.1.11.2), distributed to specific nodes, or it could be centralized by a specific node.

One may wonder how the authenticity of transactions can be guaranteed if they are computed off-chain, but as outlined in Section 2.1.4.2 you need a private key to sign a transaction and thus linking your identity to the transaction (Singhal *et al.*,

2018). Bitcoin is a stateless blockchain, everything is stored in the form of a series of transactions, while stateful blockchains contain information of the state of the block which takes up storage space because every node maintains this state constantly (Singhal *et al.*, 2018).

In stateful blockchains there is a concept known as "state channels" which are used to address the problem of high volumes of transactions between parties (Singhal *et al.*, 2018). The concept is that only the final outcome of a series of off-chain transactions are updated to the blockchain once a time threshold or transaction threshold is reached, instead of with every single transaction being executed on-chain (Wang *et al.*, 2019). Security is ensured by cryptographically signing all state channel transactions by all parties involved. The state of the blockchain is locked while the state channel transactions occur off-chain and when the transactions have been settled, the blockchain state unlocks and the final outcome is settled on the blockchain.

Clearly, deciding how to utilize off-chain and on-chain techniques with a given blockchain solution can greatly increase the effectiveness of the solution. Furthermore, there are many different ways in which these techniques can be harnessed and giving proper thought to how to employ them can greatly increase the value of a blockchain solution. A comparison between on-chain and off-chain techniques for some common blockchain processes is shown in Table 2.4 below as presented in Yang *et al.* (2021).

Table 2.4: On-chain versus Off-chain (adapted from Yang *et al.* (2021))

Process	Option	Reliability	Availability of Service	Flexibility and Opening	Deployment Cost Benefits
Data Classification	On-chain	++++	++	++	++
	Off-chain	+++	+++	+++	++++
Data Storage	On-chain	++++	++	+	++
	Off-chain	++	+++	+++	++++
Data Sharing	On-chain	++++	++	+++	++
	Off-chain	+	+++	+++	++++

+: very inappropriate, ++: inappropriate, +++: appropriate, ++++: very appropriate

2.1.11.2 Main-chain and Side-chain

Side-chains are the concept of creating a separate distributed ledger off of the main-chain and by using this side-chain ledger, performance should be able to be scaled up, as well

as increasing security and privacy (Hon *et al.*, 2016; Ali *et al.*, 2017). While side-chains are separated from the main-chain, it is possible to transfer any necessary information between the chains (Pilkington, 2016). Side-chains can also be used to create access channels, as mentioned in Section 2.1.6, by implementing the side-chain in a specific way so that only certain users are able to access the side-chain (Hon *et al.*, 2016).

Generally, the architecture of private blockchains utilising side-chains includes a central consortium blockchain consisting of all involved parties, which manages the access to the overall blockchain, while side-chains are used to facilitate transactions between specific parties, allowing only the necessary information to be shared with the necessary parties (El Ioini *&* Pahl, 2018). Since transactions require consensus, side-chains create sub-networks where only the involved parties of each sub-network will be required to validate transactions with respect to the main-chain, instead of the entire blockchain network being required to validate transaction not relevant to them (El Ioini *&* Pahl, 2018).

It must be noted that nodes without access to the side-chain will have no incentive for maintaining that chain and therefore security of side-chains needs to be considered (Hon *et al.*, 2016). However, side-chains will increase performance because less validators will need to agree on the state of the blockchain (El Ioini *&* Pahl, 2018). An advantage to side-chains is that any malicious behaviour on them will not translate to the main-chain (Hon *et al.*, 2016), as well as increasing privacy by creating private channels with greater control over access of certain blockchain data (El Ioini *&* Pahl, 2018). A comparison between employing side-chains and having a single chain for searching and matching is presented in Table 2.5 below adapted from Yang *et al.* (2021).

Table 2.5: Side-chains versus Single Chain (adapted from Yang *et al.* (2021))

Option	Processing Speed	Deployment Cost Benefits	Flexibility and Opening	Fault Tolerance
Single Chain	++	++++	++	++
Side-chain	+++	+++	+++	+++

+: very inappropriate, ++: inappropriate, +++: appropriate, ++++: very appropriate

Sharding is another scaling technique that is very similar to side-chains, where the main-chain is partitioned into parallel sub-networks (i.e. shards) and these shards are maintained by different sub-groups of nodes for which the shard is relevant (Wang *et al.*, 2019; Singhal *et al.*, 2018). This division of the blockchain enables the parallel

execution of transactions, therefore increasing transaction throughput (Singhal *et al.*, 2018). Sharding is similar to side-chains, but aimed more towards the open-access nature of permissionless blockchains, with the main objective of increasing transaction throughput (Wang *et al.*, 2019). Note that side-chains branch off the main-chain, while sharding splits the main-chain into shards.

2.1.11.3 Anchoring

The final scaling technique to be discussed is anchoring. Anchoring is the process where a large dataset that may not fit onto the blockchain is run through a hashing algorithm and the subsequent hash value is stored on the blockchain instead of the entire dataset (Vaughan *et al.*, 2016). This allows large volumes of data to be stored on the blockchain using a single transaction. This enables data integrity to be preserved while greatly reducing the amount of data stored on the blockchain. To validate the data, the same hashing algorithm will be used to generate a hash value of the data and the output is then compared with the hash stored on the blockchain to ensure the data has not been manipulated.

The reduction in data storage requirements helps the issues that blockchain solutions have with scalability. Furthermore, privacy is preserved because only hash values are stored on the transparent blockchain. Anchoring can also be used as a backup security mechanism by storing the hash values of one blockchain network on another blockchain network, therefore requiring both networks to be compromised for a successful attack (Garzik *et al.*, 2015).

However, the benefits of this approach also introduce some drawbacks. Hash values cannot be understood by humans and so anchoring undermines the transparency of blockchain networks and requires extra communication mechanisms and storage platforms if off-chain data is to be shared. Furthermore, storing the bulk of the data off-chain means that, although you might be able to detect changes to data, there is no way to prevent these changes from happening or recovering original data.

2.1.12 Forking

In permissionless blockchains, forking occurs when changes or updates are made to the blockchain network (Yaga *et al.*, 2019). There are two types of forks: soft forks and hard forks. Soft forks occur when the changes made to the blockchain network are backwards compatible, meaning that nodes which have not yet updated can continue to transact with updated nodes. Hard forks are changes to the blockchain network which are not

backwards compatible and thus any nodes that do not update will not be able to transact on the updated blockchain. Permissioned blockchains do not require the use of forks for updates because all nodes are known and thus they can require all the nodes to perform regular software updates on their systems to constantly employ the latest blockchain solution (Yaga *et al.*, 2019).

Forking is also used to describe the instance where there are temporary conflicts within the blockchain network, for example publishing a block at the same time with different data but the same block number (Yaga *et al.*, 2019). While this is a fork, it is only temporary and does not originate from updates or changes to the blockchain network. These forks are most commonly addressed by adopting the "longer chain", or the blockchain with the most work input, as the official blockchain.

2.1.13 Smart Contracts

Business activities involving multiple parties often require trust between each other and a shared understanding of the expected transactions that will take place between them. Contracts facilitate this relationship with three important characteristics, originally outlined by Szabo (1997):

1. ***Observability.*** The ability for the parties involved in the contract to observe one another's performance or prove their performance of the contract's stipulations.
2. ***Verifiability.*** The ability for the parties involved in the contract to prove that contract stipulations have been performed or breached, or the ability to find such information through other means.
3. ***Privity.*** Third parties, other than intermediaries or adjudicators, should not have a say in contract enforcement. Only parties for which knowledge and control over the performance and contents of the contract is necessary for the performance and enforcement of the contract should have this knowledge and control.

Blockchain solutions enforce contracts by the use of smart contracts on the network, which allow parties to verify that obligations have been fulfilled and provide faster and automated settlement once specific conditions have been met (Hon *et al.*, 2016). Smart contracts are simply contractual agreements that are formatted in computer code and stored and executed on the respective blockchain solution, instead of legal language conveyed on a signed contract and enforced by the judiciary system (Mattila, 2016; Hon *et al.*, 2016). These contracts can be made to be tamper-proof, automatically enforced,

and self-executing, thus reducing human intervention and making the process less risky and more cost-effective (Mattila, 2016).

These contracts need to be deterministic, in that they should be able to be represented as a logical flow chart, such as *"if A, then B, else C"* (Mattila, 2016; Morabito, 2017). This may reduce its functionality to cases without any degree of ambiguity involved, but there are many solutions proposed to address ambiguity and it is almost certain that new techniques will emerge (Mattila, 2016). As with anything man-made, smart contracts are prone to human error associated with implementing the code and thus the function and security of a smart contract depends on the capabilities of the smart contract developer (Hon *et al.*, 2016).

Furthermore, Morabito (2017) split smart contracts into two possible types: deterministic and non-deterministic. Deterministic smart contracts are executed without the need for external, off-chain data and the state of the contract can be determined solely by actors and data in the blockchain network. Non-deterministic smart contracts, on the other hand, require external, off-chain data to update contract states and thus depend on actors outside of the blockchain network to input data, known as oracles.

2.1.14 Oracles

Smart contracts, and even the general operation of a blockchain network, may require data input from sources outside of the data available on the blockchain. This is where the use of oracles (a component to transfer authentic, reliable data between a blockchain network and the physical world) becomes vital in the success of a blockchain solution. How these inputs are authenticated and verified is incredibly important in such a system because it has the potential to undermine the security of the network.

Determining how and who will verify initial entries on the blockchain, which includes establishing vetting processes and structures to prevent invalid entries, is an important task and is a process that needs to be trusted by all stakeholders involved (Lapointe & Fishbane, 2019). To create such a process effectively one needs to consider barriers to verification (dispute handling, fraudulent activities, etc.), who will do the verification, the current process for doing it and the issues it experiences, who would benefit from falsifying information, and would there be methods for checking and disputing authentication (Lapointe & Fishbane, 2019). There are four oracle types characterised by Mühlberger *et al.* (2020), as seen in Table 2.6 below.

Table 2.6: Oracle Characterisation (adapted from Mühlberger *et al.* (2020))

	Pull	Push
Inbound	The **on-chain** component **requests** off-chain data from an **off-chain** component	The **off-chain** component **sends** off-chain data to the **on-chain** component
Outbound	The **off-chain** component **retrieves** on-chain data from an **on-chain** component	The **on-chain** component **sends** on-chain data to an **off-chain** component

Oracles are conceptually challenging in the implementation of a blockchain solution because they provide a single, centralized point of failure and potentially create security and trust concerns (Mendling *et al.*, 2018). Thus, appointing an oracle is an important decision, one that all stakeholders must be satisfied with. Xu *et al.* (2016) split this choice into two by highlighting that oracles may be *external* or *internal* validation oracles. An *external* validation oracle is a third party that is trusted by all stakeholders, whether automated or manual. An *internal* validation oracle is simply the periodic injection of an external state into the blockchain, but this might cause latency issues and the source of information needs to be trusted as well.

The taxonomy of oracles can be split based on the source of data, how trust is established, design patterns, and the flow direction of information (Al-Breiki *et al.*, 2020; Beniiche, 2020). The **data source** can be separated into *software* (generated from online sources on the internet), *hardware* (scanners and sensors), and *human* (people's actions provide data). The **trust model** is determined by the number of nodes involved and is broken into *centralized* and *decentralized*, where *centralized* models rely on data from a single source, giving increased efficiency but introducing a single point of failure, while *decentralized* models have multiple sources of data, resolving the single point of failure but consequently introducing higher latency.

The **design pattern** is the set up of an oracle, which has three different possible forms: *request-response* is used when small parts of a large dataset are needed at a relevant time and requests are made for this specific information, which is then processed and the data is retrieved from off-chain infrastructure and returned on-chain. *Publish-subscribe* is used when oracles provide a broadcast service when data is expected to change over time, such as stock prices or weather. *Immediate-read* is used in situations when data is needed for an immediate decision, where the oracle will have storage that is updated and can be

looked up by on-chain applications. Lastly, is the **interaction** which can be *inbound* or *outbound*. *Inbound* simply implies that data is taken from the physical world and added to the blockchain. Outbound implies that data from the blockchain is transferred over to the physical world. A summary of these different taxonomy decisions is presented in Figure 2.15.

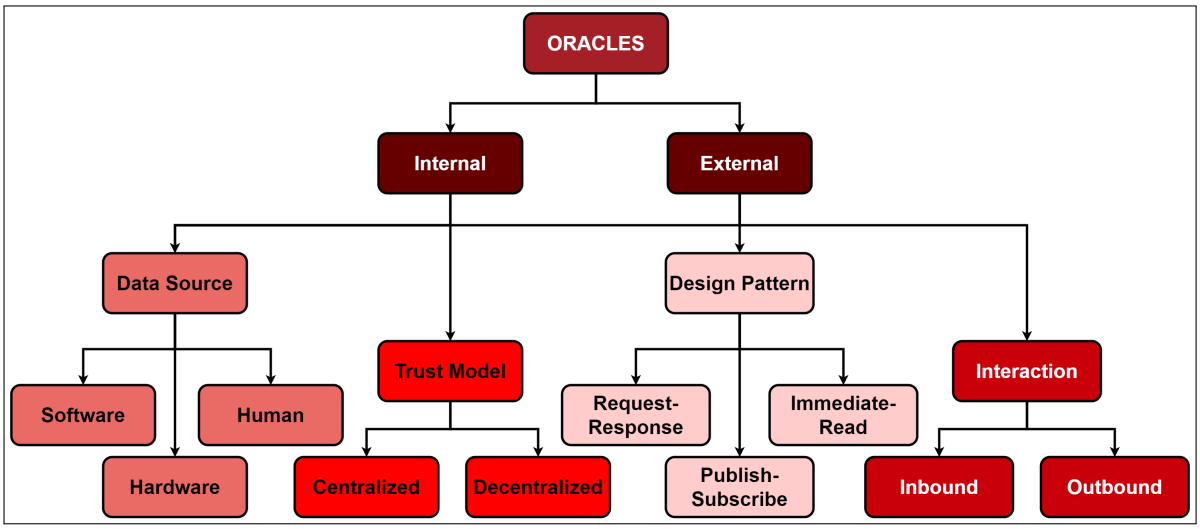


Figure 2.15: Oracle Taxonomy Choices (adapted from Al-Breiki *et al.* (2020))

2.1.15 Tokenization

Tokenization is simply the process of taking a piece of data and converting it into some random character string, which is known as a token (Morrow & Zarrebini, 2019). Thus, sensitive data is protected by converting it into non-sensitive data and the respective token is merely a reference to the original data without actually referencing what the original data is. These tokens are attached to a user's public key and managed by the same user's private key through transactions on the blockchain (Konashevych, 2020).

There are a variety of different applications for tokenization, such as the well-known cryptocurrencies, utility tokens to monitor and permit access, asset-backed tokens representing real-world or digital assets, and personal data tokens which represent sensitive personal information like healthcare information (Morrow & Zarrebini, 2019). Tokenizing tangible and intangible assets has the potential to create a more efficient and inclusive environment, where these assets can be traded with greater liquidity, transparency, and accessibility and with faster and more cost-effective transactions (Laurent *et al.*, 2018). Furthermore, data will only be traded with explicit permission through the transaction of the relevant tokens.

Oliveira *et al.* (2018) presented a basic framework for the design of a token within a blockchain network. The framework divides the classification of a token into certain attributes, which can be individually specified and will ultimately leave a token archetype specific for a particular use case. These attributes and their respective choices are shown in Figure 2.16 as presented by Oliveira *et al.* (2018). For further elaboration on the attributes and their choices consult the original study.

Purpose Parameters	**Class**	Coin / Cryptocurrency		Utility Token		Tokenised Security	
	Function	Asset-Based Token		Usage Token		Work Token	
	Role	Right	Value Exchange	Toll	Reward	Currency	Earnings
Governance Parameters	**Representation**	Digital		Physical		Legal	
	Supply	Schedule-based	Pre-mined, scheduled distribution	Pre-mined, one-off distribution		Discretionary	
	Incentive System	Enter Platform	Use Platform	Stay Long-Term		Leave Platform	
Functional Parameters	**Spendability**	Spendable		Non-Spendable			
	Tradability	Tradable		Non-Tradable			
	Burnability	Burnable		Non-Burnable			
	Expirability	Expirable		Non-Expirable			
	Fungibility	Fungible		Non-Fungible			
Technical Parameters	**Layer**	Blockchain (Native)		Protocol (Non-Native)		Application (dApp)	
	Chain	New Chain new Code	New Chain, forked Code	Forked Chain, forked Code		Issued on top of a protocol	

Figure 2.16: Token Classification (adapted from Oliveira *et al.* (2018))

Evidently, the development of a token for a blockchain solution is an involved process with many choices to be considered and careful consideration should be given to whether it is necessary for a given context. There is a lot a token can do for a blockchain solution and it can add great value, but implementing it without a specific purpose will introduce unnecessary complexities and so proper thought should be given as to whether tokens are necessary.

2.2 Blockchain Technical Synopsis

The following section will consider all the technical aspects of blockchain in conjunction with one another, ultimately giving rise to the functional characteristics, challenges and how blockchain compares to more traditional systems. Considering the technical aspects of blockchain introduced in Section 2.1, it is obvious that each layer of blockchain's architecture can be developed in multiple different ways, some of which will have mutually exclusive properties. Therefore, it is impossible to give a single definitive

answer to what the characteristics and challenges of blockchain are in its entirety. Consequently, this section will highlight the characteristics and challenges without consideration for the specific development of the blockchain solution and it is up to the reader to realize which characteristics are linked with which development decisions if it is not explicitly stated.

2.2.1 Functional Characteristics

With the technical aspects of blockchain covered in Section 2.1, one begins to see the functional characteristics it may possess. These functional characteristics are explored below, with brief explanations of how they are materialized through blockchain's chosen architecture.

1. ***Decentralized.*** Utilizing consensus mechanisms to allow direct communication between nodes enables streamlined transactions by removing unnecessary intermediaries and certain process steps, where removing these extra steps reduces the chance of errors, increases speed and decreases costs.

2. ***Immutability.*** Transactions recorded on the blockchain cannot be manipulated without the knowledge of the network and thus altering a transaction requires a new transaction to be recorded that reverses the effects of the unwanted transaction, therefore making it impossible to omit transactions.

3. ***Transparency.*** Shared identical copies of the entire transaction history, which is available to all relevant nodes at any time (distributed digital ledger), provides transparency to anyone with the relevant access.

4. ***Security.*** Cryptography (hashing and digital signatures) and consensus mechanisms coupled with the shared and distributed nature of blockchain solutions provide an extra measure of security, making it difficult to manipulate or forge data.

5. ***Verifiability.*** Blocks being immutable, sequentially linked and digitally signed enables transactions to be tracked and verified directly, and thus new transactions can be verified immediately by comparing the proposed data with the transaction history. Furthermore, this level of verifiability and traceability enables swift and straightforward auditability.

6. ***Controllability.*** The ability to track individual assets without the need for an intermediary allows the effective and exclusive control over one's digital assets and data. This control can also be securely transferred between nodes of the network.

7. ***Consistency.*** All new transactions are checked against existing blockchain transactions and are validated by the relevant nodes. This ensures that transactions remain consistent with each other, making it difficult to append blocks with inconsistent transactions.

8. ***Autonomy.*** Smart contracts enable a logical set of rules to govern specific transactions and are executed autonomously. When a transaction is performed, the smart contract code is read, executed and the results are processed without the need for intervention.

9. ***Trustless.*** Blockchain is designed to remove the need for a single entity to govern transactions and establishes trust based on group consensus, where all transactions are validated before being appended. This enables distrusting nodes to trust each other through the mechanisms by which they transact, rather than having to trust each other outright.

With the functional characteristics of blockchain identified, the usefulness of using a blockchain solution to deal with asset transactions, whether tangible or intangible assets, becomes evident. Presenting blockchain as a technology with the above functional characteristics demystifies the hype around it and instead frames it in a way where its value is clear.

2.2.2 Challenges

Being a relatively novel technology, blockchain is constantly being developed and improved because of the new challenges that continuously present themselves. As mentioned previously, blockchain is not the solution to all technological problems and it has its own struggles that it needs to overcome. Some of these challenges are already seeing innovative solutions, while other challenges are still barely being understood. A few of the most common and pressing challenges which blockchain solutions face are listed below.

1. ***Storage.*** Blockchain data is shared and distributed among nodes, who each store a local copy of the blockchain on their respective nodes. This data replication requires each node to have the necessary storage space, which will only increase in

size with time as more blocks are added. Furthermore, this data cannot be split because all transactions are needed for validation efforts.

2. ***Security.*** While blockchain increases security in some areas, it is still vulnerable to certain attacks (double-spending attack, 51% attack, sybil attack (Bamakan *et al.*, 2020)). Being unaware of its security downfalls can lead to serious vulnerabilities on the network.

3. ***Privacy.*** While immutability and transparency are mostly beneficial, it could potentially harm users' privacy because of the ability of every node to store and access a copy of the blockchain, enabling potential attackers to analyse transaction records to determine identities. While this can be mitigated by creating access permissions, appropriate thought needs to be given to who has access to which data and realize that possible data leaks are very likely with minor mistakes.

4. ***Oracle Selection.*** Oracles need to be robust and either require a strong reputation or a solid governance mechanism. Oracles, if not selected properly, can become the weakest link of the blockchain network, opening it up to many vulnerabilities. Questioning the original data entry onto a blockchain is known as the "Zero State" challenge (Lapointe & Fishbane, 2019).

5. ***Smart Contract/Software Vulnerability.*** As software/smart contracts are coded by humans, they are vulnerable to regular coding bugs. Furthermore, software/smart contracts are tamper-proof once they are implemented on the blockchain and thus removing coding bugs can be tedious. This could require the creation of new software/smart contracts to "cancel" the previous one, all the while making the network vulnerable to mistakes or attacks.

6. ***Private Key Reliance.*** Signing transactions requires nodes to have a public-private key pair to access and use the blockchain network, where private keys are not easily retrievable if lost. Consideration needs to be given to private key retrieval incorporation in the blockchain design, especially if blockchains enable control over valuable assets.

7. ***Limited Encryption Lifespan.*** With computers continually and rapidly evolving, encryption algorithms need to stay ahead of this evolution to ensure security. Outdated encryption algorithms pose a threat to the security of the data they are protecting, making the data vulnerable to exposure (Lapointe & Fishbane, 2019).

8. ***Scalability.*** As the blockchain ages, increasingly more blocks are added which make the blockchain larger with time. These transactions are all needed to validate future transactions and thus blockchain scales poorly the larger it gets, both with the amount of nodes and storage.

9. ***Misunderstanding.*** Being a new technology, there are very few people who have advanced skills and knowledge on blockchain (Atlam *et al.*, 2018). In many industries, there is a widespread misunderstanding and lack of skill in blockchain use.

10. ***Regulation.*** Regulators default to attempting to compare blockchain with current technologies, but with such a new and potentially disruptive technology you need to adopt a new mindset to keep up with the innovation it enables. Regulators need to come up with solutions quickly to ensure that all stakeholders' interests are considered when creating legal and compliance code. How this regulation unfolds will be largely out of blockchain owners and users' control.

11. ***Integration.*** Adopting a new technology often requires it to be integrated with legacy systems and undertaking such a task is strategically demanding.

It is evident that blockchain has its fair share of challenges to overcome. These challenges need to be considered in their entirety when assessing blockchain as a possible solution, because a single one of these challenges could be the difference between a successful and unsuccessful project.

2.2.3 Blockchain versus Databases

Blockchain is essentially a shared database that requires the permission of majority of the nodes to add data, where this data becomes immutable once it is appended to the blockchain, therefore updating data requires the creation of a new transaction rather than updating the necessary block. Traditional databases are, by their nature, centralized and mutable with a predefined group of known entities with exclusive access to view, insert and update the present data (Casino *et al.*, 2019). Traditional databases can either be hosted on a local server, where the owner is responsible for its upkeep, or on the cloud, where a third-party offers their server capabilities for a fee (Khan *et al.*, 2019). A comparison of permissionless and permissioned blockchain solutions with a traditional database is presented in Table 2.7 based on the work of Casino *et al.* (2019), Chowdhury *et al.* (2018), Khan *et al.* (2019), Singhal *et al.* (2018), and Wüst *&* Gervais (2018).

Table 2.7: Blockchain versus Database Comparison

Domain	Attribute	Permissionless Blockchain	Permissioned Blockchain	Database
Trust	Lack of Trusted Third Parties	High	High	Low
	Accountability	High	High	High
	Immutability	High	High	Medium
	Number of Writers	High	Low	High
	Multiple Non-trusting Writers	High	Medium	Low
	Peer-to-Peer Transactions	High	High	Low
	Traceability of Transactions	High	High	Low
	Verifiability of Transactions	High	High	Low
	Offline Data Validation	High	High	Low
Context	Data/Transaction Notarization	High	High	Low
	Data Transparency	High	High	Low
	Security	High	High	Low (depends on the implementation of the server, where access control can be used as a security measure)
	Privacy	High	Medium	Low
	Offline Operation	Operational with some offline nodes	Operational with some offline nodes	Low

Continued on next page

Continued from previous page

Domain	Attribute	Permissionless Blockchain	Permissioned Blockchain	Database
Performance	Latency and Transaction Speed	Low	Medium	High
	Maintenance Costs	High	High	Low
	Redundancy	High	High	Medium
	Scalability	Low	Medium	High
Consensus	Rules of Engagement	High	High	Low
	Need for Verifiers	High	High	Low
	Dynamic Interactions Between Transactions of Different Writers	High	High	Low

2.3 Blockchain Use Cases

As mentioned previously, many blockchain projects have ended in failure due to unstructured experimentation and failing to strategically evaluate the value of blockchain and how to feasibly capture that value. What organizations need is an indication of verifiable blockchain use cases that have proven value.

Researchers have taken a variety of approaches attempting to classify the taxonomy of blockchain use cases. A popular approach is classifying it into financial and non-financial use cases, such as Crosby *et al.* (2016) did. Another common approach is classifying the use cases based on the progressive versions (i.e., 1.0, 2.0 and 3.0), such as Swan (2015), Zhao *et al.* (2016), and Angelis *&* da Silva (2019). Finally, the last common approach identified is that used by Casino *et al.* (2019) and Zheng *et al.* (2018*b*), whereby major blockchain application areas are identified (i.e., financial, education, IoT, governance, data management, etc.) and blockchain use cases are classified accordingly.

After investigating the literature, a logical approach found to identifying blockchain use cases is to frame them in terms of the potential value they are able to provide in specific cases. While Angelis *&* da Silva (2019) take a hybrid approach of classifying blockchain use cases based on the value that each blockchain version provides, the approach is mostly centred on blockchain versions and the specific value they can provide, rather than classifying use cases based on blockchain solutions' value as a whole.

Mougayar (2016) identified six elements pertaining to the enablement of blockchain value represented by the mnemonic ATOMIC (Assets, Trust, Ownership, Money, Identity, and Contracts). These elements represent the core in which blockchain is fundamentally able to provide value. Through the use of blockchain, each of these ATOMIC elements are programmable and this is what enables blockchain to add value in a business context.

Carson *et al.* (2018) combined expert interviews, industry-by-industry analysis, and company interviews to identify over 90 distinct blockchain use cases. These use cases were then evaluated to better understand blockchain's strategic value and how it can be captured. Ultimately, Carson *et al.* (2018) identified six categories of blockchain use cases split into "Record Keeping" and "Transactions", which are presented in Figure 2.17 below.

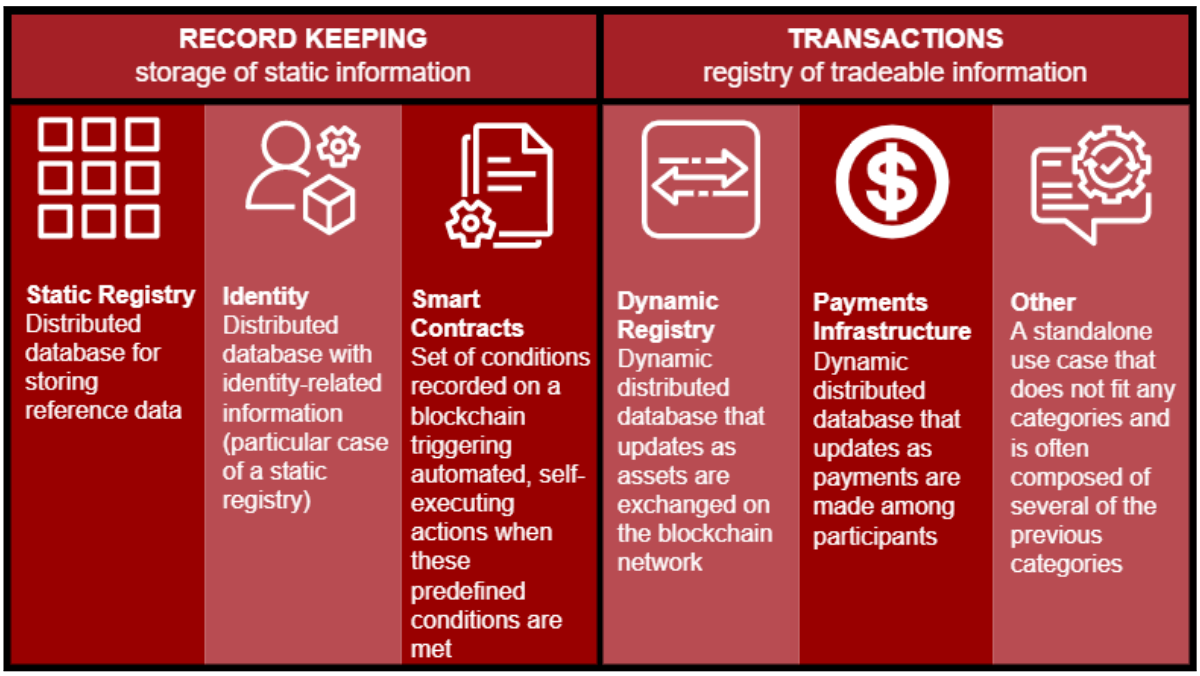


Figure 2.17: Blockchain Use Cases (adapted from Carson *et al.* (2018))

The ATOMIC concept presented by Mougayar (2016) correlates well with the use case categories identified by Carson *et al.* (2018). This model of use case identification is both logical and encompasses all use cases in a concise and relevant fashion.

2.4 Blockchain Suitability Factors

There are many factors that will influence how suitable blockchain is in a given context. This section will explore three main categories of factors (critical, organizational and process) that will influence the suitability of blockchain implementation within a particular process in a specific organization. The factors are identified through the theoretical background of the previous sections, with a focus on the functionality and challenges of blockchain, rather than attempting to cover all possible scenarios where blockchain could potentially add value, because the number of factors would be infinite in the latter case.

2.4.1 Critical Factors

The critical factors are those which are extremely important to the successful implementation of a blockchain solution within an organization's process, whereby not satisfying these factors greatly weakens the case for blockchain implementation. Assessing these factors at an early stage will allow a quick and concise indication as to whether the intended blockchain use case is sensible. If the use case requirements do

not align with the specified critical factors, there may be a more sensible solution than blockchain.

Many frameworks have been created (typically in the format of a flow chart) indicating the critical factors of blockchain adoption. In alignment with the previous literature of this study, these factors can be attributed to certain blockchain functional characteristics or lack thereof. Table 2.9 below presents the identification, combination and distillation of these critical factors and which studies have identified them according to the key in Table 2.8.

Table 2.8: Critical Factor Sources

Key	Source	Title	Description
1	Allessie (2017)	Blockchain Technology for Governmental Processes. The Design of a Blockchain Assessment Tool: A Design Science Approach	The study designs a blockchain assessment tool to help EU Institutions and Bodies make decisions on blockchain implementation to improve information exchange or registration processes.
2	Chowdhury *et al.* (2018)	Blockchain versus Database: A Critical Analysis	The study critically analyses traditional databases and blockchain by studying case studies of blockchain use, ultimately developing a decision tree to help select the most appropriate choice.
3	Gourisetti *et al.* (2019)	Evaluation and Demonstration of Blockchain Applicability Framework	This article demonstrates the use of the blockchain applicability framework to determine blockchain suitability, blockchain type, and the consensus mechanism.

Continued on next page

Continued from previous page

Key	Source	Title	Description
4	Koens & Poll (2018)	What Blockchain Alternative Do You Need?	This article analyses 30 existing decision frameworks and proposes an improved framework based on the flaws of the existing frameworks, primarily by introducing alternative solutions.
5	Lapointe & Fishbane (2019)	The Blockchain Ethical Design Framework	This white paper addresses why intentional design matters, while identifying key questions that should be asked and ultimately presents the Blockchain Ethical Design Framework to aid with integrating values and ethics into the design and implementation process.
6	Lo *et al.* (2017)	Evaluating Suitability of Applying Blockchain	This study proposes an evaluation framework to assess the suitabiltiy of blockchain for a particular use case and uses case studies to evaluate the framework.
7	Peck (2017)	Do You Need a Blockchain?	This article presents a framework to determine the applicability of the different blockchain types for a specific use case based on the characteristics of blockchain.
8	Scriber (2018)	A Framework for Determining Blockchain Applicability	This article analysed 23 blockchain implementation projects to enable the creation of their framework to evaluate blockchain's suitability for a given use case.

Continued on next page

Continued from previous page

Key	Source	Title	Description
9	Wüst & Gervais (2018)	Do you need a Blockchain?	This study critically analyses whether blockchain is suitable for a particular use case, ultimately presenting a framework for determining the most appropriate solution.
10	Yaga *et al.* (2019)	Blockchain Technology Overview	This document has a high-level look at the technical aspects of blockchain to help the readers understand how the technology works.

Table 2.9: Critical Factors

Critical Factors	Sources
Data Store/Exchange	3, 4, 5, 9, 10
Multiple Distributed Parties	1, 2, 3, 4, 5, 6, 7, 8, 9, 10
Validated Transactional Data	3, 8, 10
Lack of Trust	1, 2, 3, 5, 7, 8, 10
Lack of a Trusted Intermediary	2, 3, 4, 5, 6, 7, 9, 10
Consistent Set of Rules	4, 5
Consistent Governing Rules	5
Interrelated Transaction History	1, 4, 5, 6, 8, 10
Mapping Party Transactions	8
Transparency Importance	3, 5, 6, 8
Immutability and Auditability Importance	2, 3, 5, 6, 10
Censorship or Attack Reduction	3, 5, 7

The presence of these factors in a specific scenario indicates a strong use case for blockchain implementation. Of course, other factors need to be considered because these factors only address the high-level blockchain characteristics without consideration for more detailed specifics of the use case. However, these high-level critical factors allow a broad view of the applicability of blockchain for a given scenario to be determined.

2.4.2 Organizational Factors

Organizational factors are identified as those factors which would affect how well suited the organization is for the successful implementation of a blockchain solution.

Kamal (2006) identified five domains which organizational factors can be mapped to regarding adopting an IT innovation within an organization and further presented critical success factors within each domain for successful adoption. Allessie (2017) used these domains and critical success factors, along with expert interviews, to identify the organizational factors within these five domains pertaining to the successful implementation of blockchain specifically.

The organizational factors are identified using these domains and the associated organizational factors identified by Allessie (2017), coupled with insights from the previous sections of literature and the works of other authors within the IT or blockchain sphere. While these domains helped to identify the organizational factors, it was found that the factors could be better separated into the domains identified below, where the domains used by Kamal (2006) were not as descriptive in their naming. It should also be noted that some of the factors identified by certain authors are only relevant to specific use cases, hence these factors are either removed or altered to make them more general. The identification, combination and distillation of the organizational factors, their sources and their relevant domains are presented in Table 2.11 according to the key shown in Table 2.10 below.

Table 2.10: Organizational Factor Sources

Key	Source	Title	Description
1	Allessie (2017)	Blockchain Technology for Governmental Processes. The Design of a Blockchain Assessment Tool: A Design Science Approach	The study designs a blockchain assessment tool to help EU Institutions and Bodies make decisions on blockchain implementation to improve information exchange or registration processes.

Continued on next page

Continued from previous page

Key	Source	Title	Description
2	Barua *et al.* (2004)	Assessing Internet Enabled Business Value: An Exploratory Investigation	This study proposes an exploratory model to assess the electronic business value involved with IT applications, processes, operational and financial performance metrics, and business partner readiness.
3	Erol *et al.* (2020)	Assessing the feasibility of blockchain technology in industries: evidence from Turkey	This study quantitatively assesses how feasible blockchain is in a variety of industries using a comprehensive list of indicators.
4	Scriber (2018)	A Framework for Determining Blockchain Applicability	This article analysed 23 blockchain implementation projects to enable the creation of their framework to evaluate blockchain's suitability for a given use case.
5	Yaga *et al.* (2019)	Blockchain Technology Overview	This document has a high-level look at the technical aspects of blockchain to help the readers understand how the technology works.

Table 2.11: Organizational Factors

Domain	Organizational Factors	Sources
Critical	Administrative Authority Support	1, 2
	Financial Support	1, 2
	Legal/Regulatory Framework	1, 3, 5
Core Expertise	Managerial Capabilities	1
	Blockchain Complexity	1
	Risk Aversity	1
	IT Capabilities	1, 3, 4
	Blockchain Enthusiast	1
	Technological Uncertainty	1
Operation	Interoperability	1
	Decentralized Characteristics	1
Willingness	Top-management Dedication	1
	Collaborating Parties Willingness	1, 4
	Inter-organizational Trust	1, 4
	External Influence to Adopt	1
Industry	Similar Use Cases in the Market	1, 3
	Collaborating Parties Competencies	1, 2, 3, 4
	Fraud Prevalence	3

Assessing these organizational factors will enable a particular organization to better understand how well suited their organization is for blockchain implementation. Incorporating these factors into a blockchain assessment framework will provide useful information on the applicability of blockchain for a particular organization.

2.4.3 Process Factors

Process factors are those which will determine how well a particular process or process's environment is suited for a blockchain solution. Again, Allessie (2017) identifies four domains which segment the process factors, based on the available literature and expert interviews. Process factors were identified using these four domains and the process factors identified by Allessie (2017), coupled with insights from previous literature and the work of other authors in the IT or blockchain sphere. Again, these domains helped identify the relevant process factors, but it was found that they are better separated into the domains identified below, where the domains used by Allessie (2017) could be altered to better encapsulate the process factors. Furthermore, a few of the factors identified by some of the authors are only relevant for specific use cases, and thus these factors are either removed or altered to make them more general. The identification, combination, and distillation of the process factors, their sources, and the relevant

domains are presented in Table 2.13 according to the key presented in Table 2.12.

Table 2.12: Process Factor Sources

Key	Source	Title	Description
1	Allessie (2017)	Blockchain Technology for Governmental Processes. The Design of a Blockchain Assessment Tool: A Design Science Approach	The study designs a blockchain assessment tool to help EU Institutions and Bodies make decisions on blockchain implementation to improve information exchange or registration processes.
2	Erol *et al.* (2020)	Assessing the feasibility of blockchain technology in industries: evidence from Turkey	This study quantitatively assesses how feasible blockchain is in a variety of industries using a comprehensive list of indicators.
3	Gourisetti *et al.* (2019)	Evaluation and Demonstration of Blockchain Applicability Framework	This article demonstrates the use of the blockchain applicability framework to determine blockchain suitability, blockchain type, and the consensus mechanism.
4	Scriber (2018)	A Framework for Determining Blockchain Applicability	This article analysed 23 blockchain implementation projects to enable the creation of their framework to evaluate blockchain's suitability for a given use case.

Table 2.13: Process Factors

Domain	Process Factors	Sources
Users	Predictable Actor Behaviour	1
	Limited Trust in Current Process	1, 2, 4
	Desired User Control Over Data	1
	High Importance of User Experience	1
	Transparency Required	1, 2, 3, 4
Process Facilitation	P2P Potential	1, 2
	Low Interest of Organization Being Intermediary	1
	High Availability of Bandwidth	1
	Low Throughput of Data	1
	Current Laborious Human Facilitations	1
	Workflow Simplification	4
Hardware and Software	Legacy Systems in Place	1, 2
	Interface Differentiation	1
Control	Low Institutionalized Environment	1, 2, 4
	Network Ability to Implement Technology Standards	1, 2, 4
	Importance of Control Over the Infrastructure	1
Data	Data Complexity	1
	Low Trust in Current Data Storage	1
	Traceability Required	1, 2, 4
	Data Integrity	2
	Interoperability Possibility	1, 3
	Inter-organizational Information Exchange	1, 2, 4
	Transaction Dependency	1
	Asset Digitization Potential	2
	Privacy of Sensitive Data	1, 3, 4

Assessment of the above process factors will allow the applicability of blockchain to be determined based on specific process characteristics and the process's environment. Incorporating these factors into a blockchain assessment framework will allow the applicability of blockchain for a particular process to be determined.

2.5 Blockchain Adoption

The proceeding section begins by identifying what a typical blockchain lifecycle entails. This is followed by identifying considerations that need to be thought of before undertaking blockchain implementation and the section ends by presenting four different blockchain adoption strategies based on certain industry factors.

2.5.1 Blockchain Lifecycle

As with any IT system, there are a variety of frameworks that can be used to analyse the lifecycle of a blockchain network. While these frameworks may not use the exact same terms, the general idea of each can be easily identified and extracted. As explored by Miraz *&* Ali (2020), software development life cycle models are not well suited to the nature of blockchain. Blockchain, being an IS consisting of hardware and software to provide a service, could be analysed as a Product-Service System (PSS), because it is an integrated combination of both products and services and thus the lifecycle models of a PSS will be considered.

In the work of Cavalcante *&* Gzara (2018), the authors identify typical product lifecycle models and service lifecycle models and then impose these models on identified PSS lifecycle models. This enabled the authors to identify common concepts across all models and allows gaps to be identified in the PSS lifecycle models. Ultimately, a holistic model is proposed which aims to integrate both the product and service aspects. The model is presented in Figure 2.18 below.

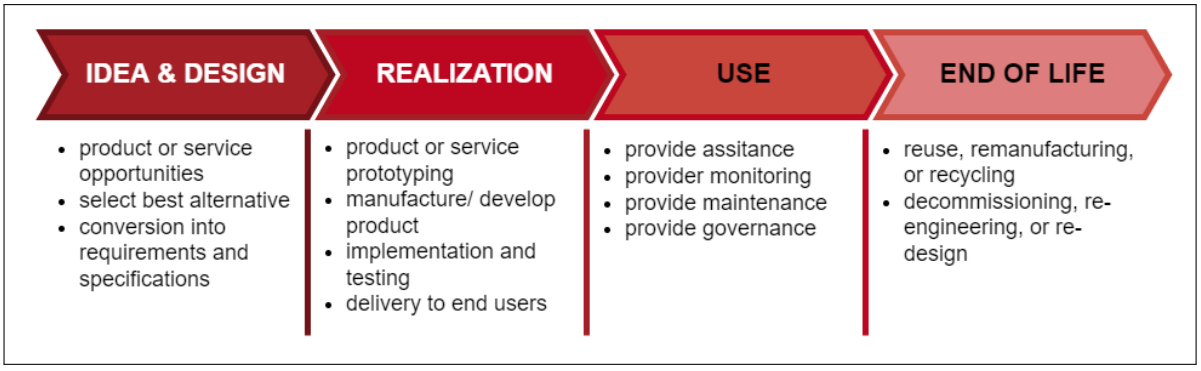


Figure 2.18: PSS Lifecycle Model (adapted from (Cavalcante *&* Gzara, 2018)

Comparing this model with the model proposed by Duarte *&* Costa (2012) for IS's and the models proposed by Beck *&* Müller-Bloch (2017), Kharitonov (2017), and (Wang *et al.*, 2016) for blockchain solutions, it can be seen that the PSS model correlates well

with these models. While terms may differ, the general concept remains and this leads to the proposed four-step blockchain lifecycle model below that is based off of the above mentioned models.

1. ***Discovery*** – this initial stage includes a feasibility study to create, recognize, elaborate, and articulate the potential blockchain opportunity, build an internal community, stimulate interest, scrutinize the solution, and strategize a way forward.
2. ***Implementation*** – this stage includes evolving the opportunity into a business proposition, requirement analysis, design and development, experimentation, training users, and finally integrating the solution using a replacement procedure (redesigning the current business process).
3. ***Operation*** – this stage includes the regular use, optimization, and maintenance of the solution.
4. ***Disposal*** – this stage begins when the benefits are lower than the costs and thus the solution becomes obsolete, whereby the system is then converted into knowledge and experience. Phasing out of the solution begins, typically in favour of a newer solution.

This lifecycle model enables different adoption considerations to be identified during each of the lifecycle phases outlined. This will allow a better understanding of the considerations in question by giving them more context in terms of the blockchain solution.

2.5.2 Adoption Considerations

Adopting any technology is a challenge and this challenge is only compounded when the technology is as new as blockchain is. Consequently, there are many aspects one will need to consider before deciding to invest time, money and effort into adopting a blockchain solution.

There are various frameworks which address these considerations from multiple different perspectives. Considering these frameworks in conjunction with the literature of Chapter 2, blockchain adoption considerations can be identified and presented in a relevant framework.

The framework adopted is an adapted version of the Guidelines Regarding Architecture Alignment (GRAAL) framework (Zarvić *&* Wieringa, 2014). Similarly to Kharitonov

(2017), the framework represents the blockchain architecture layers superimposed onto the EA layers on the y-axis as identified in Section 2.1.2, while the x-axis represents the typical blockchain lifecycle as identified in Section 2.5.1, instead of system aspects as in the GRAAL framework.

Blockchain is not an isolated technology and exceeds a specific organization's boundaries, thus requiring the context of the environment in which the organization operates and as such, an extra layer, "Enterprise Environment", is added to the y-axis to account for this as suggested by Zarvić & Wieringa (2014). Finally, a base layer, "Foundations", can be added which represents the considerations no matter the lifecycle stage or EA layer.

This framework was chosen because it allows the dynamic nature of a blockchain ecosystem to be captured by using the lifecycle view (Ruokolainen *et al.*, 2011), while also enabling the consideration of both current and future states within an EA (Kharitonov, 2017). The construction of this framework with relevant and generic considerations is addressed in Section 3.2.2.4.

The typical considerations during a blockchain's lifecycle are presented in Table 2.15, along with their respective definitions and sources. These considerations were determined by using the previous literature presented in this chapter, as well as being informed by the work of the sources identified in Table 2.14 below, which forms the basis of the key used for the sources identified in Table 2.15.

Table 2.14: Adoption Consideration Sources

Key	Source	Title	Description
1	Kharitonov (2017)	A framework for strategic intra- and inter-organizational adoption of the blockchain technology	This study provides a framework for identifying adoption considerations.

Continued on next page

Continued from previous page

Key	Source	Title	Description
2	Allessie (2017)	Blockchain Technology for Governmental Processes. The Design of a Blockchain Assessment Tool: A Design Science Approach	The study designs a blockchain assessment tool to help EU Institutions and Bodies make decisions on blockchain implementation to improve information exchange or registration processes.
3	Joannou *et al.* (2020)	Realizing the Role of Permissioned Blockchains in a Systems Engineering Lifecycle	This study describes the implementation of permissioned blockchains within a systems engineering lifecycle.
4	Morabito (2017)	Business Innovation Through Blockchain The B^3 Perspective	This book is aimed and presenting and discussing the main trends and challenges of blockchain for digital business innovations.
5	Toufaily *et al.* (2021)	A framework of blockchain technology adoption: An investigation of challenges and expected value	This study investigates the implications and challenges of blockchain adoption in both public and private sectors.
6	Wang *et al.* (2016)	A maturity model for blockchain adoption	This study presents and discusses the blockchain maturity model and its adoption process.
7	Yaga *et al.* (2019)	Blockchain Technology Overview	This document has a high-level look at the technical aspects of blockchain to help the readers understand how the technology works.

Table 2.15: Blockchain Adoption Considerations

Consideration	Definition	Sources
Industrial Initiatives	Consider existing use cases within the same (or similar) industry demonstrating success with a similar use case context.	1, Section 2.3
Legal Environment	Consider any applicable current and possible future laws and regulations the solution should be compliant with when handling data, ensuring constant communication with authoritative stakeholders to address concerns in this dynamic environment.	1, 4, 5, 7
External Stakeholders	Consider the position of all possible external stakeholders and address their concerns and ensure their satisfaction with the solution's direction.	1
SWOT	Understand the current technological situation so both the current and future strengths, weaknesses, opportunities and threats of blockchain can be identified.	1, 4, 5
Technology Acceptance	The acceptance of the shift brought about through a blockchain solution, both within an organization and the industry as a whole, is crucial for its success.	4
Ecosystem Readiness	Consider potential ecosystem stakeholders' availability of organizational resources for IT innovation adoption (financial, infrastructure, and human resources) and their capacity to use and adapt to new and innovative knowledge.	5, 7
Rationale & Feasibility	Consider the purpose blockchain is being regarded opposed to other solutions and whether there is a feasible approach to realize this purpose using a blockchain solution.	1

Continued on next page

Continued from previous page

Consideration	Definition	Sources
Strategic Planning	Disregarding start-ups, consider how blockchain will integrate with the current business model and processes and the consequent effect on reputation, knowledge, and Return on Investment (ROI). One needs to strategically plan how to effectively incorporate the blockchain solution with the current business model.	1, 5
Education	Consider the importance of educating users on the use of blockchain and the opportunities it presents, allowing users to realize opportunities within their domain and understand it to know if it is being used optimally or possibly maliciously.	1, 4
Internal Stakeholders	Consider the position of all internal stakeholders and address their concerns and ensure their satisfaction with the solution's direction.	1
Organizational Readiness	Consider the availability of particular organizational resources required for IT innovation adoption (financial, infrastructure, and human resources) and the capacity for utilizing and adapting to new and innovative knowledge.	5
Gap Analysis	Consider the gap or opportunity that the current process presents and determine how a blockchain solution will be used to address this gap and whether it is feasible.	1, 4
Assets & Data	Consider what assets will be involved in blockchain transactions and whether they can be digitized and furthermore what type of asset data will be made available and hence transacted.	1, Section 2.1.10

Continued on next page

Continued from previous page

Consideration	Definition	Sources
New Technology Success and Maturity Delay	Consider that new technologies will not achieve their potentials from the first version and see this as a method for uncovering areas of improvement, and continue to drive change by engagement and collaboration.	4
Business Process Re-engineering	Consider how the business process will be redesigned, to improve quality, output, cost, speed, service, etc. by utilizing a blockchain solution, using a business process re-engineering approach.	1, 2, 4
Solution Stack: Smart Contracts	Consider whether your use case will implement smart contracts and who will be designated with coding them and whether they will be deterministic or non-deterministic and how they will be coded during the blockchain solution's operation.	1, Section 2.1.13
Solution Stack: Performance	Consider the importance of the speed of the output of the system, where blockchain solutions tend to lag behind more traditional solutions and what hardware will be needed to achieve the required performance.	1, 5, 7
Solution Stack: Scalability	Consider the importance of sustaining performance as the blockchain system grows, where scalability concerns are more easily accounted for during development by considering what method of scaling might be used (off-chain, side-chain, and anchoring techniques) and what hardware might be required to achieve this.	1, 5, 7, Section 2.1.11

Continued on next page

Continued from previous page

Consideration	Definition	Sources
Solution Stack: Storage	Consider what data will be stored on the blockchain and the storage requirements to do so, and whether any special techniques will be used to reduce these storage requirements (off-chain or anchoring) and what hardware will be required to achieve this. Consult Sections 2.1.11.1 and 2.1.11.3 for more information.	1, Section 2.1.11.1, Section 2.1.11.3
Solution Stack: Tokenization	Consider whether the use of tokens within the blockchain solution could be beneficial to the specific use case and how this token will be used to create value within the network. Consult Section 2.1.15 for more information on the possible configuration of a token.	Section 2.1.15
Solution Stack: Fundamentals	Consider how the blockchain blocks will be structured, essentially considering what information does each block require in the header and body and how big will each block be (transaction limit or size limit).	1, Section 2.1.3
Convincing Proof of Concept (PoC)	Consider the effect of a convincing PoC that demonstrates the solid use case of a blockchain solution to potential stakeholders.	4
Adoption & Network Effects	Consider that higher blockchain adoption leads to quicker definition of standards and protocol and better leverage of network effects (higher value with greater use/adoption).	1, 5
Cooperation Agreements	Consider the agreements that must be reached on how the blockchain solution will operate within the industry, including governance, updates, responsibilities, and management. Further consider whether incentives can be used to promote cooperation between parties and what type of incentive could work.	1, 3, 4, Section 2.1.7, Section 2.1.9

Continued on next page

Continued from previous page

Consideration	Definition	Sources
Security	Permissionless blockchain applications must consider the possibility of 51% attacks, hard forks, and system bugs, while permissioned blockchain applications must consider the possibility of centralized control, fraud, data tampering and the lack of consensus mechanisms.	1, 5
Data Privacy	With blockchain solutions disclosing more data than traditional solutions, it is important to consider what data is available to which participants on the network under what circumstances and ensuring that this complies with regulations and confidentiality agreements. Further consider what mechanisms will be used to ensure this.	1, 5, Section 2.1.6
Lack of Common Standards	Consider the current lack of industry standards due to the developing nature of blockchain and how the evolution of these standards might affect your use case.	3, 4, 6
Change Management	Consider the change management approach to be adopted to prepare and support the organization with the strategization and integration of a blockchain solution with legacy systems and processes (phased implementation, parallel running, or direct changeover techniques).	1, 2, 4
Set-up Costs	Consider the costs associated with blockchain implementation (infrastructure, education, development, etc.) required for long-term success and to ultimately receive the benefits of the solution.	2, 4, 5
Oracles	Consider who will verify initial blockchain data entries and relevant vetting processes and structures to prevent invalid entries. Consider the different oracles required according to Figure 2.6 and determine the taxonomy of each using Figure 2.15 as a guideline.	Section 2.1.14

Continued on next page

Continued from previous page

Consideration	Definition	Sources
Acquisition/ Development	Consider the approach that will be taken when acquiring or developing (in-house, freelance, or outsource) a blockchain solution, where it is important to never separate business expertise and the development process. Consider what development approach will be used (from scratch, integrated with a current system, or using a blockchain development platform). If using a development platform, consider the optimal one for the specific use case.	1
Software Vulnerability	Blockchain software, being written by humans, will always be imperfect and existing bugs and poorly written code make the system vulnerable to malicious activity and will increase as the complexity and interconnectedness of the software increases.	4
Network-User Interaction	Consider how users of the network will interact with the system (web interface, mobile application, or administrative interface).	Section 2.1.8
Deployment	Consider how the blockchain system will be deployed (on-premises, third-party clouds, or a hybrid).	Section 2.1.8.1
Interoperability	Consider that blockchain interoperability is still in its infancy, making it difficult to connect separate ledgers and facilitate cross-chain communication and value transfer. Consider the tools you can use to promote interoperability (off-chain, side-chain, and anchoring techniques) and how these might be used in practice. Consult Section 2.1.11 for more information.	1, 2, 5, 6
Key Management	Consider the importance of managing your public and private keys and how to approach this, generally using methods including safekeeping and key recovery.	3, Section 2.1.4.2

Continued on next page

Continued from previous page

Consideration	Definition	Sources
Permission/ Access Levels	Consider whether the system permissions will allow enough granularity to differentiate specific roles that may be required to perform certain actions within the system. It will also help to determine which users need access to what specific data.	3, 7, Section 2.1.6
Permission Administration	Consider how and who administers the required permissions and whether permissions can be revoked and how this will be done.	7, Section 2.1.6
Infrastructure	Consider what infrastructure might be needed to implement blockchain for the required process based on the network requirements, storage requirements, process power requirements, consensus mechanism requirements, and the node requirements (cloud-based or server-based).	1, 6, Section 2.1.2
Environment Monitoring	Consider the complexities of operating within an interconnected environment and the constant need to ensure the system is operating as intended and all stakeholders are satisfied. Consider what mechanisms will be used to ensure this.	1
Altering Historical Records	Consider whether altering historical records should be possible in the system and how it will be implemented to ensure data integrity (permissions, agreement, etc.).	1, Section 2.1.10
Evolution & Maintenance	Consider how the system will be maintained and evolved and what methods will be implemented to do so and who will be responsible for it.	1, 6, Section 2.1.12
Governance	Consider the roles of system stakeholders and what the rules and protocols would be that govern the system and who sets up this governance and how it would be changed if necessary and how it would be enforced on stakeholders.	1, 6, Section 2.1.7

Continued on next page

Continued from previous page

Consideration	Definition	Sources
Reduced Transaction Efforts	Consider the reduction in the effort of transacting with counterparties by reducing the steps involved in a process using a blockchain solution.	2, Section 2.2.1
Eliminate Opportunism	Consider the elimination of opportunism by the imposition of extreme transparency and the possible automatic execution of certain tasks using smart contracts.	2
Trusted Inter-organizational Data Exchanges	Consider the increase in trust within data exchanges due to the elimination of opportunism and the transparency with which one can analyse transactions.	2, 5, Section 2.2.1
Reliance on Network for Compliance	Consider that system stakeholders may have conflicting goals and objectives or be in direct competition and majority of participants must agree in order to validate transactions, giving increased control to counterparties in transactions.	2, 3, Section 2.1.5
Full Transaction History	Consider how the availability and transparency of the full history of digital asset transactions will affect the current process by considering who will have access to this data.	7, Section 2.2.1
Streamlined Processes	Consider how a blockchain solution might enable streamlined processes by making transactional steps transparent to users, both internally and possibly externally, and by reducing the need for intermediaries.	2, 6, Section 2.2.1
Error/ Forgery Protection	Consider that blockchain will increase the protection against errors/forgery because data will need to correlate with previous data and data tampering is near impossible without the knowledge of the network.	2, 7, Section 2.2.1

Continued on next page

Continued from previous page

Consideration	Definition	Sources
Data Integrity	Eliminating the need for centralization by sharing the ledger across the network and ensuring data correlation increases data integrity by allowing easy auditing of reliable transaction data.	2, Section 2.2.1
Decentralized Monitoring	Consider that monitoring the input and behaviour of system actors will be decentralized and thus reduce the need for hierarchical monitoring and will open the network to scrutinization from all involved parties.	2, Section 2.2.1
Scalability Issues	Consider that blockchain systems are not easy to scale and that large and efficient scaling operations will require large capital investment. However, permissioned blockchains tend to be more scalable due to the lower number of validating nodes.	3, 4, 5, 6, Section 2.1.11, Section 2.2.2
Tracing Compromised Nodes	Consider the ease with which compromised nodes can be identified because of the extreme transparency and availability of the full transaction history and the requirement to digitally sign transactions.	3
Tracing Conflicting Data	Consider the ease with which conflicting data can be identified due to the extreme transparency and availability of the full transactional history and the use of consensus to validate data.	3
Dissolution of Commitment	Consider how the commitment of stakeholders will be dissolved once the blockchain solution has run its course and the approach that will be best suited for this dissolution.	1
Evaluation	Consider how the blockchain solution will be evaluated at the end of its life to determine whether it met its expectations during its lifetime.	1

Continued on next page

Continued from previous page

Consideration	Definition	Sources
User Migration	Consider whether the system users will be migrated to a new system and what methods will be used to accomplish this user migration.	1
Data Migration	Consider whether the system data will be migrated to a new system and what methods will be used to accomplish this data migration.	1
Redeployment/ Disposal of Hardware	Consider whether the system hardware will be redeployed for use in a new system or if it will be disposed, and consider how this redeployment or disposal will be approached and completed.	1, Section 2.5.1
Investing & Financing	Consider how the financing/investing needed for the blockchain solution will be acquired and the agreements that will be necessary. Furthermore, consider how much capital will be required and how it will be allocated.	1
Knowledge Management	Consider the amount and type of knowledge that will be created during such a large and complex project and how it will be created, organized, used, and shared to ensure that the right knowledge is easily accessible to those who need it when they may need it.	1

It must be realized that these considerations may not be applicable to all scenarios, as well as there may be extra considerations that have not been included as this list is not exhaustive. These considerations will vary depending on the specific use case and will also depend on the strategic adoption approach being implemented. These are simply the most common considerations one may encounter when implementing a blockchain solution.

2.5.3 Adoption Strategy

There are a variety of ways in which an organization may undertake the adoption of a relevant IT system. Proudlock *et al.* (1999) originally identified four typical ways in which a business will approach IT adoption:

1. Purchase cutting edge technology to gain a competitive advantage
2. Expand on existing IT systems
3. Purchase off-the-shelf technology
4. Purchase the industry standard or market-leading technology

Each of these approaches have their own associated cost, risk, and potential for competitive advantage and it is up to the organization to decide which approach to utilize for IT adoption (Proudlock *et al.*, 1999). These approaches correlate well with the findings of Carson *et al.* (2018), whereby blockchain adoption strategies are recommended based on the market position of an organization, as well as the standardization and regulatory barriers present within the organization's industry. The market position refers to the organization's ability to influence key parties in the industry with regards to a possible blockchain use case. The standardization and regulatory barriers simply refers to the approval requirements or the requirement for coordination on standards. Based upon these two factors, a framework can be presented which indicates the optimal strategic approach to blockchain adoption.

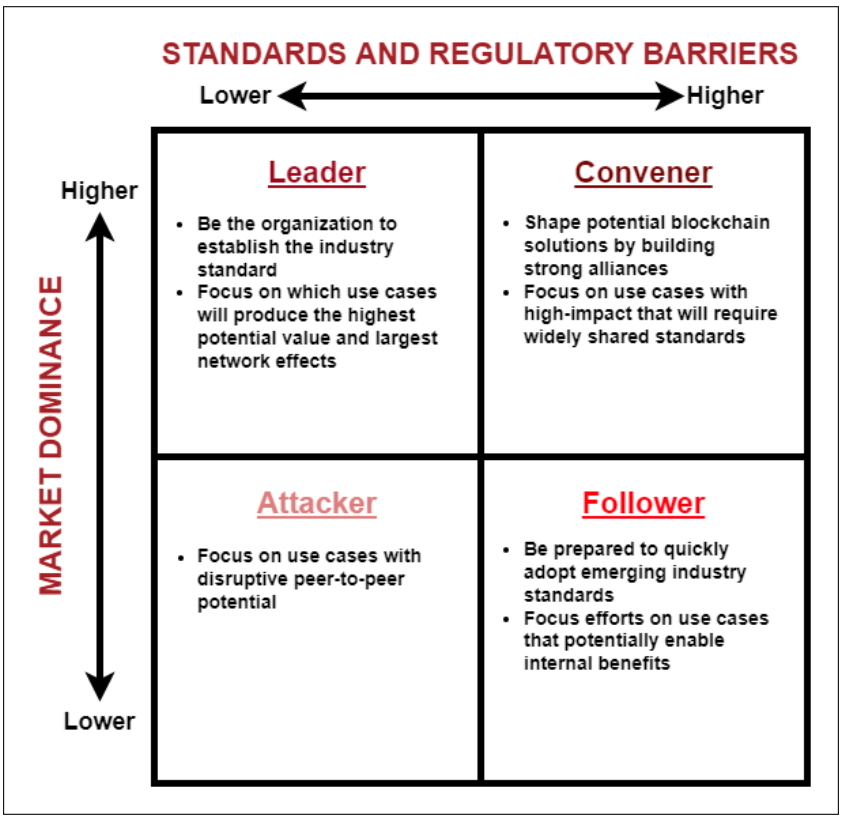


Figure 2.19: Optimal Strategic Approach for Blockchain Adoption (adapted from Carson *et al.* (2018)

As seen in Figure 2.19, there are four strategic approaches for blockchain adoption that were identified by Carson *et al.* (2018), which can be summarised as follows:

- ***Leaders*** – to maintain their strong market position, leaders need to act swiftly to set industry standards and accepted market solutions, where the greatest risk to them may be not acting at all and thus losing their competitive advantage.
- ***Conveners*** – while they may not have direct control over the direction of the industry standard because of higher regulation barriers, they must take advantage of their strong market position to shape the developing standards and capture blockchain's potential value fully.
- ***Followers*** – without the capability to influence the industry standard, such an organization must be aware of market innovations and emerging industry standards and must be prepared to move swiftly to adopt them, being aware of forming consortia and the possibility of getting left out.

- ***Attackers*** – without a strong market position to protect, these organizations need to seek out disruptive business models utilizing blockchain solutions to gain traction within that industry and could possibly partner with a larger, more dominant organization to leverage their influence.

While being high-level, these strategic adoption approaches provide valuable insight into what may be best suited for a given context. This allows the organization to identify where they should invest the most time and effort and the possible return for doing so. However, one must constantly make an effort to not be blinded by the hype surrounding blockchain and need to constantly assess it against their particular use case, as well as comparing it to more traditional solutions that may be suitable for the use case.

2.6 Blockchain Comparison Metrics

Being able to effectively assess blockchain requires one to be able to compare a blockchain solution to other potential solutions, such as an existing IS solution. Such a comparison requires standard metrics that can be used to determine how the solutions size up against one another. These metrics can be broadly classified into two categories: *Hard Metrics* and *Soft Metrics* (Lukáš, 2017). *Hard Metrics* are objective and easily measurable indicators which monitor business objectives development, business activities, or customer relations and these metrics can be divided into earnings/cost and performance. *Soft Metrics* are concerned with evaluating how the IS supports individual processes or functional areas, such as evaluating how an IS affects the rate of innovation, and is often more subjective.

Considering that this study is intended to be more quantitative, only the hard metrics will be considered. As such, the remainder of this section is split into two subsections represented by the division of *Hard Metrics*: performance and earnings/cost. According to (Lukáš, 2017), there are five critical success factors for implementing metrics to evaluate an IS:

1. ***A business and information strategy need to exist***, so that future development is clear and the role of the IS within this strategy is clear.

2. ***Understand the properties of a metric*** to ensure that the metrics identify priorities to aim at, are derived from business activities and goals, demonstrates how the IS adds value, are objectively measurable, are processed using mathematical or statistical methods, are repeatedly measurable (cost

acceptable), address short-, medium- and long-term goals, are comprehensible, and are interpretable.

3. ***Evaluating based on measurements*** implies that trends must be evaluated instead of individual measurements, establish responsibility for measurement accuracy for when individual metrics are necessary, and must be objectively measurable.

4. ***Skills and knowledge*** are required for persons measuring and evaluating the metrics.

5. ***Common sense*** is required when measuring and evaluating metrics.

Using these critical success factors, metrics can be identified from extant literature which apply to both traditional IS solutions and blockchain solutions and can ultimately be used to compare the two. This section continues by looking at the performance and cost metrics to enable this comparison.

2.6.1 Performance Metrics

There are a variety of metrics that can be used to evaluate the performance of a blockchain solution, but many of these metrics are specifically for blockchain solutions and are thus only useful for comparing blockchain solutions to one another and not other IS solutions. Consequently, performance metrics need to be identified that are able to transcend the boundary between traditional IS solutions and blockchain solutions. There are many literary works investigating the performance of blockchain solutions using relevant metrics that can also be used to measure the performance of traditional IS solutions and thus enable comparison between the two in terms of performance. Table 2.17 below captures and organizes these metrics, as well as identifying the sources according to the key identified in Table 2.16.

Table 2.16: Performance Metric Sources

Key	Source	Title	Description
1	Bergman *et al.* (2020)	Permissioned blockchains and distributed databases: A performance study	This study compares the Hyperledger Fabric (permissioned blockchain) with the Apache Cassandra (distributed database), by investigating latency with varying network sizes and workloads.
2	Dabbagh *et al.* (2021)	A survey of empirical performance evaluation of permissioned blockchain platforms: Challenges and opportunities	This study compares different permissioned blockchain platforms using a comparative framework based on existing empirical performance evaluations.
3	Dabbagh *et al.* (2020)	Performance Analysis of Blockchain Platforms: Empirical Evaluation of Hyperledger Fabric and Ethereum	This study compares two major blockchain platforms, Hyperledger Fabric and Ethereum, based on four performance metrics: average latency, success rate, resource consumption, and throughput.
4	Khan *et al.* (2022)	Empirical Performance Analysis of Hyperledger LTS for Small and Medium Enterprises	This study identifies the affect of workload and network size variance on the following performance metrics: success rate, latency, and throughput.
5	Kombe *et al.* (2018)	A review on healthcare information systems and consensus protocols in blockchain technology	This study evaluates the three most common blockchain-based healthcare systems, focusing on resource usage.

Continued on next page

Continued from previous page

Key	Source	Title	Description
6	Kuzlu *et al.* (2019)	Performance Analysis of a Hyperledger Fabric Blockchain Framework: Throughput, Latency and Scalability	This study evaluates the performance (throughput, latency, and scalability) of Hyperledger Fabric based on varying network workload.
7	Maharjan (2018)	Performance Analysis of Blockchain Platforms	This study analyses the performance of the blockchain platforms Ethereum, Hyperledger Fabric, and Parity to allow comparison between them.
8	Monrat *et al.* (2020)	Performance Evaluation of Permissioned Blockchain Platforms	This study compares the effect of varying workloads on the performance of popular blockchain platforms Ethereum, Corda, Hyperledger Fabric, and Quorum.
9	Performance & Group (2018)	Hyperledger Blockchain Performance Metrics	This paper defines key metrics that should be used to evaluate the performance of a blockchain solution.
10	Ruan *et al.* (2021)	Blockchains vs. Distributed Databases: Dichotomy and Fusion	This study compares blockchain systems to distributed databases across four aspects: replication, storage, sharding, and concurrency, and how these design choices are driven and affect performance.
11	Smetanin *et al.* (2020)	Bllockchain Evaluation Approaches: State-of-the-Art and Future Perspective	This study systematically reviews the current approaches to blockchain evaluation and identifies the limitations of them and provides future perspectives.

Continued on next page

Continued from previous page

Key	Source	Title	Description
12	Sukhwani *et al.* (2018)	Performance Modeling of Hyperledger Fabric (Permissioned Blockchain Network)	This study presents a performance model to identify the bottlenecks to the performance of Hyperledger Fabric.
13	Zheng *et al.* (2018*a*)	A Detailed and Real-time Performance Monitoring Framework for Blockchain Systems	This study presents performance metrics to monitor blockchain's performance during different stages.

Table 2.17: Blockchain Comparison Performance Metrics

Performance Metric	Definition	Sources
Throughput	Successful transactions or read operations per second.	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 13
Latency	Response time for transactions or read operations from initialization to execution and commitment.	1, 2, 3, 4, 5, 6, 7, 8, 9, 12, 13
Scalability	The number of participants the network is able to accommodate.	1, 8
Success Rate	The ratio of successful operations performed to the total number of operations.	3, 5, 8
Transactions Per CPU/GPU	The degree to which a CPU/GPU is consumed for blockchain operations.	5, 8, 9, 10, 11, 13
Transactions Per Memory Second	The degree to which memory is consumed per second of transactions for temporary operations that require memory for computation efforts.	5, 8, 9, 10, 11, 13
Transactions Per Disk I/O	The degree to which I/O is consumed by blockchain operations for reading from the hard disk (permanent storage) and writing to it.	9, 11, 13
Transactions Per Network Data	The degree to which the network flow (upload and download capabilities) are used for blockchain operations such as transferring data blocks.	9, 10, 11, 13

These are the performance metrics that are tied to blockchain solutions that will give a good indication of how well it performs and whether it is suited to a specific use case, while also being suitable in determining the performance of traditional IS solutions, thus allowing the two to be directly compared with regards to performance. The last four performance metrics listed are calculated in a specific way to enable consistent results. The equations for these performance metrics are given below, but more particular information can be found on them in the work of Zheng *et al.* (2018*a*).

Transactions Per CPU of a single user

$$TPC = \frac{Count(txs\ in\ (t_i, t_j))}{\int_{t_i}^{t_j} F \cdot CPU(t)} (txs/(GHz \cdot s)) \tag{1}$$

Where the numerator represents the number of transactions between the time interval $t_i - tj$, F is the frequency of a single CPU core and $CPU(t)$ is the usage of the CPU at time t. The average for the entire network can be calculated by simply adding all users TPC and dividing by the number of users and *Transactions Per GPU* can be similarly calculated.

Transactions Per Memory Second of a single user

$$TPMS = \frac{Count(txs\ in\ (t_i, t_j))}{\int_{t_i}^{t_j} RMEM(t) + VMEM(t)} (txs/(MB \cdot s)) \tag{2}$$

Where $RMEM(t)$ is the real memory used at time t and $VMEM(t)$ is the virtual memory used at time t. The average can be calculated using the same method as for TPC.

Transactions Per Disk I/O for a single user

$$TPDIO = \frac{Count(txs\ in\ (t_i, t_j))}{\int_{t_i}^{t_j} DISKR(t) + DISKW(t)} (txs/kilobytes) \tag{3}$$

Where $DISKR(t)$ is the size of the data which is read from the disk at time t and $DISKW(t)$ is the size of the data that is written to the disk at time t. The average can again be calculated using the same method as for TPC.

Transactions Per Network Data for a single user

$$TPND = \frac{Count(txs\ in\ (t_i, t_j))}{\int_{t_i}^{t_j} UPLOAD(t) + DOWNLOAD(t)} (txs/kilobytes) \tag{4}$$

Where $UPLOAD(t)$ is the size of the data being uploaded to the network at time t and $DOWNLOAD(t)$ is the size of the data being downloaded from the network at time t. The average can be calculated using the same method as for TPC.

Through reviewing the relevant literature on blockchain performance metrics a few insights revealed themselves. Firstly, the performance of a blockchain solution is incredibly nuanced, and evidently different configurations of blockchain will have vastly different performance metric outcomes and the challenge is in being able to configure a blockchain solution to perform as required by a paritcular use case, where performance is dependent on a vast range of factors from the hardware used by nodes to how the blockchain solution was developed (consensus mechanism, permissions, smart contracts, etc.). Secondly, being a relatively novel technology, there is not a plethora of case studies available and thus performance data is only available for very specific cases and attempting to identify the relationship between a blockchain solution's performance and the factors that affect the performance are out of the scope of this study. Lastly, there seems to be no common metrics with which to analyse blockchain solutions or to use to compare to traditional solutions and thus case studies are often using disparate metrics, making it difficult to gain insight on the performance of varied configurations.

This does not imply that the literature is useless in this domain, but rather it is limited and thus care should be exercised when searching for case studies that could indicate the performance of a certain blockchain solution. Appendix A.1 presents the performance of a number of different solutions with varied configurations, but keep in mind that although some solutions may appear similar in their configuration, there may be underlying elements which are fundamentally different, such as the hardware of the nodes on which they operate.

It is clear from Table A.1 that there are a lack of studies identifying performance values for different blockchain configurations using a range of performance metrics, with most studies focusing on throughput and latency. The studies tend to stick with two main blockchain platforms: Ethereum and Hyperledger Fabric. While these may provide great data for these specific configurations, data is greatly lacking for other potential configurations.

This points to the fact that there are not many studies focusing on other configurations, but there are other blockchain platforms which use different consensus mechanisms and blockchain types. Focusing on the consensus mechanisms used, a variety of blockchain platforms are listed below along with the relevant consensus mechanism being utilized

as identified by Thanujan *et al.* (2020).

- ***Proof of Work*** – Bitcoin, Ethereum, Litecoin, Dogecoin
- ***Proof of Stake*** – Ethereum, Peercoin, Nxt
- ***Delegated Proof of Stake*** – Bitshares, Nano, Cardano
- ***Proof of Elapsed Time*** – HyperLedger
- ***Practical Byzantine Fault Tolerance*** – Hyperledger Fabric, Hyperledger Iroha, Oracle, Hydrachain, BigchainDB

Note that some blockchain platforms are repeated, this is either because different versions of the platform use different consensus mechanisms or the platform can be configured with different consensus mechanisms depending on the use case. While academic literature is scarce on the performance analyses of a few of these blockchain platforms, certain performance metrics may be retrieved through documents published by the blockchain platform themselves or through experience with the blockchain platform.

2.6.2 Blockchain Costs

There are a variety of costs that can be incurred during the development, deployment and operation of a blockchain solution. Coupling this with the multiple configurations of a blockchain solution, determining the cost of a blockchain solution is not straightforward and heavily depends on a variety of nuanced factors. Two factors that will heavily dictate the time spent on development, and thus direct costs incurred, is the inclusion or exclusion of certain features during development and which development approach is taken. A few key items that may influence the cost of a blockchain solution have been identified in Table 2.18 through the previous work of the literature review, as well as the work of Gopalakrishnan *et al.* (2021) and Leewayhertz (2019).

Table 2.18: Development Cost Influencers

Cost Influencer	Options
Blockchain Type	Public Permissionless
	Public Permissioned
	Private Permissioned
	Private Permissionless

Continued on next page

Continued from previous page

Cost Influencer	Options
Financial Transaction	Application requires financial transaction
	Application does not require financial transaction
Network-User Interaction	Web interface
	Mobile application
	Admin interface
	Desktop interface
Proof of Concept	PoC required
	PoC not required
Deployment	Third-party cloud computation being utilized
	No cloud computation (on-premises)
	Hybrid
Developers	In-house
	Freelancers
	Agency/Outsourcing
Operation Complexity	Blockchain network is its own IS
	Blockchain network interacts with other IS's outside itself
Development Approach	From scratch
	Integrated with existing system
	Blockchain development platform (Hyperledger, Ethereum, R3, etc.)
Development Speed	Normal development speed
	Fast development
	Immediate development
Number of User Types (customer, supplier, administrator, customer support, etc.)	Any size required, noting that increased users affect performance

The items listed in Table 2.18 all have the ability to influence the cost of blockchain development, deployment and operation depending on the options chosen. Takyar (2019) identifies five different phases of blockchain implementation and the fraction of the total cost that each phase typically incurs. While these implementation phases do not line up perfectly with the blockchain lifecycle used in this study, as identified in Section 2.5.1,

there is overlap between the two. These phases, with their representative cost fractions and the typical cost elements associated with each phase, are presented in Table 2.19 below, with the information received from Takyar (2019) and Davies (2021), .

Table 2.19: Blockchain Implementation Cost Distribution

Blockchain Implementation Phase and Cost Distribution	Typical Cost Elements
Consulting Phase: 10%	Consultant fees
Design Phase: 15% - 20%	White paper cost Prototype development
Development Phase: 50% - 60%	Development (in-house, freelancer or agency) Smart contracts User interface development Cryptocurrency/Tokens (existing or new)
Quality Assurance: 20% - 25%	Security (sales, cyber) Legal costs Know your customer (KYC) costs Anti-money laundering (AML) costs Agency costs Individual costs
Deployment, Operation and Maintenance: 15% - 25% of the total project value paid yearly	Node hosting costs (third-party services or local) System Migration Maintenance and upgrading Continuous integration Storage and energy costs Infrastructure

Suppose an organization is considering designing and developing a blockchain solution from scratch, then all of the phases in Table 2.19 will be relevant. Conversely, if an organization decides to utilize a development platform for designing and developing a blockchain solution, there may be phases that are not relevant for this user. Regardless of the decision made, it is important to know what each stage entails so that the organization is aware of the possible costs that may be incurred in their development journey.

The consulting phase is the phase in which a range of services are used to ensure the successful development and ultimate deployment of a blockchain solution. During this

phase consultants will analyse the needs of the customer and diligently work with them to identify any further needs required of a blockchain solution and will ultimately present a framework identifying what their blockchain solution should and should not entail (Gopalakrishnan *et al.*, 2021). This phase takes a minimum of 10 hours, but can continue for weeks depending on the scale of the project (Gopalakrishnan *et al.*, 2021).

The design phase takes the needs identified in the consulting phase and creates a blockchain solution addressing these needs. This design solution is documented (typically in the form of a white paper) for future referral and can be used as a guide map for the trajectory of the solution (Gopalakrishnan *et al.*, 2021). Testing the solution as a prototype, before implementing it as an actual solution, forms part of the design phase due to the iterative element it introduces into the design.

The development phase consists of the activities required to physically develop the solution. This includes coding and developing the blockchain solution, as well as coding any smart contracts (or a method for implementing smart contracts) to ensure certain actions are taken when specific conditions are met. Furthermore, the inclusion or exclusion of a cryptocurrency or token should be considered, where an organization can either choose to develop their own or use an existing one. Useful interaction with the solution is of paramount importance and thus a relevant interface is required to access and input data to the system. Finally, the use of sensors should be considered and what data will be required and eventually retrieved from them and shared on the blockchain network.

The quality assurance phase involves the activities required to ensure that the legal and security aspects of the solution are addressed adequately (Gopalakrishnan *et al.*, 2021). It focuses on aspects of the blockchain solution that are aimed at ensuring that inputs are genuine and data is consistent. Typical options for this phase include KYC and AML analyses that are used for data and user authentication (Gopalakrishnan *et al.*, 2021). Furthermore, the effective use of oracles should be considered during this phase as addressed in Section 2.1.14.

The final phase is focused on the deployment, operation and maintenance of the blockchain solution. The deployment can either be via local servers or using a third-party service to host the nodes, where it is important to consider the pros and cons of each as addressed in Section 2.1.8.1. The operation focuses on the activities required to operate the system, such as information exchange and data storage. Maintenance is focused on ensuring that the blockchain solution operates as it should, by ensuring all nodes operate

effectively and that the solution's code is up to date without weaknesses.

It is evident from Table 2.19 that the cost of blockchain implementation is incredibly variable, and with such little data it is difficult to predict the cost of blockchain implementation for a particular use case. However, a number of the elements identified can be linked with an average estimated cost as shown in Table A.2. While these costs may vary quite drastically depending on a number of factors, it gives a good indication to the range of costs that can be expected.

A private blockchain consulting firm headquartered in San Francisco, which develop blockchain solutions themselves, provide quotes on expected costs and time based on a variety of aspects: development platform, blockchain type, financial transaction requirement, cloud deployment, network-user interface, development speed, PoC requirement, and the number of user types (Leewayhertz, 2019). Five various scenarios are presented in Table A.3 with the estimated costs and time associated with blockchain implementation.

Scenario 1 represents the most costly instance of blockchain implementation, while Scenario 2 represents the least costly instance of blockchain implementation. These five scenarios give a good indication of the range of costs that can be expected when implementing different kinds of blockchain solutions. However, note that these estimates can change drastically depending on a number of factors.

While blockchain has many costs associated with its implementation, there is a reason that an organization would decide to incur such costs. Often these reasons can be recognized in the process cost reductions that a blockchain solution will inherently introduce through the characteristics it possesses. Therefore, these process cost reductions are identified through the characteristics that blockchain solutions may possess. The main process cost reductions introduced by a blockchain solution are identified in Table 2.20 below.

Table 2.20: Blockchain Process Cost Reductions

Process Cost Reduction	Definition	Source
Verification Costs	Blockchain enables data to be distributed between multiple parties securely and thus reduces unnecessary duplication of data and constant requests for data, consequently saving time and money.	Hassani *et al.* (2018)
Improved Settlement Speeds	With one shared version of the truth, parties can transact with greater trust and thus reduce the need for intermediaries to process transactions to ensure integrity, thus reducing time and saving money.	Hassani *et al.* (2018); Niranjanamurthy *et al.* (2019).
Enhanced Security & Data Integrity	Data cannot be changed and all new information is shared with the relevant parties, making it secure because alterations can be tracked and monitored, thus requiring less effort in ensuring data integrity.	Hassani *et al.* (2018)
Policing & Enforcement Costs	Blockchain's transparency and immutability allow regulators to more easily and swiftly scrutinize any transactions to ensure compliance and that all parties stick to the terms of an agreement.	Hassani *et al.* (2018); Chen *et al.* (2022)
Transaction Costs	Reducing the need for constant administrative searching and communication activities, eliminating intermediaries, and increasing process transaction efficiency will reduce overhead costs because blockchain allows distributed access to a single, immutable source of truth.	Hassani *et al.* (2018); Hedman *&* Kalling (2003); Niranjanamurthy *et al.* (2019); Wang *et al.* (2016)

Continued on next page

Continued from previous page

Process Cost Reduction	Definition	Source
Bargaining Costs	Smart contracts can be used to automatically execute certain code based on set conditions in a transparent and efficient manner, thus reducing the need for complex and time consuming human interaction to reach agreement between parties on an appropriate contract.	Hassani *et al.* (2018); Panuparb (2019); Niranjanamurthy *et al.* (2019); Chen *et al.* (2022)
Search & Information Cost	Blockchain provides a "single line of sight", enabling more agile responses to events and more inter-organizational collaboration, while reducing the need for costly administrative searching and communication activities.	Chen *et al.* (2022)
Debugging Costs	Due to synchronization mishaps, data between organizations may be misaligned and addressing these misalignments can be time-consuming and costly, whereas blockchain removes the possibility of such misalignment.	Hassani *et al.* (2018)

Clearly, blockchain has many costs associated with it and the decision to implement it must not be taken lightly. However, the benefits that it potentially provides could outweigh the costs. A few of these benefits are outlined in Table 2.20 and it can be seen that many of the benefits have to do with reducing delays between certain actions. It is of utmost importance to weigh costs and benefits against each other to ensure that the investment is sound and will yield returns that are worth the effort of implementation.

2.7 Blockchain Assessment Aspects

It is evident by now that blockchain is an inherently complex technology and there are many aspects of it that can be assessed in a variety of different ways. This section will investigate the different ways in which blockchain has been assessed in academic literature since its inception, with the aim of identifying those blockchain assessment aspects that are prevalent in literature and ultimately which of these aspects should be included in an all-encompassing assessment framework.

The scope of such a framework has been determined by identifying the aspects addressed and methods used in academic literature to assess blockchain or elements of blockchain. The studies found to asses blockchain, along with the relevant areas of assessment they addressed, is presented in Table 2.21 below. This is followed by Table 2.22 where the strengths and weaknesses of each of the studies are explored.

Table 2.21: Blockchain Assessment Aspects

Assessment Study	Consensus Analysis	Type Analysis	Wave/ Maturity Analysis	Value Analysis	Fit Analysis	Adoption Analysis	Characteristics Analysis	Success Factors	Adoption Inhibitors
Scriber (2018)					X		X		O
Angelis & da Silva (2019)			X	X	X				
Wang *et al.* (2016)			X			O	O		
Fabrizio *et al.* (2019)					O		O		
Kharitonov (2017)						X	O		
Allessie (2017)	X	X		O	X		X	O	
Gourisetti *et al.* (2019)	X	X		O	X		X		
Erol *et al.* (2020)					X		X		
Yang *et al.* (2021)	X	X		O	X		X		
Ar *et al.* (2020)					X		X		

Continued on next page

Continued from previous page

Assessment Study	Consensus Analysis	Type Analysis	Wave/ Maturity Analysis	Value Analysis	Fit Analysis	Adoption Analysis	Characteristics Analysis	Success Factors	Adoption Inhibitors
Lo *et al.* (2017)					X		X		
Wüst *&* Gervais (2018)		X			X		X		
Yaga *et al.* (2019)	O				X		O		X
Peck (2017)		X			X				
Koens *&* Poll (2018)		O			X				
Lapointe *&* Fishbane (2019)		O			X	X	X		
Casino *et al.* (2019)		O					X		
Toufaily *et al.* (2021)				X		O	X		X

X = addressed

O = addressed to a limited degree

Table 2.22: Assessment Studies' Strengths and Weaknesses

Assessment Study	Strengths	Weaknesses
Scriber (2018)	A good fit analysis using quantitative aspects	Not a comprehensive assessment
	Uses blockchain characteristics to inform the analysis	Subjective inputs
	Highlights important considerations	Very high-level
Angelis *&* da Silva (2019)	Identifies how value is realized through blockchain characteristics and what that value entails	Not a comprehensive assessment
	Highlights important considerations	Very high-level
		No tangible outcomes (more conceptual)
Wang *et al.* (2016)	Identifies blockchain's maturity in different aspects	Not a comprehensive assessment
	Highlight important considerations during the adoption process	Very high-level
		No tangible outcomes (more conceptual)
Fabrizio *et al.* (2019)	Highlights important considerations for evaluating blockchain	Focused only on the process of invoice discounting
		Less an assessment approach, instead showing how blockchain was evaluated for the use case

Continued on next page

Continued from previous page

Assessment Study	Strengths	Weaknesses
Fabrizio *et al.* (2019)		No tangible outcomes
		Not comprehensive
Kharitonov (2017)	Highlights important considerations and a way for structuring thought around blockchain considerations	Not a comprehensive assessment
	Has good potential to provide in-depth analysis	Can be very subjective
Allessie (2017)	Assesses blockchain fit quantitatively and thoroughly	Is comprehensive, but not complete
	Presents a good high-level and quantitative design process linked to performance criteria	Many subjective inputs
	Highlights the different ripple effects expected from implementing blockchain	Specific to governmental information exchange and registration processes
Gourisetti *et al.* (2019)	Assesses blockchain design quantitatively and thoroughly	Not a comprehensive assessment
	Assesses blockchain fit quantitatively and thoroughly	Has subjective inputs
	Identifies different blockchain use cases	A lot of inputs required for the outcome

Continued on next page

Continued from previous page

Assessment Study	Strengths	Weaknesses
Erol *et al.* (2020)	Identifies different indicators for blockchain feasibility	Not a comprehensive assessment
	Assesses blockchain feasibility quantitatively	Only investigates industries in Turkey
Yang *et al.* (2021)	Quantitatively assesses different blockchain decision items based on evaluation criteria	Not a comprehensive assessment
		Specific to knowledge-based conversation systems
Ar *et al.* (2020)	Quantitatively assesses the feasibility of blockchain based on specific criteria	Not a comprehensive assessment
		Specific to logistics operations
Lo *et al.* (2017)	Assesses blockchain feasibility based on blockchain characteristics	Not a comprehensive assessment
		Very high-level
Wüst & Gervais (2018)	Assesses blockchain suitability based on blockchain characteristics	Not a comprehensive assessment
	Identifies specific blockchain type	Very high-level

Continued on next page

Continued from previous page

Assessment Study	Strengths	Weaknesses
Yaga *et al.* (2019)	Assesses blockchain feasibility based on blockchain characteristics	Not a comprehensive assessment
	Recommends alternative solutions if blockchain is not feasible	Very high-level
	Highlights important considerations	
Peck (2017)	Assesses blockchain feasibility based on blockchain characteristics	Not a comprehensive assessment
	Identifies specific blockchain type	Very high-level
Koens & Poll (2018)	Assesses blockchain feasibility based on blockchain characteristics	Not a comprehensive assessment
	Recommends alternative solutions if blockchain is not feasible	Very high-level
		Only considers public permissionless blockchain solutions
Lapointe & Fishbane (2019)	Assesses blockchain feasibility based on blockchain characteristics	Not a comprehensive assessment
	Highlights important considerations	Very high-level
	Identifies alternative blockchain solutions	

Continued on next page

Continued from previous page

Assessment Study	Strengths	Weaknesses
Casino *et al.* (2019)	Highlights important considerations	Less an assessment approach and more an analysis of blockchain applications
	Compares blockchain solutions to traditional databases	Not comprehensive
	Compares the different blockchain types	No tangible outcomes
	Identifies different blockchain use cases	
Toufaily *et al.* (2021)	Highlights important considerations	Not a comprehensive assessment
	Investigates the expected value of different blockchain solutions	No tangible outcomes (more conceptual)

Using the above table as a reference, the scope of blockchain assessments within literature can be seen. Using this information, these assessment aspects can be combined and distilled to be left with four main areas of blockchain analysis. The four areas are identified as follows:

- **Blockchain Fit Analysis** - an analysis to determine how well suited blockchain is for a particular process within a particular organization and to determine blockchain suitability on a high level.
- **High Level Blockchain Design** - an analysis to determine a high level blockchain design based on the end user's use case and preferences.
- **Blockchain Adoption Analysis** - an analysis to determine the blockchain adoption approach on a high level, as well as identifying considerations during the blockchain solution's lifecycle.
- **Blockchain Value Analysis** - an analysis to determine the value of a blockchian solution within a particular scenario, using hard metrics to present this.

With these main areas of blockchain analysis identified, each of the different aspects identified in Table 2.21 will fall under at least one of the identified areas. By being able to categorize any useful blockchain assessment aspect under at least one of these four main areas of blockchain analysis indicates that the scope of these areas is all-encompassing. This provides a solid base from which a blockchain assessment approach may be developed. Furthermore, Table 2.22 helps to identify the strengths that can be combined from the different studies, as well as the weaknesses to be avoided.

2.8 Chapter Summary and Conclusion

This chapter built the foundation of literature necessary for the ultimate outcome of the study. It began with an extensive review of blockchain technology in Section 2.1, where the operation and components of blockchain were identified and explored. This section was used to create a deep understanding of what blockchain entails and showcase the complexity involved when dealing with it and the myriad of choices to be made when developing a blockchain solution.

This was followed by Section 2.2 in which the functional characteristics of blockchain were identified by considering how it operates and what it is potentially composed of. Furthermore, this section looked at the challenges of blockchain and compared blockchain

solutions to more traditional databases. Section 2.3 highlighted the different use cases in which blockchain solutions may provide value. Section 2.4 analysed the different factors which dictate blockchain's suitability in a particular context, whereby these factors were broken into critical, organizational, and process factors.

Section 2.5 delved into blockchain adoption and what the typical blockchain lifecycle entails. This was followed by different considerations to be taken during blockchain adoption and ended with different strategies for blockchain adoption. Section 2.6 introduced different metrics that can be used to compare blockchain solutions with one another and other IS solutions, using both performance and cost metrics. Finally, Section 2.7 identified the different aspects of blockchain assessment and distilled them into four main areas of blockchain assessment and went on to identify the strengths and weaknesses of the current approaches.

This chapter answered multiple research questions: SO1.1, SO1.2, SO2.1, SO2.2, SO2.3, SO2.4, SO3.1, SO4.1, and SO4.3. The chapter has gathered all of the literature required to satisfy the main objective of the study. The insights gathered throughout this chapter are now put to use in Chapter 3 to design the solution that will ultimately satisfy the main objective of this study. Chapter 3 is focused on identifying a design approach and using the insights of Chapter 2 to identify the design requirements and design a blockchain assessment framework.

3 SOLUTION APPROACH AND DESIGN

Coming from the literature review of Chapter 2, the complexity of blockchain is evident and the need for an assessment framework to assist in the analysis of such a complex technology for business scenarios is clear. Such a framework will greatly enhance the analysis of blockchain solutions, allowing for insights that could lead to drastically lower failure rates. This chapter of the study will outline the approach and design of such an assessment framework.

3.1 Design Requirements

A crucial element in the success of the proposed assessment framework is the ability to define the design requirements. It is crucial to compile these requirements so that the needs and wants of the potential assessment framework user are established (Dieter *et al.*, 2013). Firstly, to identify the design requirements, it is important to understand what the end user should be able to accomplish using this assessment framework.

The assessment framework must enable the end user to structure their thinking around the analysis of blockchain feasibility for an organization, by promoting logical and systematic thinking, ultimately facilitating an understanding of the topic. Providing tangible outcomes from the assessment framework will enhance the understanding of such an analysis. The assessment framework should force decisive selections of varying importance to be made, thereby reducing unnecessary variables. The assessment framework should also be comprehensive, transparent, and simple to use and implement, so as to reduce the impact of any potential biases. Ultimately, the assessment framework must act as a communication tool to drive decision making regarding blockchain feasibility in a concise manner, by identifying what information is important and what can be neglected.

3.1.1 Requirement Categories

The design requirements of the assessment framework can be divided into four different categories, as identified by van Aken & Berends (2018). The categorization of the design requirements ensures that certain requirements are not overlooked and it can further aid as a type a checklist to determine requirements more easily according to the relevant categories. These design requirement categories are identified and defined as follows:

1. ***Functional Requirements (F)*** – these form the core of the requirement specifications and are usually in the form of framework performance or result demands (Brockmöller, 2008). Realization of these functional requirements in the assessment framework should satisfy the study's main objective (van Aken & Berends, 2018).

2. ***User Requirements (U)*** – these are the requirements that can be identified from the viewpoint of the user and regard the use of the final design (Brockmöller, 2008).

3. ***Boundary Conditions (B)*** – these requirements must be met unconditionally without any alteration (Krause & Schutte, 2015).

4. ***Design Restrictions (D)*** – these requirements address the preferred solution space, by highlighting limits, exclusions and neglected elements of the solution (Krause & Schutte, 2015). The difference compared to boundary conditions is that design restrictions are potentially negotiable (van Aken & Berends, 2018).

The design requirements simply represent the functional needs and wants of a specific design within a certain solution space, which enable ideas to be converted into design features allowing the end design to perform its desired function (Privitera, 2015). While some requirements may be more crucial than others, the requirements simply highlight the elements that require consideration during the design of a successful assessment framework. The design requirements of the assessment framework can now be identified according to the above categorisation in the proceeding sections. The design requirements are determined using the insights gained from the literature review of Chapter 2 and the input of industry experts.

3.1.2 Functional Requirements

As mentioned previously, the functional requirements form the core of the solution design and ultimately guide what the assessment framework should enable the user to accomplish by using it. The functional requirements for the assessment framework are presented, with motivations, in Table 3.1 below.

Table 3.1: Assessment Framework Functional Requirements

Requirement Tag	Description
F1	*Requirement:* the assessment framework must comprehensively and quantitatively determine the feasibility of a blockchain solution within a specific business case context to guide decision-makers in the decision-stages of blockchain implementation and provide motivation for such a decision by providing insights on a blockchain solution's feasibility and applicability.
	Motivation: this is the overarching goal of the framework and is required to satisfy the main objective of this study identified in Section 1.3.1.
F2	*Requirement:* the assessment framework must assess the critical factors that relate to the high-level fit of blockchain within the business case context.
	Motivation: assessing these critical factors early on in the assessment framework will enable faster decision making on blockchain's suitability for a specific business case context.
F3	*Requirement:* the assessment framework must assess the process factors related to *users, process facilitation, hardware and software, control, and data* that define the fit of a blockchain solution within a particular process.
	Motivation: assessing these process factors will enable quantitative values to be produced that rate the fit of a blockchain solution within a particular process.
F4	*Requirement:* the assessment framework must assess the organizational factors related to *core expertise, critical, operation, willingness, and industry* that will define the fit of a blockchain solution within a particular organization.
	Motivation: assessing these organizational factors will enable quantitative values to be produced that rate the fit of a blockchain solution within a particular organization.

Continued on next page

Continued from previous page

Requirement Tag	Description
F5	*Requirement:* the assessment framework should accept blockchain characteristic preference inputs to allow a high-level blockchain design to be presented as an outcome.
	Motivation: the determination of a specific blockchain configuration will allow more precise predictions of certain metrics to be presented and thus provide more accurate outcomes, increasing the chances of an indicative assessment.
F6	*Requirement:* the assessment framework should allow a broad use case to be identified based on the specific business scenario being investigated.
	Motivation: use case identification will enable a better understanding of the solution space and will make the high-level blockchain design more specific.
F7	*Requirement:* the assessment framework must enable a thought experiment on the many considerations and potential effects applicable to blockchain implementation and its lifecycle.
	Motivation: presenting the many considerations allows the user to identify and prepare for any possible trajectories the blockchain solution may take, thus enabling a comprehensive view from which to make effective decisions regarding blockchain.
F8	*Requirement:* the assessment framework must identify different avenues of potential blockchain revenues and costs.
	Motivation: revenue and cost identification will allow the user to better anticipate the possible current and future business value potential of blockchain solutions and therefore make a more informed decision regarding blockchain.
F9	*Requirement:* the assessment framework must indicate the balance between the level of control the owner has over the blockchain solution and the decentralization or openness of the blockchain network.

Continued on next page

Continued from previous page

Requirement Tag	Description
F9	*Motivation:* there is a fine balance between control and decentralization in blockchain business solutions and this needs to be considered and addressed by the user for a more applicable solution.

3.1.3 User Requirements

The assessment framework users considered are persons with a limited knowledge of blockchain solutions and they have the potential to implement a blockchain solution within a business environment. The user is expected to have knowledge of the current IS, if applicable. The user requirements for the assessment framework are presented, with motivations, in Table 3.2 below.

Table 3.2: Assessment Framework User Requirements

Requirement Tag	Description
U1	*Requirement:* the assessment framework must be user-friendly, i.e. easy to use, understandable, and logically designed.
	Motivation: a user-friendly assessment framework will promote the use of itself and will ensure it is accessible to a wide range of users, not only specialists.
U2	*Requirement:* the assessment framework must allow the user to apply their own discretion when using it.
	Motivation: the complex nature of blockchain requires an assessment framework that is adaptable and customisable to suit the specific business scenario being assessed.
U3	*Requirement:* the assessment framework must provide clear and concise explanations.
	Motivation: clear and concise explanations on the use of the assessment framework will simplify the use and increase the adoption of the assessment framework for analysing blockchain solutions within business contexts.

Continued on next page

Continued from previous page

Requirement Tag	Description
U4	*Requirement:* the assessment framework must be seen as a decision-making tool for the user.
	Motivation: there is much uncertainty about the future trajectory and success of a blockchain project and thus the assessment framework should help users decide if the risk is reasonable.
U5	*Requirement:* the assessment framework should foster an understanding of blockchain for the user to better grasp the technology they intend to implement.
	Motivation: with a better understanding of what blockchain is and what it entails, the user will be able to make a more informed decision on blockchian implementation.

3.1.4 Boundary Conditions

The boundary conditions of the framework tend more towards rules, as opposed to requirements, and thus need to be met during the design of the framework. The boundary conditions for the assessment framework are presented, with motivations, in Table 3.3 below.

Table 3.3: Assessment Framework Boundary Conditions

Requirement Tag	Description
B1	*Requirement:* the assessment framework should be used in an ethical manner by potential users.
	Motivation: the author has no control over how the assessment framework will be used and thus needs to design it in such a way that future use is ethical.
B2	*Requirement:* the assessment framework should not be able to be used to negatively impact any party involved in the assessment directly or indirectly.

Continued on next page

Continued from previous page

Requirement Tag	Description
B2	*Motivation:* the assessment framework should not be used to exploit or manipulate any parties involved for the benefit of another and the design must reflect this aversion to malpractice.
B3	*Requirement:* the assessment framework should provide value to all parties involved and establish trust among them with regards to blockchain decision-making.
	Motivation: blockchain is a cooperative technology and the assessment framework should promote this by providing value and improving trust among involved parties.
B4	*Requirement:* the assessment framework should aid the user and potential blockchain owner in identifying potential regulatory considerations.
	Motivation: blockchain is a new technology and there is a lot of uncertainty surrounding it and thus the assessment framework needs to enable a thought experiment on the possible rules and regulations that may be introduced or have been introduced.
B5	*Requirement:* the assessment framework must be flexible, allowing it to be used for multiple industries as opposed to optimized for one.
	Motivation: flexibility forms part of the main objective identified in Section 1.3.1, where 'generic' and 'flexible' can be used interchangeably.

3.1.5 Design Restrictions

The design restrictions indicate the limits of the design by highlighting the solution space of the assessment framework. The design restrictions will consequently indicate the scope of the assessment framework. The design restrictions for the assessment framework are presented, with motivations, in Table 3.4 below.

Table 3.4: Assessment Framework Design Restrictions

Requirement Tag	Description
D1	*Requirement:* the assessment framework must identify barriers to entry for potential users and hence potential blockchain adopters.
	Motivation: there are certain barriers to overcome, identified as critical factors in Section 2.4.1, in order to receive any potential value from blockchain.
D2	*Requirement:* the assessment framework need not include an exhaustive set of methods and components to indicate blockchain feasibility, but it should be enough to provide sufficient value for a more informed blockchain feasibility decision.
	Motivation: there are many avenues of a blockchain solution and addressing all of them in one assessment framework will make it convoluted and hard to use and thus only the primary elements of blockchain, which will affect the outcome, need to be considered to satisfy the main objective of the study.
D3	*Requirement:* the assessment framework will not act as a legal guide regarding blockchain implementation.
	Motivation: the assessment framework is intended to be used in a variety of industries and the legalities of these industries will be specific to the industry and will require specialists, which this assessment framework will not claim to be.
D4	*Requirement:* the assessment framework will not guarantee success, but rather the potential feasibility of blockchian in a particular business scenario.
	Motivation: there are many factors that will influence the success of a blockchain solutions and this assessment framework will not account for all of them and thus is solely an indication of feasibility.
D5	*Requirement:* the assessment framework is intended primarily for assessing technical feasibility, with secondary assessments indicating high-level financial feasibility, organization feasibility, process feasibility, and implementation considerations.

Continued on next page

Continued from previous page

Requirement Tag	Description
D5	*Motivation:* there are many aspects to a technology's feasibility and this assessment framework will not attempt to address all in-depth, but will instead only look at those mentioned.
D6	*Requirement:* the assessment framework is intended for businesses within South Africa that are contemplating blockchain as a potential IS solution, either replacing a current one or as an entirely new IS solution.
	Motivation: different countries and use case scenarios will have different landscapes and considerations and thus this assessment framework will consider only businesses within South Africa. This is not to say it cannot be used in other countries and use cases, but it may need tweaking to do so.
D7	*Requirement:* certain inputs will be subjective to the user and thus different users assessing the same business scenario may receive different outcomes as a result.
	Motivation: as discretion is intended to be used, subjective inputs are expected and thus certain outcomes will differ between users naturally.
D8	*Requirement:* the assessment framework must be user focused.
	Motivation: the assessment framework needs to ensure it focuses on the problem presented by the user and understands what the user needs in order to solve this problem and ultimately contributes what is needed.
D9	*Requirement:* the assessment framework must primarily be used for an initial blockchain assessment but must also allow for multiple levels of increasing detail through the use of iteration and feedback loops.
	Motivation: users might require more in-depth outcomes than what the first high-level pass of the assessment framework provides, thus highlighting the need for potentially more passes.

3.2 Framework Design

This section will present the chosen design methodology and the actual design of the assessment framework solution. It begins with explaining the methodology behind the design, the high-level assessment framework objectives and the potential users of the assessment framework. Armed with this information, the actual components and structure of the assessment framework are identified and pieced together to create the final blockchain assessment framework solution.

3.2.1 Design Methodology

While the design is presented in a linear fashion, an iterative design methodology was used throughout. There are three main phases that can be identified in this iterative cycle: requirements definition, design, and solution demonstration and validation. The employed methodology uses a feedback loop between the requirements definition phase and the design phase, using the requirements to guide the design and conversely using the design to adjust the requirements as more information is presented. The initial requirements were distilled via the theoretical background from the literature review and input from industry experts, and the initial design was created using these distilled requirements. New information presented by the design process was used to alter the requirements and then using these altered requirements to adjust the design. Finally, a use case and expert analysis were employed to test and gather feedback on the design of the assessment framework, ultimately being used as inputs to alter the requirements and hence the design. This iterative design methodology is presented in Figure 3.1 below.

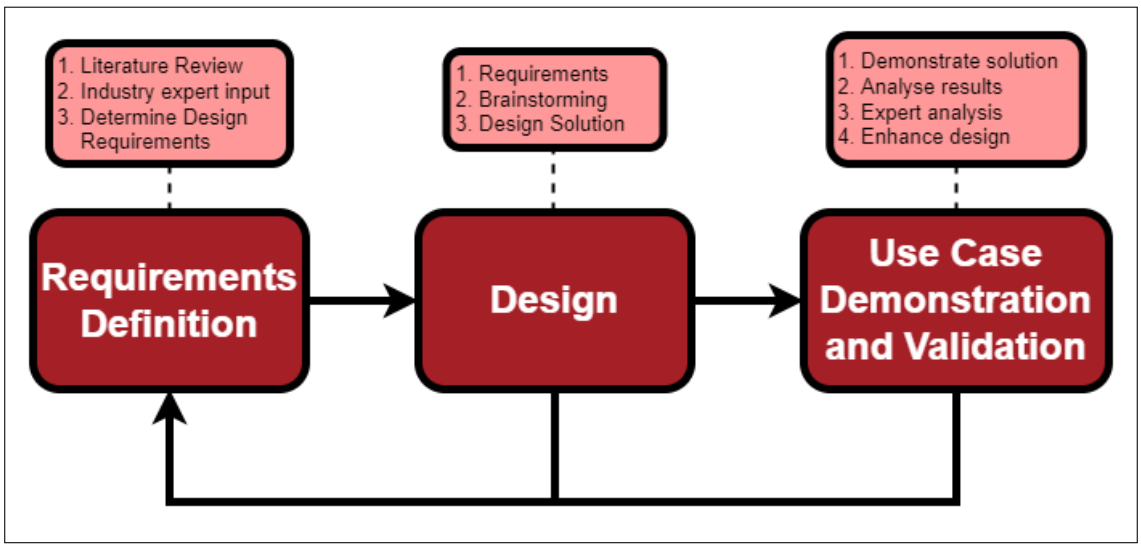


Figure 3.1: Iterative Design Methodology

3.2.2 Framework Elements

According to functional design requirement F1, the assessment framework is required to be comprehensive and therefore must include certain analyses to cover the scope of a comprehensive blockchain assessment framework. The literature review, coupled with the functional requirements identified in Section 3.1.2 and the main aspects of blockchain assessment identified in Section 2.7, can be used to identify the analyses that are required for the successful design of a comprehensive blockchain assessment framework. The combination of these areas results in the actualization of the main framework elements identified in Figure 3.2.

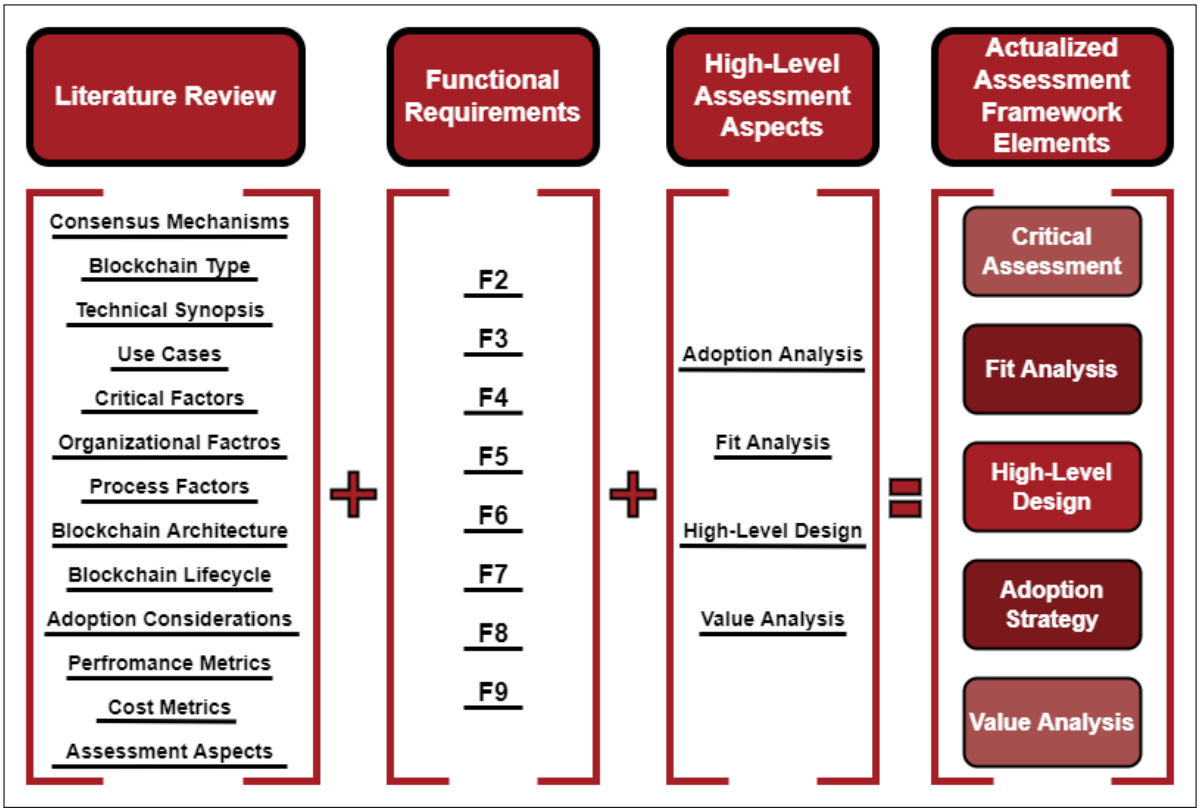


Figure 3.2: Actualized Framework Elements

The actualized blockchain assessment framework elements identified can now be used in conjunction with one another to form a comprehensive blockchain assessment framework. All of the areas and their respective aspects are represented in at least one of the actualized elements, where each element will have a specific outcome tied to it. These elements are designed and presented below. The design is informed by the design requirements identified in Section 3.1 and the strengths and weaknesses of current blockchain assessment approaches as identified in Table 2.22.

3.2.2.1 Blockchain Critical Assessment

This element of the blockchain assessment framework focuses on determining the applicability of blockchain within a particular context based on certain critical factors. Using the theoretical background of Chapter 2, namely Section 2.4.1, these critical factors can be identified and linked with evaluation questions that are used to allow the user to swiftly determine whether blockchain is applicable in their specific scenario. Taking the critical factors from Section 2.4.1, the evaluation questions that are used to gauge all of the factors are presented in Table 3.5 below.

Table 3.5: Critical Factor Evaluation Questions

Critical Factor	Evaluation Question
Data Store/Exchange*	Do you need to store or exchange data?
Multiple Distributed Parties*	Are there multiple parties inputting, updating, and reading information from distributed locations?
Validated Transactional Data*	Are exchanges/transactions involved or is the data transactional and must these transactions be validated?
Lack of Trust	Is there a lack of trust or conflicting interests among involved parties?
Lack of a Trusted Intermediary	Is there a lack of a trusted intermediary or need/want to remove them?
Consistent Set of Rules	Can a consistent set of rules help achieve the process outcome?
Consistent Governing Rules	Will the governing rules be consistent over time?
Interrelated Transaction History	Is transaction history required and are transactions dependent or interrelated?
Mapping Party Transactions	Must parties be mapped to their transactions or do transactions have increased value when claimed by a party?
Transparency Importance	Is transparency of the transactions a beneficial feature?
Immutability and Auditability Importance	Is an immutable, auditable record of transactions beneficial?
Censorship or Attack Reduction	Can a distributed infrastructure reduce the risk of censorship or attack?

**essential for blockchain suitability*

An affirmative answer for the evaluation questions indicate that blockchain is a suitable candidate for the specific use case. While an affirmative answer is not required for all critical factor evaluation questions, the greater the number of negative answers, the weaker the case is for blockchain implementation within the specific use case. Furthermore, the first three critical factors are required for blockchain implementation, otherwise the use case is better suited with an alternative solution.

The more negative answers there are, the more nuanced the blockchain solution will become, pushing it further away from the ideal situation in which a blockchain solution would operate. Consequently, any more than three negative answers indicates that the blockchain solution becomes too nuanced or is not being used to its full potential and is thus not suited for the specific use case.

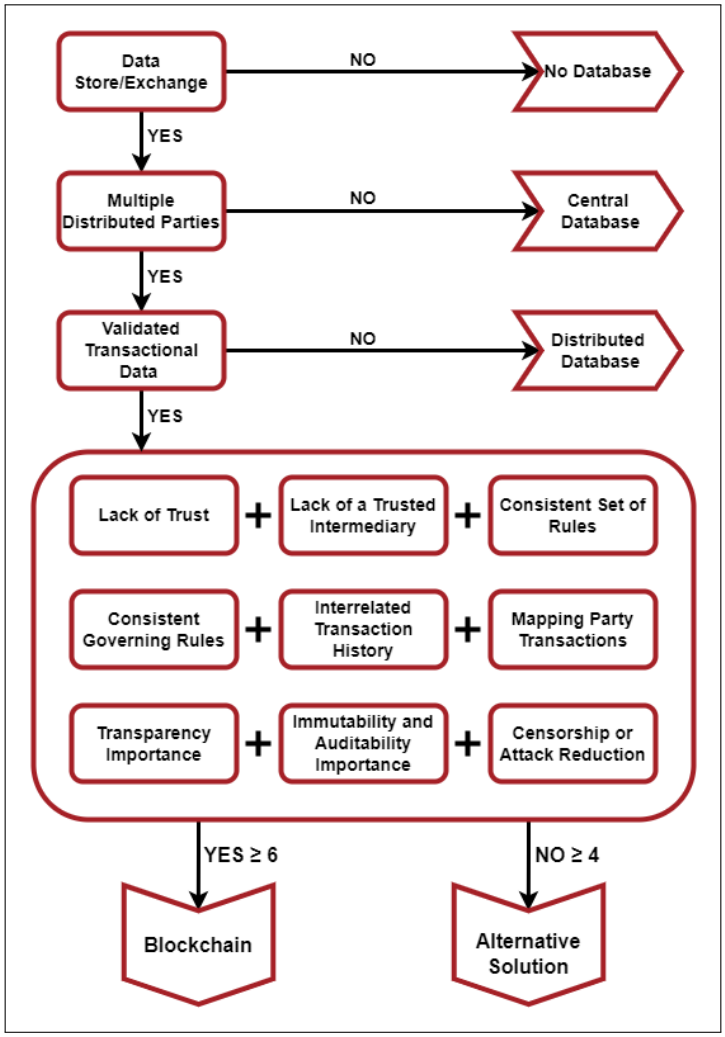


Figure 3.3: Critical Assessment Framework

Figure 3.3 can be used in conjunction with Table 3.5 to swiftly and concisely determine the applicability of blockchain for a specific use case based on the features that blockchain solutions enable and the features that the use case requires. It should be noted that a central database is recommended when there are not multiple parties, or the participants are not distributed. Furthermore, a distributed database is recommended when there are no exchanges or transactions or these transactions are not required to be validated. Lastly, the alternative solution proposed when there are more than four negative answers simply implies that the solution space is nuanced and requires a more in-depth comparison of all alternatives, including blockchain, to determine the applicable solution, if any.

3.2.2.2 Blockchain Fit Analysis

This element of the blockchain assessment framework assumes that blockchain is suitable for the specific use case on a high-level, whereby this element then determines how well suited blockchain is for the given use case. The theoretical background of Chapter 2, primarily Sections 2.4.2 and 2.4.3, is used to identify the factors that will influence the fit of blockchain in a given scenario. Blockchain's fit is broken into two components for this element, it's fit within an organization and it's fit within a particular process within that organization. The fit of blockchain within these two components will be represented by the "Organizational Fit Score" and the "Process Fit Score", which will indicate how well suited blockchain is for a particular process within a particular organization. This element is consequently separated with each section indicating the presenting the method for determining the respective "Scores".

Organizational Fit Score

There are certain factors which will affect how well suited blockchain is for a particular organization. These factors can be extracted from Section 2.4.2, where they were identified, combined, and distilled from the previous literature as well as various studies. These factors can be investigated for a particular organization by answering the evaluation questions and statements presented in Table 3.6.

Table 3.6: Organizational Factor Evaluation Questions and Statements

Domain	Organizational Factor	Evaluation Question/Statement	Threshold Value	Importance
Critical	Administrative Authority Support	The administrative authority supports blockchain experimentation.	61	1.0
	Financial Support	The financial means are available for blockchain experimentation and implementation.	61	1.0
	Legal/ Regulatory Framework	The legal/regulatory framework allows for blockchain experimentation and implementation within this industry/organization.	61	1.0
Core Expertise	Managerial Capabilities	The managerial capabilities are available for blockchain experimentation and implementation.	51	0.75
	Blockchain Complexity	The organization comprehends blockchain's complexity.	51	0.35
	Risk Aversity	The organization is risk averse with IT innovation experimentation and implementation.	51	0.6
	IT Capabilities	The organization has the IT capabilities or the ability to outsource for blockchain experimentation and implementation.	61	0.8

Continued on next page

Continued from previous page

Domain	Organizational Factor	Evaluation Question/Statement	Threshold Value	Importance
Core Expertise	Blockchain Enthusiast	Is there a blockchain enthusiast within the organization that understands blockchains and is willing to experiment with and implement it?	Maybe	0.4
	Technological Uncertainty	The organization is capable of handling technological uncertainty linked with blockchain applications.	51	0.8
Operation	Interoperability	The organization does not use a particular set of data in multiple different network systems.	51	0.3
	Decentralized Characteristics	The organization is willing to decentralize data storage.	51	0.6
Willingness	Top-management Dedication	The organization's top-management is dedicated to blockchain experimentation and implementation.	51	0.8
	Collaborating Parties Willingness	Potential stakeholders are willing to participate in blockchain experimentation and implementation that is led by the organization.	51	0.8
	Inter-organizational Trust	Potential stakeholders trust the organization to facilitate data exchange/registration.	51	0.2
	External Influence to Adopt	There are external influences on the organization to adopt blockchain (pressure, incentives, penalties, etc.).	51	0.2

Continued on next page

Continued from previous page

Domain	Organizational Factor	Evaluation Question/Statement	Threshold Value	Importance
Industry	Similar Use Cases in the Market	Are there existing use cases similar to the one being explored?	Maybe	0.45
	Collaborating Parties Competencies	Potential stakeholders are competent to experiment with and implement blockchain.	51	0.8
	Fraud Prevalence	Is fraud prevalent in your industry or organization?	Maybe	0.3

The questions are simply answered with a "Yes", "No" or "Maybe", while the statements are all answered on a scale of 0 – 100, where different ranges indicate various levels of agreement with the statement as outlined in Table 3.7. The threshold answer identified in Table 3.6 refers to the value within the range that indicates the threshold between blockchain being suitable and not being suitable. The threshold values tend to mostly fall around the middle mark, but for some factors a blockchain solution requires it to be more true, and thus these factors have a higher threshold value to indicate this.

Table 3.7: Statement Answer Range

Range	Answer
0 – 20	Very False
21 – 40	False
41 – 50	Partially False
51 – 60	Partially True
61 – 80	True
81 – 100	Very True

Finally, the importance value for each organizational factor indicates the factor's importance to a suitable blockchain fit. The importance values fall on a scale from 0 – 1, where different ranges indicate various levels of importance as indicated in Table 3.8. The importance ratings are assigned based on the effect that not satisfying the factor would induce, where a greater effect leads to a higher importance. The effect of not satisfying a factor was determined by considering whether the blockchain solution would still be viable should the factor not be satisfied, and whether there are ways in which to implement the blockchain solution such that the factor's importance can be reduced by developing it in an alternative manner and the consequent effort of having to do so.

Table 3.8: Importance Answer Range

Range	Importance
0 – 0.25	Not Important
0.26 – 0.50	Mildly Important
0.51 – 0.75	Important
0.76 – 1.0	Very Important

With the information presented above, the **Organizational Fit Score** can now be calculated. A simple formula is required that takes into account both the importance

weightings and the answer value for each evaluation statement/question. Thus, the fuzzy weighted average method is used, which was originally proposed by Dong & Wong (1987) and is shown in Equation 5 below.

$$Organizational\ Fit\ Score = \frac{\sum_{i=1}^{i=n} w_i \cdot x_i}{\sum_{i=1}^{i=n} w_i} \tag{5}$$

Where w_i = importance weighting, x_i = factor answer value, and n = number of factors. This formula is used to calculate the user's **Organizational Fit Score** based on their respective answers for each factor and the importance ratings assigned to them. Non-numeric answers are scored as shown in Table 3.9 below.

Table 3.9: Non-numeric Answer Values

Answer	Value
Yes	75
Maybe	50
No	25

All tools are now available to calculate a user's **Organizational Fit Score** for their specific organization. Using the above information, a threshold score can be calculated using the threshold answers and importance weightings of Table 3.6. This threshold score represents the **Organizational Fit Score** where a blockchain solution becomes suited for an organization. **The threshold value for the Organizational Fit Score is 54.30.** Thus, a score above the threshold score indicates that blockchain is a good fit for the organization, while a score below the threshold score indicates that blockchain is not a good fit for the organization.

Process Fit Score

With the factors that define the fit of blockchain within an organization, there are also factors which will affect how well suited blockchain is for a particular process within that organization. These factors are extracted from Section 2.4.3, where they were identified, combined, and distilled from the previous literature of the study as well as various other studies. These factors can be evaluated for a particular process by answering the evaluation questions presented in Table 3.10.

Table 3.10: Process Factor Evaluation Questions and Statements

Domain	Process Factor	Evaluation Question	Answer Range & Threshold Value	Importance
Users	Predictable Actor Behaviour	How predictable is the data input and behaviour of potential actors in the network?	Predictability (0 – 100): **61**	0.8
	Limited Trust in Current Process	Do current actors lack trust in the current process?	Lack of Trust (0 – 100): **50**	0.4
	Desired User Control Over Data	Will potential stakeholders want to store their data locally for better control in the process?	Desired Control (0 – 100): **50**	0.7
	High Importance of User Experience	What is the level of importance for the user's experience and ease of use in the process?	UX Importance (0 – 100): **50**	0.3
	Transparency Required	Is it required for transparent data to exist between potential stakeholders involved in the network?	Transparency (0 – 100): **61**	0.7
Process Facilitation	Peer-to-Peer Potential	Is there potential for the process to be facilitated by peer-to-peer interactions?	**Yes**/No/Maybe	0.8
	Low Interest of Organization Being Intermediary	Is there a low interest of the organization being the intermediary in this process?	Yes/No/**Maybe**	0.3
	High Availability of Bandwidth	Does the network have enough available bandwidth and computing power for the required specifications?	Availability (0 – 100): **50**	0.8

Continued on next page

Continued from previous page

Domain	Process Factor	Evaluation Question	Answer Range & Threshold Value	Importance
Process Facilitation	Low Throughput of Data	What is the frequency of transactions experienced?	High (>2000tps)/ **Medium**/ Low (<100tps)	0.6
	Current Laborious Human Facilitations	Is human labour required to facilitate the process?	Yes/No/**Maybe**	0.3
	Workflow Simplification	Will distributed ledger technology help simplify the workflow of the process?	Simplification (0 – 100): **50**	0.9
Hardware/ Software	Legacy Systems in Place	What is the level of the legacy systems that are currently in place?	**Brownfield**/ Greenfield	0.3
	Interface Differentiation	Do all involved parties have their own interfaces for the process or are all interfaces standardized?	**Single**/Multiple	0.55
Control	Low Institutionalized Environment	Is there a lack of bureaucracy in place for this process?	Lack of Bureaucracy (0 – 100): **50**	0.9
	Network Ability to Implement Technology Standards	Do the potential stakeholders adapt well to new technology standards?	Yes/No/**Maybe**	0.7

Continued on next page

Continued from previous page

Domain	Process Factor	Evaluation Question	Answer Range & Threshold Value	Importance
Control	Importance of Control Over the Infrastructure	How reasonable is it to have a lack of control over the infrastructure of the network?	Lack of Control (0 – 100): **50**	0.4
Data	Data Complexity	Are there multiple data formats involved in the process?	**Single**/Multiple	0.55
	Low Trust in Current Data Storage	Is there a lack of trust or information asymmetry in the data storage of the current system?	Yes/No/**Maybe**	0.4
	Traceability Required	Is it required to be able to trace who has accessed and created data in the network?	Traceability (0 – 100): **61**	0.5
	Data Integrity	What level of data integrity is required for the process?	Data Integrity (0 – 100): **50**	0.6
	Interoperability Possibility	Is the data from the current process involved in other processes? Is there one or many different uses of the data?	**Single**/Multiple	0.55
	Inter-organizational Information Exchange	Is there data exchange between multiple organizations or distributed branches of the same organization?	**Yes**/No/Maybe	1.0

Continued on next page

Continued from previous page

Domain	Process Factor	Evaluation Question	Answer Range & Threshold Value	Importance
Data	Transaction Dependency	Are there interactions between the transactions created by the potential stakeholders of the network?	Yes/No/**Maybe**	0.75
	Asset Digitization Potential	How much potential is there for the assets involved in the transactions/exchanges to be digitized?	Potential (0 – 100): **50**	0.8
	Privacy of Sensitive Data	Is there process information that is privacy sensitive?	Privacy Importance (0 – 100): **50**	0.4

These evaluation questions are either answered on a scale of 0 – 100 when gauging a certain characteristic or they are simply "Yes", "Maybe", or "No" answers or they are specialized answers specific to the question as identified in Table 3.10. Different ranges within the 0 – 100 scale indicate various levels of agreement with the specific characteristic it pertains to as outlined in Table 3.11. Similar to the "Organizational Fit Score", there are threshold values which are indicated in bold in Table 3.10. The threshold values again tend to fall around the middle mark, but some factors require greater levels of agreement and the threshold values will indicate this.

Table 3.11: Question Answer Range

Range	Answer
0 – 20	Very Low
21 – 40	Low
41 – 60	Medium
61 – 80	High
81 – 100	Very High

Similar to the **Organizational Fit Score**, there is an importance weighting indicating the factor's importance to a suitable blockchain fit within a particular process. The importance weighting ranges are identical to that of the **Organizational Fit Score** ranges and are presented in Table 3.12 again for ease of use. Furthermore, the importance weightings were assigned using the same conceptualization as for the **Organizational Fit Score** importance weightings assignment.

Table 3.12: Importance Answer Range

Range	Importance
0 – 0.25	Not Important
0.26 – 0.50	Mildly Important
0.51 – 0.75	Important
0.76 – 1.0	Very Important

With the information above, the **Process Fit Score** can now be calculated using Equation 6. This is the same equation used for the **Organizational Fit Score** and is simply repeated for ease of use.

$$Process\ Fit\ Score = \frac{\sum_{i=1}^{i=n} w_i \cdot x_i}{\sum_{i=1}^{i=n} w_i} \tag{6}$$

Where w_i = importance weighting, x_i = factor answer value, and n = number of factors. This formula can be used to calculate the user's **Process Fit Score** based on their respective answers for each factor and the importance weightings assigned to them. Non-numeric answers are scored as shown in Table 3.13 below.

Table 3.13: Non-numeric Answer Values

Answer	Value	Answer	Value
Yes	75	Brownfield	75
Maybe	50	Greenfield	25
No	25	Low	75
Single	75	Medium	50
Multiple	25	High	25

The above information provides all the necessary tools to calculate a user's **Process Fit Score**. The threshold value can be calculated using Equation 6 and the threshold values and importance weightings of Table 3.10. **The threshold value for the Process Fit Score is 57.72.** Thus, a score above the threshold score indicates that blockchain is a good fit for the process, while a score below the threshold score indicates that blockchain is not a good fit for the process.

With the calculation of the scores apparent, this element of the assessment framework is outlined in Figure 3.4 below. It can be seen in the figure that the scores can be plotted onto a graph that is split into four quadrants based on the threshold values. Scoring above both threshold values indicates that blockchain is fit for both the organization and the process. Scoring below both threshold values indicates that blockchain is fit for neither the organization nor the process. The remaining two quadrants represent a borderline case, where it is up to the user's discretion to determine whether continuing with blockchain experimentation is worthwhile. This decision might be based on how closely to the threshold value each score sits.

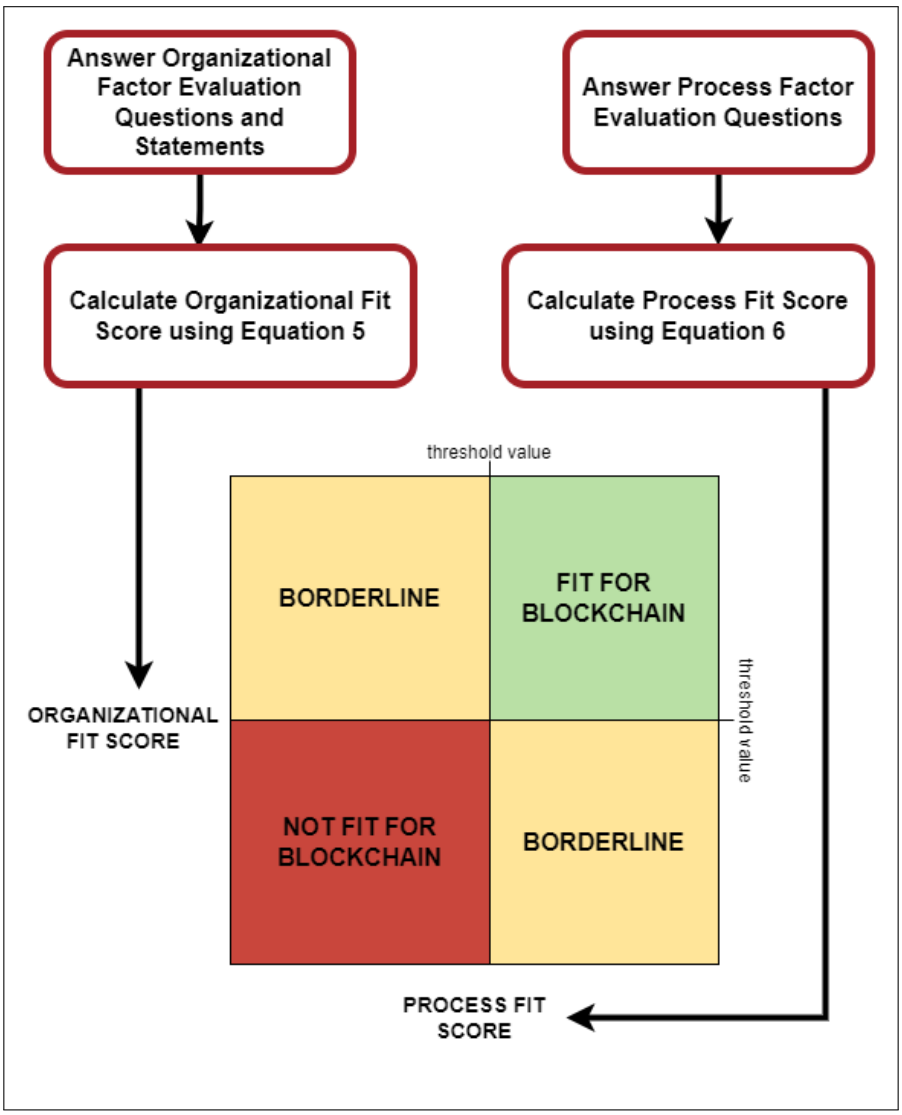


Figure 3.4: Blockchain Fit Analysis Process

3.2.2.3 High-Level Blockchain Design

This element of the blockchain assessment framework focuses on presenting a high-level blockchain design based on a specific use case and performance criteria preferences identified by the user. This element uses the theoretical background of Chapter 2 to provide insight, enabling the identification of different use cases, design features which present a choice to be made by the user, and how these design features affect certain performance criteria. This high-level design will be solely focused on the performance of the blockchain solution, where other aspects will be addressed in different analyses.

The design features can be identified by considering which features of blockchain in Chapter 2 present a choice to be made by the user and which of them will affect

performance of a blockchain solution. There are certain generic features of blockchain that might differ between blockchain solutions, but this difference will not create a great disparity in any notable performance criteria, such as the block structure. Contrastingly, there are certain features that will create a disparity in performance criteria, but these are either standardized or too nuanced to be addressed for individual use cases, and the selection of such a feature will typically be up to the discretion of the developer, such as cryptographic mechanisms. Then there are features that most definitely provide a choice to the user, but will not effect the performance of a blockchain solution but rather some other criteria, such as cloud-based versus server-based nodes which would affect cost.

The features that are left present a choice to be made by the user and each choice has different consequences on the performance of the solution. The first choice, and perhaps the most crucial, is that of the consensus mechanism. The literature review provided an in-depth comparison of the relevant consensus mechanisms in Section 2.1.5.6, which will provide a solid foundation from which to determine the different effects each consensus mechanism has on certain criteria. There are specific criteria pertaining to the consensus mechanisms which differentiate them from each other, these criteria can be drawn from the theoretical background and are presented and defined below.

1. ***Energy Efficiency*** – this refers to the ability of the solution to operate while producing minimal resource waste and cost.

2. ***Latency Performance*** – this refers to the amount of time it takes from the initiation of a transaction to the commitment of the transaction.

3. ***Throughput Performance*** – this refers to the amount of operations (read or write operations) that can be performed per a unit of time (usually seconds).

4. ***Hardware Dependence*** – this refers to the solution's dependence on hardware to be implemented and operate.

5. ***Centralization*** – this refers to the amount by which the implementation of a specific solution promotes centralization.

6. ***Scalability (validating nodes)*** – this refers to the ability of the solution to scale up the number of validating nodes in the network.

7. ***Scalability (client nodes)*** – this refers to the ability of the solution to scale up the number of client nodes in the network.

8. ***Security/Fault Tolerance*** – this refers to the solution's ability to handle faults or security breaches.

9. ***Settlement Finality*** – this refers to the finality of a transaction, which can either be deterministic (immediate) or probabilistic (not immediate/subject to change).

10. ***Incentivization*** – this refers to the ability of the solution to incentivize the validation mechanism.

Using the criteria identified above, the relevant blockchain consensus mechanisms can be compared to one another. The comparison of these consensus mechanisms according to the identified criteria is shown in Table 3.14 below.

Table 3.14: Consensus Mechanism Impact on Process Criteria

Process Criteria	PoW	PoS	DPoS	PoET	pBFT
Energy Efficiency	−−	+	+	++	++
Latency Performance	−	+	+	+	++
Throughput Performance	−	o	++	+	++
Hardware Dependence	++	+	o	++	o
Centralization	−−	o	+	o	+
Scalability (validating nodes)	+	++	+	++	−−
Scalability (client nodes)	+	++	++	++	++
Fault Tolerance	−	++	++	−	+
Settlement Finality	Prob	Prob	Prob	Prob	Det
Incentivization	Yes	Yes	Yes	Yes	No

++ = very high, + = high, o = average, − = low, −− = very low

This table enables a direct comparison of the relevant consensus mechanisms over a variety of process criteria. The next crucial choice to be made is that of blockchain type as addressed in Section 2.1.6. The process criteria which differentiate the blockchain types are drawn from the theoretical background and are presented below, but without the process criteria that has already been identified and defined above.

1. ***Organizational Control*** – this refers to the control that the organization which owns the solution will have over the solution and other network stakeholders.

2. ***Actor Identity (clients and validators)*** – this refers to the transparency of the identities of clients or validators to actors of the system.

3. ***External Transparency*** – this refers to the transparency of data to those not within the system.

4. ***Immutable*** – this refers to the inability of users of the solution to tamper with data on the system.

5. ***Data Accessibility (read and write)*** – this refers to the ability of the public to read or write data on the network.

6. ***Consensus Participation*** – this refers to the permissions of nodes able to participate in the consensus process.

Using the identified criteria above and extra criteria from the consensus mechanism comparison, the different blockchain types can be effectively compared against one another. The comparison of the different blockchain types is presented in Table 3.15 below.

Table 3.15: Blockchain Type Impact on Process Criteria

Process Criteria	Public Permissionless	Public Permissioned	Private Permissioned	Private Permissionless
Consensus Participation	Permissionless	Permissioned	Permissioned	Permissionless
Data Accessibility (read)	Public	Public	Private	Private
Data Accessibility (write)	Public	Public	Private	Private
Actor Identities (clients)	Unknown	Unknown	Known	Known
Actor Identities (validators)	Unknown	Known	Known	Unknown
Organizational Control	−−	−	+	o
External Transparency	++	++	−−	−
Latency and Transaction Speed	−	+	+	−
Scalability	−	+	+	−
Energy Efficiency	−	−	+	+
Immutable	++	++	+	+

++ = very high, + = high, o = average, − = low, −− = very low

This table enables a direct comparison of the different blockchain types over a variety of process criteria. These are the only two aspects identified in the literature review which will have an effect on the performance of a blockchain solution. Therefore, it is critical to select the right consensus mechanism and blockchain type because of the scarcity of design decisions at this stage.

The process criteria requirements for a user's specific use case can be assessed by using two values: the value requirement and an importance weighting. The value requirement is the value for a specific process criterion that the assessment framework user requires for their use case. This is either a value in the range 1 – 5 or a choice between two opposing options to correlate with the comparison tables above, where there are five values (––, –, o, +, ++) or two options for each process criteria. The importance weighting is simply a value in the range 0 – 1 to indicate the importance of the different process criteria relative to each other, where different ranges indicate different levels of importance. The range of importance weightings are shown in Table 3.16 below. On the next page, the different ranges and the associated scores used for each process criterion are presented in Table 3.17.

Table 3.16: Importance Answer Range

Range	Importance
0 – 0.25	Not Important
0.26 – 0.50	Mildly Important
0.51 – 0.75	Important
0.76 – 1.0	Very Important

Table 3.17: Process Criteria Ranges

Process Criteria	Value Range		
Energy Efficiency	1: minimal energy efficiency	2: low energy efficiency	3: average energy efficiency
	4: high energy efficiency	5: maximal energy efficiency	
Latency Performance	1: very high latency (>10000 ms)	2: high latency (10000-6000 ms)	3: average latency (6000-4000 ms)
	4: low latency (4000-1000 ms)	5: very low latency (<1000 ms)	
Throughput Performance	1: very low throughput (<100 tps)	2: low throughput (100-500 tps)	3: average throughput (500-1000 tps)
	4: high throughput (1000-2000 tps)	5: very high throughput (>2000 tps)	
Hardware Dependence	1: no dependence	2: slightly dependent	3: moderately dependent
	4: dependent	5: fully dependent	
Centralization	1: fully decentralized	2: minimally controlled decentralization	3: controlled decentralization
	4: highly controlled decentralization	5: fully centralized	
Scalability	1: not scalable	2: minimal scalability	3: average scalability
	4: high scalability	5: maximum scalability	
Security/ Fault Tolerance	1: not secure/fault tolerant	2: minimally secure/fault tolerant	3: moderately secure/fault tolerant
	4: highly secure/fault tolerant	5: maximally secure/fault tolerant	

Continued on next page

Continued from previous page

Process Criteria	Value Range		
Settlement Finality	2: probabilistic	4: deterministic	
Incentivization	2: yes	4: no	
Organizational Control	1: very low control	2: low control	3: average control
	4: high control	5: very high control	
Actor Identity	2: unknown	4: known	
External Transparency	1: no transparency	2: highly controlled transparency	3: moderately controlled transparency
	4: slightly controlled transparency	5: full transparency	
Immutable	1: fully mutable	2: highly controlled mutability	3: moderately controlled mutability
	4: slightly controlled mutability	5: fully immutable	
Data Accessibility	2: public	4: private	
Consensus Participation	2: permissionless	4: permissioned	

It should be noted that the process criteria which present two options, have those options scored with a '2' or '4' to ensure that they fall on either side of the mid-point at '3'. The user's preferences for each process criterion can now be represented as numerical values using Table 3.17, which is then ultimately used to compare the different design choices.

The high-level design step is further enhanced by utilizing use case selection to identify which process criteria should be prioritized. Typical blockchain use cases were captured effectively in Section 2.3 by the framework adapted from Carson *et al.* (2018) and backed up with the Assets, Trust, Ownership, Money, Identity, and Contracts (ATOMIC) concept by Mougayar (2016). Each use case presented will have particular process

criteria and process criteria values which are suited to them. Using the definitions of the process criteria and the definitions of the use cases identified, coupled with the theoretical background, the process criteria and their respective values are linked with the use cases in Table 3.18 below.

Table 3.18: Use Cases with Associated Process Criteria

Use Case	Linked Process Criteria (Value)	Reason
Static Registry	Throughput Performance (4)	Many read operations will be required during operation so that reference data may be retrieved without bottlenecking.
	Security/Fault Tolerance (4)	Reference data will need to be stored securely and one should trust the mechanism they are using to store their data.
	Actor Identity – clients (known)	It will be beneficial to know who the clients are to know what data to make available.
	Actor Identity – validators (known)	It will be beneficial to know who is validating the reference data to be able to react to mistakes and monitor behaviour.
	External Transparency (private)	It would be preferred to have the reference data transparent only to those with the necessary permissions.
	Immutable (4)	It is preferable to not be able to tamper with the reference data, or know when it has been tampered with.
	Data Accessibility – read (private)	The static register will better serve its purpose if it is known who has access to read the data.
	Data Accessibility – write (private)	The static register will be more useful if write operations are restricted to a particular group.
	Consensus Participation (permissioned)	Approving which nodes participate in the consensus mechanism will be vital for data integrity and easier to introduce repercussions for malpractice.

Continued on next page

Continued from previous page

Use Case	Linked Process Criteria (Value)	Reason
Identity	Throughput Performance (4)	Many read operations will be required during operation so that identity data may be retrieved without bottlenecking.
	Security/Fault Tolerance (4)	Identity data will need to be stored securely and one should trust the mechanism they are using to store their identity data.
	Actor Identity – clients (known)	The identity of clients is required to be able to store their respective identity data.
	Actor Identity – validators (known)	It will be beneficial to know who is validating the identity data to be able to react to mistakes and monitor behaviour.
	External Transparency (private)	It would be required to have identity data transparent only to those with the necessary permissions.
	Immutable (4)	It is preferable to not be able to tamper with identity data without prior knowledge and approval.
	Data Accessibility – read (private)	Identity data is often sensitive and it is thus required to know who has access to what information on the network.
	Data Accessibility – write (private)	The changing or updating of identity data should only be possible for a select group of writers.
	Consensus Participation (permissioned)	Approving which nodes participate in the consensus mechanism will be vital for identity data integrity and easier to introduce repercussions for malpractice.
Smart Contracts	Latency Performance (4)	Once conditions are met, the contract should execute as quickly as possible so that contractual agreements are not delayed.
	Throughput Performance (4)	Higher throughput will ensure the smart contracts are not backlogged in a queue when executing.
	Security/Fault Tolerance (4)	The ability to alter any data or smart contracts will greatly affect the integrity of the network.

Continued on next page

Continued from previous page

Use Case	Linked Process Criteria (Value)	Reason
Smart Contracts	Settlement Finality (deterministic)	Deterministic settlement finality will allow contract execution without the possibility of reversing transactions and creating confusion.
	Immutable (4)	Having immutability will ensure that the smart contracts that are executed cannot be reversed without knowledge and approval.
Dynamic Registry	Energy Efficiency (4)	With many transactions being processed, an energy efficient network will drive down costs for users.
	Latency Performance (4)	Executing transactions as quickly as possible will increase the value and usability of a dynamic register.
	Throughput Performance (4)	Having the ability to perform multiple transactions simultaneously will enable higher value by ensuring there are no long transaction queues.
	Scalability - client nodes (4)	It will be essential to be able to onboard clients as the system grows and more parties join.
	Security/Fault Tolerance (4)	Being able to ensure that data has not been tampered with and is protected is essential.
	Settlement Finality (deterministic)	Knowing that transactions are final once they have been validated will increase value and the flow of physical assets.
	Immutable (4)	Immutability will ensure that transactions are not reversed without knowledge or approval.
Payments Infrastructure	Energy Efficiency (4)	With a high throughput of transactions, high energy efficiency will allow transaction costs to be driven down.
	Latency Performance (4)	Ensuring a short time between transaction proposal and approval will increase value greatly.
	Throughput Performance (4)	Ensuring that thousands of transactions can be processed simultaneously is essential to a successful payments infrastructure.

Continued on next page

Continued from previous page

Use Case	Linked Process Criteria (Value)	Reason
Payments Infrastructure	Scalability - client nodes (4)	A payments infrastructure will require many clients on the system to be useful.
	Security/Fault Tolerance (4)	Transactions need to be secure and fault tolerant because of the amount of money that is tied in such a system.
	Settlement Finality (deterministic)	Once transactions have been approved, there cannot be any chance for the transaction to be undone due to forking or the like.
	Immutable (4)	Transactions should not be able to be reversed once processed without knowledge and approval.
	Data Accessibility - write (public)	Users of the network need to be able able to access it and transact for higher value through network effects.

While certain use cases are suited better with certain process criteria values, there is no reason they cannot be used with the opposite process criteria value (such as a payments infrastructure being better suited for a public environment, but nothing is preventing it from being successful in a private environment). For this reason, certain process criteria are omitted from use cases because of this behaviour duality. The "Other" use case is simply a combination of the five use cases and thus this use case will depend on the use cases it consists of.

To reflect the importance of the relevant process criteria for these particular use cases, the importance weighting assigned by the user should be multiplied by 1.2 if the user's process criterion value is equal to or greater than the value for the process criterion identified in Table 3.18, otherwise the importance rating should be multiplied by 0.8. If the process criteria is not linked with the particular use case, the importance rating remains untouched.

The preceding information enables the determination of two scores that are relevant to the user's particular use case: **Consensus Mechanism Score** and **Blockchain Type Score**. The determination and use of these scores is outlined in Figure 3.5 below and explained further thereafter.

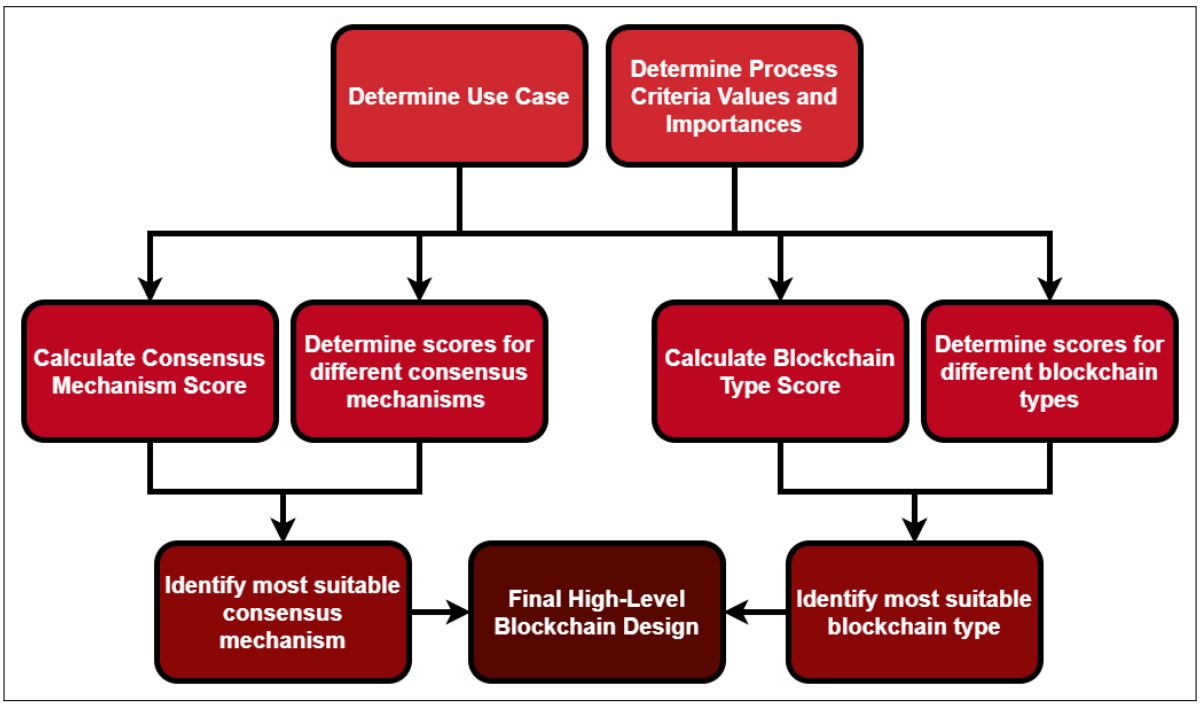


Figure 3.5: Blockchain High-Level Design Framework Component

The high-level blockchain design process begins with determining the use case relevant to the user, as well as the required process criteria values and their respective importance weightings. With these inputs, the **Consensus Mechanism Score** and **Blockchain Type Score** can be determined using the fuzzy weighted average method originally proposed by Dong & Wong (1987):

$$Score = \frac{\sum_{i=1}^{i=n} w_i \cdot x_i}{\sum_{i=1}^{i=n} w_i} \tag{7}$$

Where w_i are the adjusted importance weightings, x_i is the value of a particular process criterion, and n represents the number of process criteria being included. For the **Consensus Mechanism Score**, only the relevant process criteria identified in Table 3.14 are included in the above equation. Similarly, for the **Blockchain Type Score** only the relevant process criteria identified in Table 3.15 are included in the calculation. The adjusted importance weightings are calculated as follows:

$$w_i = \begin{cases} i_i \cdot 1.2 & \text{if criterion is relevant to use case and } \geq \text{ indicated value} \\ i_i \cdot 0.8 & \text{if criterion is relevant to use case and } < \text{ indicated value} \\ i_i \cdot 1.0 & \text{if criterion is not relevant to use case} \end{cases} \quad (8)$$

Where i_i is the original importance weighting identified by the user for each process criterion. With the **Consensus Mechanism Score** and **Blockchain Type Score** calculated, scores for each consensus mechanism and blockchain type are also determined. The scores are determined identically to the **Consensus Mechanism Score** and **Blockchain Type Score** by using the identified use case, the user's importance weightings and the values for each process criteria identified in Table 3.14 and Table 3.15, where the values are designated as: '−−' = 1, '−' = 2, 'o' = 3, '+' = 4, and '++' = 5. This allows scores to be calculated for each consensus mechanism option and each blockchain type option.

The **Consensus Mechanism Score** is then compared with the scores calculated for each consensus mechanism option and the most suitable consensus mechanism for the particular use case and process criteria preferences is the option which scores closest to the **Consensus Mechanism Score**. The **Blockchain Type Score** is used identically with the scores for the different blockchain types to identify which blockchain type is the most suitable for the particular use case. Ultimately, the output of this element is an indication of which consensus mechanism and blockchain type is most suited for the user's specific use case and process criteria preferences.

3.2.2.4 Blockchain Adoption Approach

This element of the blockchain assessment framework focuses on presenting the user with a high-level strategic approach to blockchain adoption, as well as a framework to identify adoption considerations for the user's use case. This element is built upon the theoretical background of Chapter 2, specifically Sections 2.1.2 and 2.5. This element provides two useful outcomes, which can be used in conjunction with one another to provide deeper insight into the adoption process and what can be expected during blockchain implementation.

The first outcome requires input from the user to identify the optimal strategic approach to blockchain adoption. This outcome is straightforward and based off of the framework presented by Carson *et al.* (2018). The user must simply determine their market dominance within their industry, as well as the standardization and regulatory barriers

that exist within their industry in order to identify the optimal strategic approach for their business context as explained in Section 2.5.3 and presented again in Figure 3.6 below.

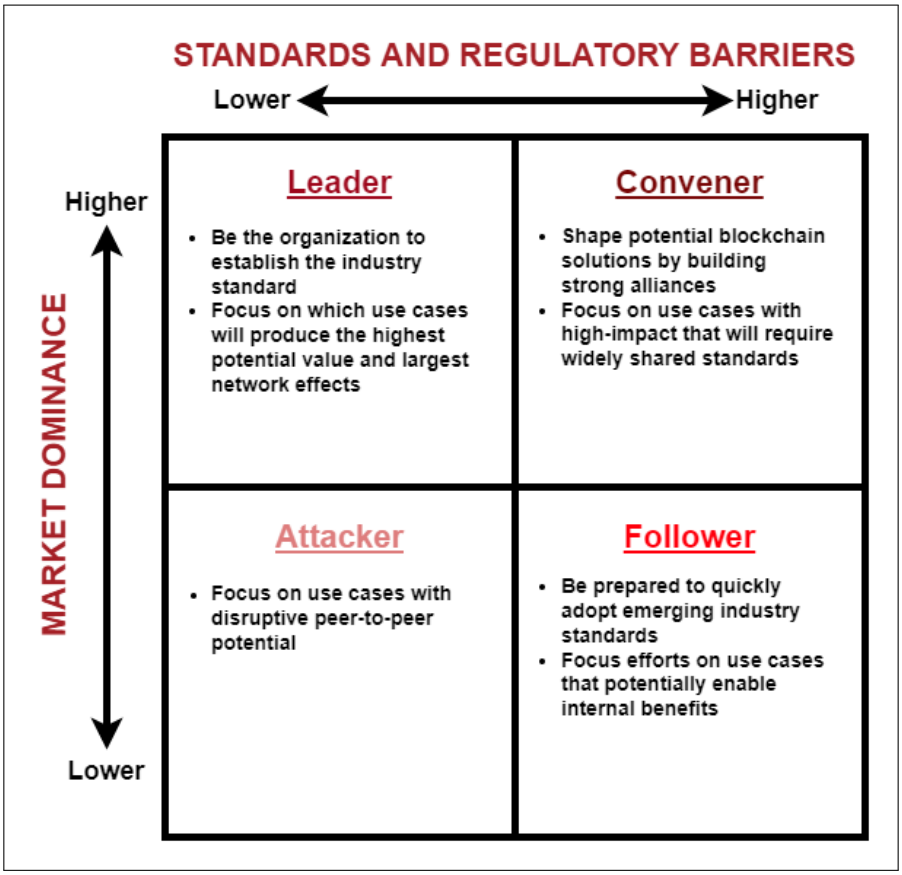


Figure 3.6: Optimal Strategic Approach for Blockchain Adoption (adapted from (Carson *et al.*, 2018)

The second outcome uses an adaptation of the GRAAL framework presented by Zarvić & Wieringa (2014) as outlined in Section 2.5.2. Superimposing blockchain's architecture onto the EA, as discussed in Section 2.1.2, enables an all encompassing architecture that accounts for both blockchain and the organization in which it operates. This conjoined architecure can be combined with blockchain's lifecycle stages, as identified in Section 2.5.1, to create the adapted GRAAL framework, similar to what Kharitonov (2017) presented. The framework is altered slightly to include an "Enterprise Environment" and "Foundation" layer as discussed in Section 2.5.2. This adoption considerations framework canvas can be seen in Figure 3.7 below.

	DISCOVERY	IMPLEMENTATION	OPERATION	DISPOSAL
ENTERPRISE ENVIRONMENT				
BUSINESS LAYER				
PROCESS LAYER				
APPLICATION LAYER				
BLOCKCHAIN LAYER (execution layer, consensus layer, network layer, data layer)				
HARDWARE LAYER				
FOUNDATION LAYER				

Figure 3.7: Adoption Consideration Framework Canvas

This framework canvas can be used individually by an organization to identify potential considerations, where each cell of the framework represents the context of a certain set of considerations which take place within a certain EA layer at a certain stage in a blockchain solution's lifecycle. The one exception to this is the "Foundations" layer which is relevant regardless of the EA layer or lifecycle phase. This framework canvas allows the organization to identify the considerations which are relevant to them and decide on a particular depth for each consideration, allowing it to be used in a variety of blockchain adoption settings.

However, it is noted that a completely blank canvas might be an intimidating prospect

for certain organizations to undertake and thus the adoption considerations identified in Section 2.5.2 are plotted on the framework canvas, with an attempt to keep the framework as generic as possible. This adoption considerations framework with the reference considerations is shown in Figure 3.8, where it should be noted that considerations may span multiple different cells and their meanings might differ slightly depending on the context of the cell.

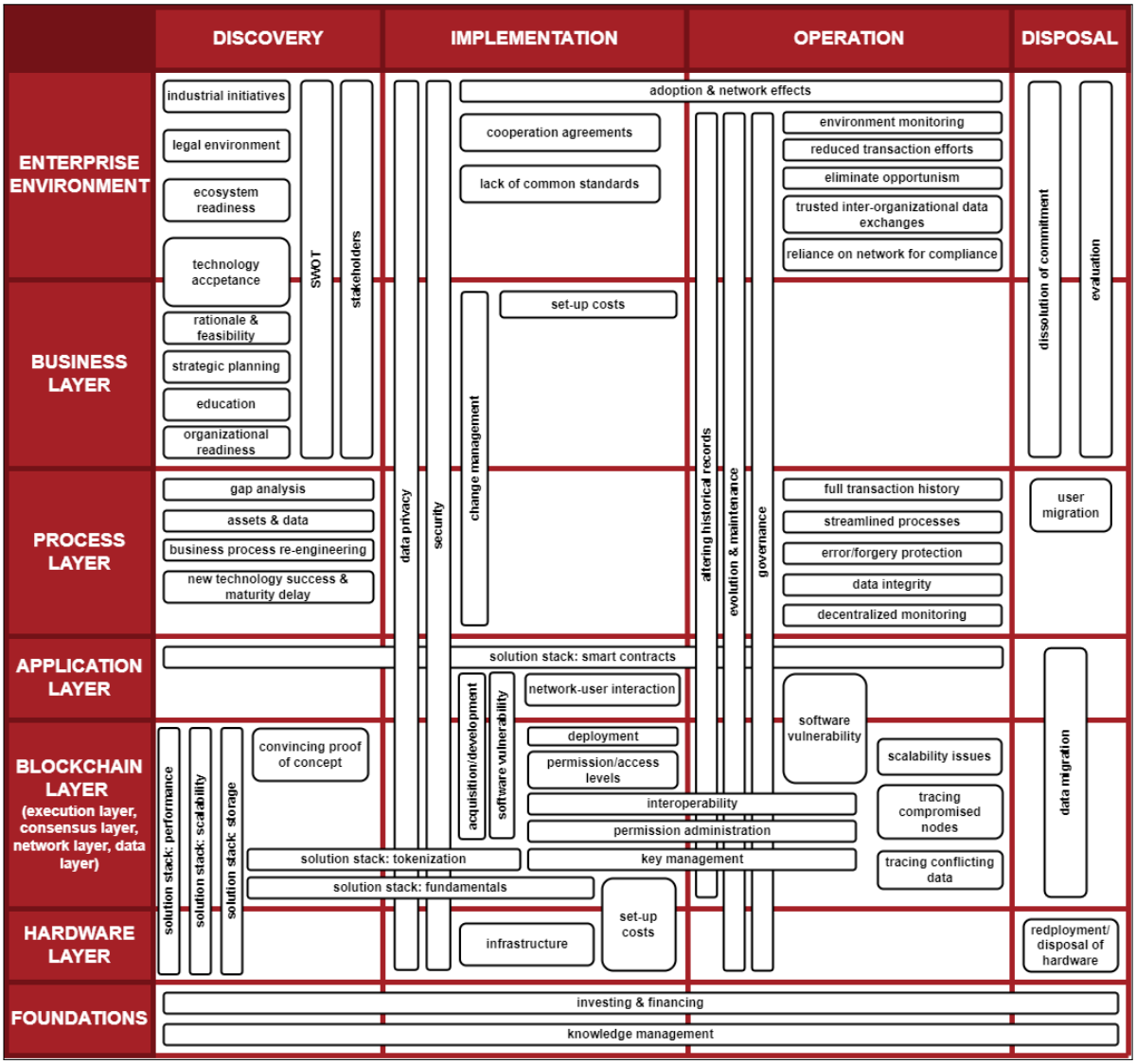


Figure 3.8: Reference Adoption Consideration Framework

This reference adoption considerations framework is simply an aid in identifying adoption considerations, where the use of it should be undertaken in two steps:

1. Select all relevant considerations from the framework, because the complete reference framework exceeds what an organization may potentially need to consider.

2. Add any relevant, unaccounted for considerations, as the reference framework does not present an exhaustive list of considerations and may lack certain elements, such as industry specific considerations.

Furthermore, while these considerations are divided into the different lifecycle stages, this does not imply they must only be addressed at the respective lifecycle stage, rather they must all be considered during the discovery stage so that the organization is prepared for any possible future trajectories of the blockchain solution. Note that the importance of these considerations will shift as the blockchain solution proceeds through its lifecycle.

This element of the blockchain assessment framework is more geared towards a thought experiment for the user of the tool, which enables contemplation on the many different aspects involved throughout the stages of a blockchain solution's lifecycle. It is less reliant on inputs from the user, but allows the determination of relevant considerations to be identified in a useful framework that can structure thoughts in a logical manner, allowing more constructive decisions to be made on blockchain implementation.

3.2.2.5 Blockchain Value Analysis

There are two areas in which analysing blockchain value will produce useful outcomes for an organization: performance and cost. This element of the blockchain assessment framework focuses on presenting a framework that can be used to identify costs, performance metrics, and process cost reductions. This element of the assessment framework builds upon the theoretical background of Chapter 2, specifically that of Section 2.6 and the *Hard Metrics* that were identified within the section.

Due to the scarcity of both performance and cost data on different blockchain solution configurations, the inclusion of a quantitative value analysis falls outside the scope of this study. Rather, this element of the assessment framework consists of a framework highlighting the value that a blockchain solution could potentially provide. It is then up to the user's discretion to determine what aspects of the framework are applicable to their use case. The framework is presented in Figure 3.9 on the next page.

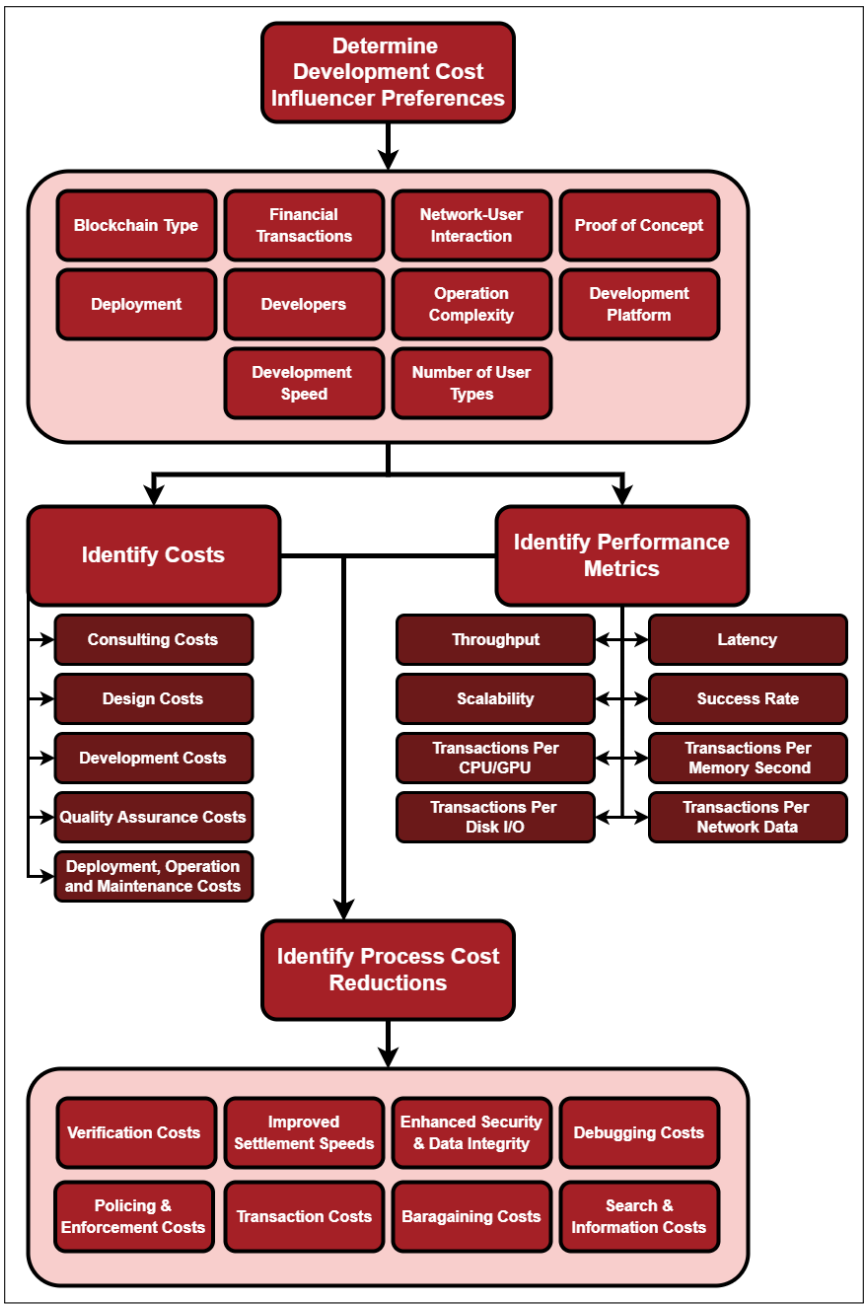


Figure 3.9: Value Analysis Framework

The framework proceeds in a linear manner to allow the user to logically connect how certain choices will affect specific outcomes. It begins by identifying preferences for certain development cost influencers, where the options are shown in Table 2.18. Based on these preferences, the insight from the adoption considerations, and the blockchain design from the design element of the framework, the costs associated with the specific use case can be identified according to the categories shown in the framework and the typical cost elements shown in Table 2.19. Average estimated costs can be found in

Appendix A.2 for certain cost elements, as well as for typical blockchain solutions, to give the user an indication of the range of costs that can be expected.

Furthermore, with the development preferences, the insight from the adoption considerations, and the blockchain design from the design element, relevant performance metrics can be identified which the user deems necessary for comparing blockchain solutions with one another, as well as with traditional solutions. Typical performance metric values for specific blockchain solution configurations is presented in Appendix A.1 to give the user an idea of the expected values a blockchain solution will output.

Finally, based on the costs of the blockchain solution and the relevant performance metrics, the user can then identify any process cost reductions that a blockchain solution may enable. While the framework does not provide an exhaustive list, it gives a good indication of where costs can be reduced by using a blockchain solution. Further explanations of these process cost reductions can be found in Table 2.20.

Again, this framework is merely to provoke deep contemplation on the different aspects involved in the cost and benefits of a particular blockchain solution, as opposed to providing tangible outcomes. Inputs to the framework are of lesser importance, the framework rather acts as a guideline to direct the thoughts of the user in a logical and structured way to identify the potential costs and benefits of a particular blockchain solution by indicating the link between certain choices and the outcomes they may affect.

3.3 Blockchain Assessment Framework

With all of the elements of the blockchain assessment framework, identified from Section 3.2.2, fully defined and completed, the blockchain assessment framework elements can be brought together into one cohesive framework, indicating the relationship between them and the logical flow of information and inputs required. The final assessment framework is presented in Figure 3.10 below, with initial iterations shown in Appendix B.1.

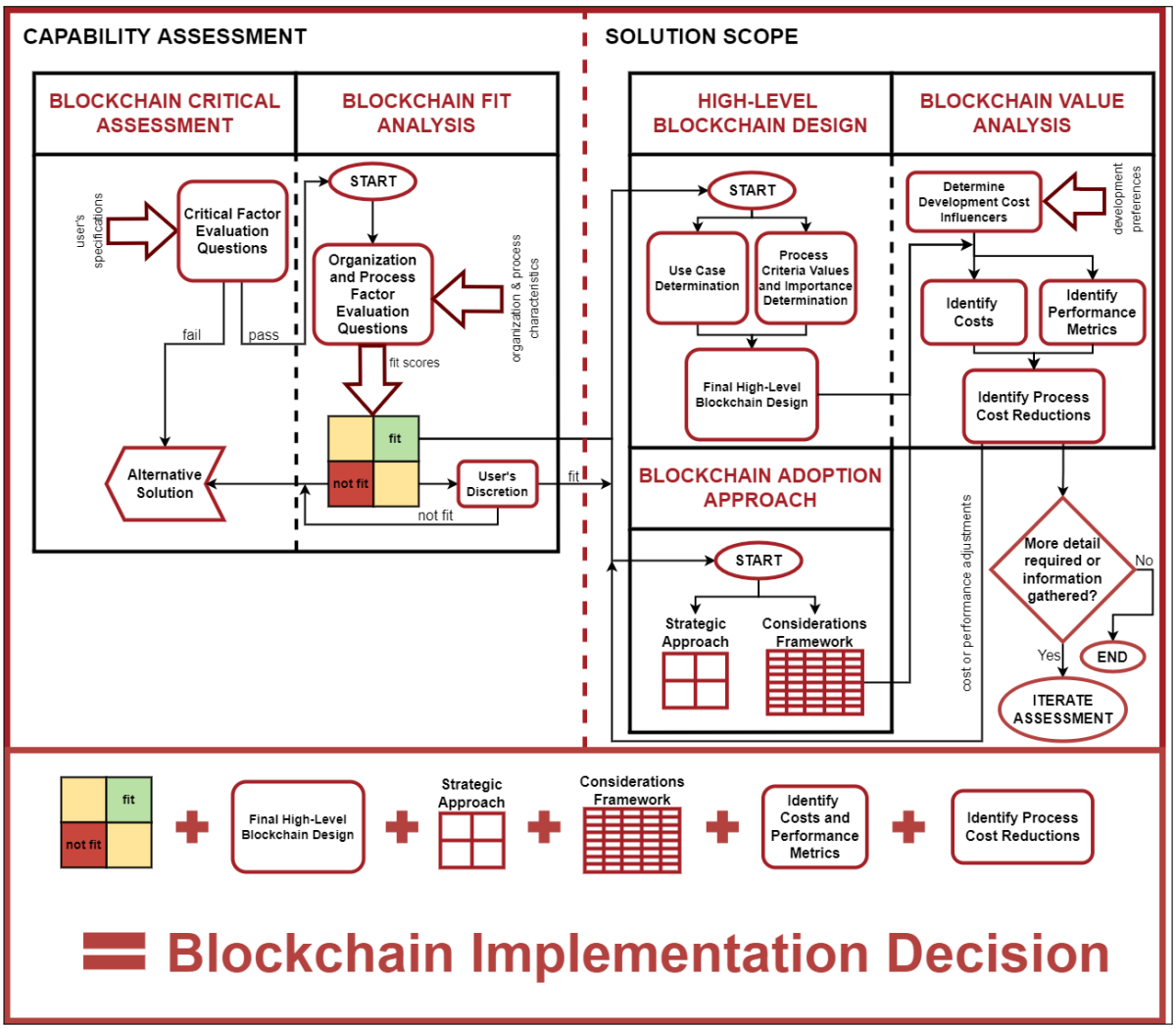


Figure 3.10: Blockchain Assessment Framework

This blockchain assessment framework exists to show how the elements are linked to one another and the logical order in which to complete each element. When completing a specific element, indicated in the boxes with red headings, one must refer to their relevant section in Chapter 3 above. The blockchain assessment framework is split into two main phases: "Capability Assessment" and "Solution Scope". The "Capability Assessment" phase consists of the "Blockchain Critical Assessment" and the "Blockchain Fit Analysis" and is focused on what blockchain is capable of providing an organization and whether it is relevant for an organization based on their needs and certain characteristics of their organization and the relevant process. The "Solution Scope" phase consists of the "High-Level Blockchain Design", "Blockchain Adoption Approach", and "Blockchain Value Analysis" and is focused on what an organization requires of a blockchain solution and the most optimal way to go about extracting what

is needed from this blockchain solution for the organization and its relevant process.

The first assessment to be completed is the "Blockchain Critical Assessment" of the "Capability Assessment" phase, which requires the user's specifications as an input and is completed according to Section 3.2.2.1. If the assessment is failed, an alternative solution is recommended, whereas if the test is passed, the user may continue with the second assessment of the framework, the "Blockchain Fit Analysis".

The "Blockchain Fit Analysis" requires the user to input the organization and process characteristics according to the steps defined in Section 3.2.2.2, allowing the user to determine their "Organizational Fit Score" and "Process Fit Score" and plotting them on the threshold graph to determine which quadrant they fall into. The bottom left quadrant indicates that blockchain is not fit for their organization and process and an alternative solution is recommended. The top left and bottom right quadrants indicate that either the organization or the process is not fit for blockchain and it is then up to the user to decide whether to continue with the analysis or opt for an alternative solution based on how close the fit scores are to the threshold values. The top right quadrant indicates that blockchain is fit for both the organization and the process and that the assessment can continue into the "Solution Scope" phase.

The "Capability Assessment" phase is now complete and the user will be aware of whether a blockchain solution is capable of providing the required specifications needed by their process within their organization. The "Solution Scope" phase will now provide a tailored solution and implementation approach optimized to their organization. This phase can begin with either the "High-Level Blockchain Design" or the "Blockchain Adoption Approach". The "High-Level Blockchain Design" requires the user to identify their general use case, as well as values for a range of process criteria and the importance of each of them according to the steps identified in Section 3.2.2.3. This element will provide the user with a high-level blockchain design that suits their needs.

The next element is the "Blockchain Adoption Approach" and while this element requires minimal input from the user, it provokes thought regarding important decisions during the solution's lifecycle. This element must be completed according to the process identified in Section 3.2.2.4 and its outputs are an optimal strategic approach to blockchain adoption, as well as a framework highlighting the considerations for blockchain adoption during its lifecycle and in each enterprise layer.

The final element to be completed in the first pass of the assessment framework is the "Blockchain Value Analysis", as presented in Section 3.2.2.5. This element begins with

the determination of different cost influencers by identifying the user's development preferences. Then using these cost influencers along with the high-level blockchain design and the adoption considerations framework, the user can identify which costs and performance metrics are relevant to their scenario and further use these to identify where blockchain can help reduce process costs.

Proceeding this step, the user can decide to iterate, beginning the "Capability Assessment" phase again if there are required cost or performance adjustments, making alterations to their preferences to affect the eventual outputs and consequently alter the cost or performance as required. Alternatively, the user may require more detail or they may have gathered extra information that can be used to more accurately complete the assessment, at which point they can decide to begin the entire assessment again to obtain more accurate representations of what can be expected of a blockchain solution within their organization. Lastly, the user can decide to end the assessment. At this point the true usefulness of the framework comes to light, whereby the user will use all of the gathered outputs in conjunction with one another to draw insight and ultimately make a decision on blockchain implementation within their organization.

3.4 Chapter Summary and Conclusion

This chapter explored the design of the blockchain assessment framework which was informed by the design requirements identified in Section 3.1. The design requirements were split into four categories to ensure no requirements were overlooked. This was followed by Section 3.2 in which the design methodology was explained and the elements of the blockchain assessment framework were designed. Five elements were designed in total: The Blockchain Critical Assessment, Blockchain Fit Analysis, High-Level Blockchain Design, Blockchain Adoption Approach, and Blockchain Value Analysis. These elements were combined into one cohesive framework in Section 3.3, which is the final blockchain assessment framework.

This chapter addressed many research questions: SO4.3, SO5.1, SO7.1, SO7.2, SO7.3, and SO7.4. The assessment framework needs to be demonstrated and validated to ensure that it produces the intended results. Chapter 4 focuses on addressing this demonstration and validation of the blockchain assessment framework.

4 SOLUTION DEMONSTRATION AND VALIDATION

The previous chapter focused on developing and explaining a blockchain assessment framework to assess the technical suitability, economical feasibility, high-level design, adoption approach and business value potential of a blockchain solution for a particular process within an organization. This chapter deals with the demonstration and validation of this framework and answers the research questions SO6.1, SO6.2, SO7.3, SO7.4, SO8.2, SO8.3, and SO8.4. The methods used to demonstrate and validate the blockchain assessment framework are briefly explained below.

1. **Demonstration:** Case Study
   - An enterprise asset management company (referred to as 'the company) provided a process they wished to investigate for blockchain implementation, along with the required inputs for the framework. This information was used to demonstrate the use of the blockchain assessment framework.
2. **Validation:** Expert Analysis
   - Two experts involved with the case study were presented with the outcomes of the assessment and a semi-structured interview was used to gain the experts' perspective on the rational and usefulness of the framework.

Both the case study and expert analysis provided insight and feedback that was used to enhance the design of the blockchain assessment framework. The iterative process used to validate the framework is shown in Figure 4.1 below.

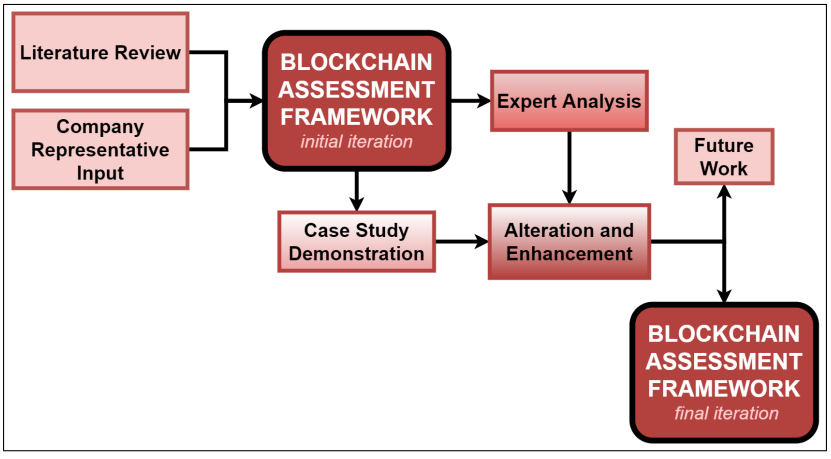


Figure 4.1: The Demonstration and Validation Process

The initial iteration of the blockchain assessment framework was developed using the work of the literature review in conjunction with input from the company's representatives. This iteration of the framework is demonstrated using the provided case study and analysed by experts for validation. The feedback from the demonstration and validation are then used to alter the framework to produce the final iteration. The demonstration and validation also provided insight on beneficial future work that could occur.

4.1 Hypothesis

It would be useful to revisit the problem statement identified in Chapter 1 and couple this with the research in Chapter 2 and the eventual solution created in Chapter 3, to derive a hypothesis for the outcome of the demonstration and validation of the blockchain assessment framework.

PROBLEM STATEMENT

Literature on the assessment of fundamental blockchain aspects within organizations – technical suitability, detail design, adoption approach, economical feasibility, business value potential – is scattered and often lacks either generality or thoroughness. Consequently, blockchain assessment is a tedious process and often yields subpar results.

This allows the hypothesis to then be stated based on what is expected of the blockchain assessment framework and what the design requirements intended of the solution and whether these were incorporated into the final design. After the validity of the framework has been investigated, the outcome can be checked to see if it supports the hypothesis and consequently, whether the framework accomplishes what it is intended to.

HYPOTHESIS

A comprehensive and generic blockchain assessment framework can be designed to help aid decision makers regarding blockchain exploration and implementation within an organization.

4.2 Demonstration

The following section is focused on using a case study to demonstrate the use of the blockchain assessment framework. The intention is to both gain insight on possible improvements and to showcase the use of the framework and the thought that goes along with it. The section begins with an overview of the case study and then goes on to generate results by demonstrating the use of the assessment framework and ultimately ends with a conclusion of what the assessment framework was able to accomplish.

4.2.1 Case Study Overview

The organization on which the case study is being performed has requested to remain anonymous in this study and shall thus simply be referred to as 'the company' throughout. The company is a multinational business focused on developing, delivering and maintaining EAM solutions. EAM can be seen as utilizing a combination of services, software, and systems to control and maintain operational assets, in turn optimizing the quality and utilization of these assets throughout their lifecycle, increasing uptime and decreasing operational costs (IBM, 2022).

The company provides services to allow their clients to move from a reactive state to a proactive state, where asset availability is optimised. They understand that there is no best solution and that each scenario requires a customised asset management strategy, based on the services they provide, to increase asset performance while minimizing costs and risks. Based on an assessment of the client, the company is able to identify the exact EAM road map required. The full EAM road map, along with the company's services offered, is shown in Figure 4.2.

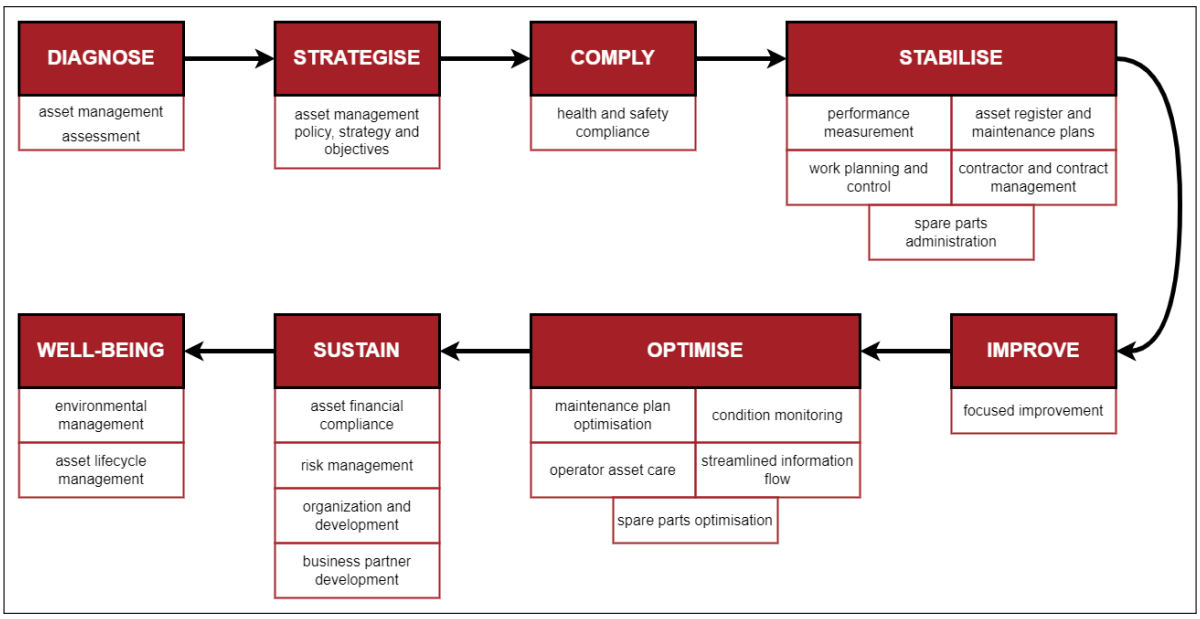


Figure 4.2: The Company EAM Services Road Map

The company uses their skills and expertise to offer services in a wide variety of asset intensive industries, including manufacturing, original equipment manufacturers, facilities and retail, mining and minerals, oil and gas, and public infrastructure. The company offers a return on their client's investment in three areas: improved asset performance, cost reduction and risk reduction.

IMPROVED ASSET PERFORMANCE	COST REDUCTION	RISK REDUCTION
• Increased availability • Improved reliability • Consistent service delivery • Sustainable quality • Maximum asset utilisation	• Improved labour utilisation • Optimised stock levels • Effective contractor management • Accurate repair or replace decision making	• Compliance with legislation • Health, safety, security and environment requirements • Reduce breakdowns to minimise business risks

Figure 4.3: The Company Return on Asset Investment

The company offers a range of EAM software solutions, known as an Enterprise Asset Management System (EAMS), allowing clients to effectively manage their assets, people and resources by configuring systems specific to a given scenario that enable streamlining asset management tasks and allow clients to access necessary information to support their

organization's strategy. The company is interested in investigating the applicability and benefits of implementing a blockchain solution as the basis of an EAMS.

The process the company selected to investigate is the flow of work orders and invoices between the company and a client. A high-level overview of this process can be seen in Figure 4.4. It must be realized that in the process shown, a client identifies the problem with an asset but this may also be scheduled maintenance, which will follow a similar flow except for the initiation of the work order.

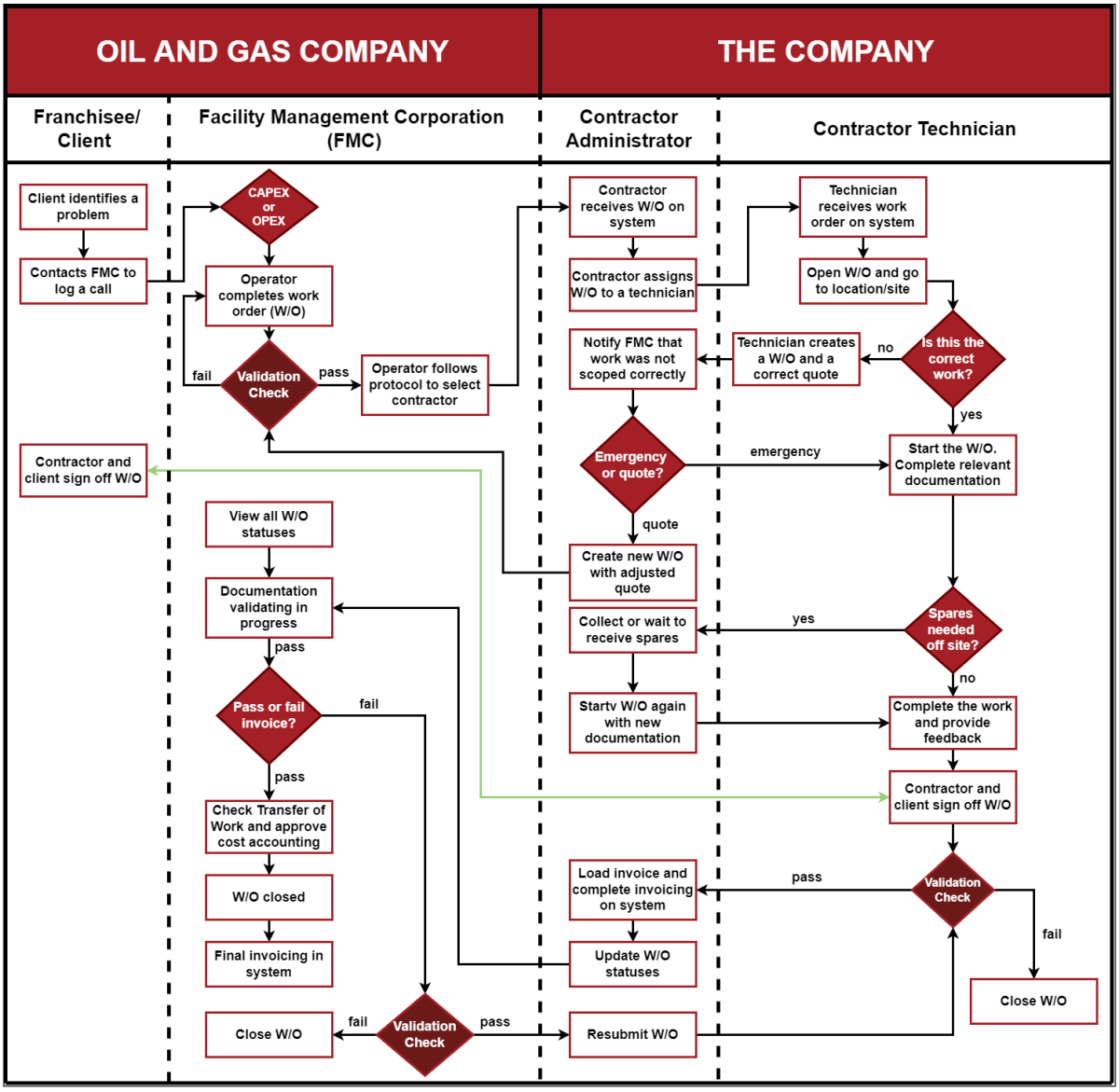


Figure 4.4: The Company Process

It can be seen from Figure 4.4 that there can be up to four actors in the system: the franchisee/client, the Facility Management Corporation (FMC), the contractor administrator, and the contractor technician. The franchisee/client and the FMC may be the same entity and similarly, the contractor administrator and technician could be the same entity. Regardless of the scenario, there is information exchange between multiple, distributed stakeholders. Furthermore, there are a number of validation checks throughout the process, which form a large part of the company's interest in a blockchain solution and its ability to implement smart contracts to automate these checks. Proceeding this section is the demonstration of the blockchain assessment framework for this process and organization.

4.2.2 Case Study Demonstration

The information of the previous section, along with the framework inputs received from the company's divisional manager and head of product development, enables the completion of the blockchain assessment framework. Regardless of the outcome of each step, the assessment will continue with the proceeding element to demonstrate the use of the blockchain assessment framework. The assessment begins with the "Capability Assessment" phase and more specifically the "Blockchain Critical Assessment".

Blockchain Critical Assessment

The company inputs for this element of the blockchain assessment framework are presented in Appendix C.1, which is simply the yes/no answers to the critical factor evaluation questions. Based on these inputs, the critical assessment may begin. The first three critical factors are satisfied for the company's process and thus the assessment may continue with the main collection of critical factors. For the company's process and their organization, there are seven critical factor evaluation questions answered in the affirmative, excluding the first three, and thus blockchain is applicable for this process because more than 6 critical factors are satisfied from the main collection. The critical factors which were satisfied are indicated in green in Figure 4.5. With this outcome, the assessment may proceed to the second element of the "Capability Assessment" phase: the "Blockchain Fit Analysis".

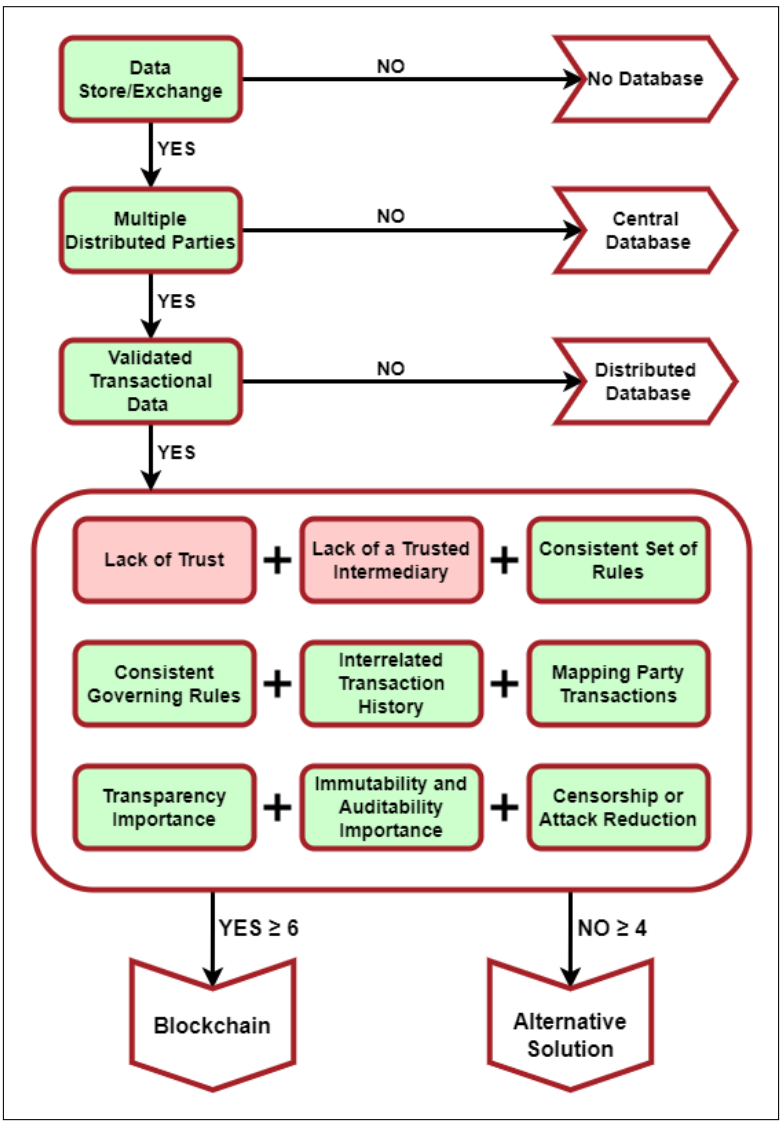


Figure 4.5: Blockchain Critical Assessment Satisfied Factors

Blockchain Fit Analysis

The company inputs for this element of the blockchain assessment framework are presented in Appendix C.2, which is simply the answers to each organizational and process factor evaluation questions and statements. Based on these inputs, the fit analysis may begin. Firstly, the "Organizational Fit Score" is calculated based on the characteristics of the company's organization. The "Organizational Fit Score" has a threshold value of 54.30 as identified in Section 3.2.2.2. Using the company's inputs from Table C.2 and converting all answers to numerical values using Table 3.9, Equation 5 may now be used in conjunction with the importance weightings from Table 3.6 to calculate the company's "Organizational Fit Score". The company achieves an "Organizational

Fit Score" of 62.76.

Secondly, the "Process Fit Score" may now be calculated based on the company's selected process' characteristics. As identified in Section 3.2.2.2, the "Process Fit Score" threshold value is 57.72. Using the company's inputs as presented in Table C.3 and converting all answers to numerical values using Table 3.13, Equation 6 can be used in conjunction with the importance weightings from Table 3.10 to calculate the company's "Process Fit Score". The company achieves a "Process Fit Score" of 60.47.

These fit scores can now be plotted onto a simple graph to indicate the company's blockchain fit, as indicated in Figure 3.4. The specific graph for the company is presented in Figure 4.6 below. It can be noted that the company's final fit scores place them in the top right quadrant, indicating that their organization and process are both fit for blockchain. However, it should be noted that the the "Process Fit Score" is only marginally over the threshold value of 57.72 and thus caution should be exercised should the company decide to implement blockchain and deeper analyses should be conducted. Regardless, the output indicates that blockchain is fit and thus the assessment may continue into the "Solution Scope" phase, beginning with the "High-Level Blockchain Design".

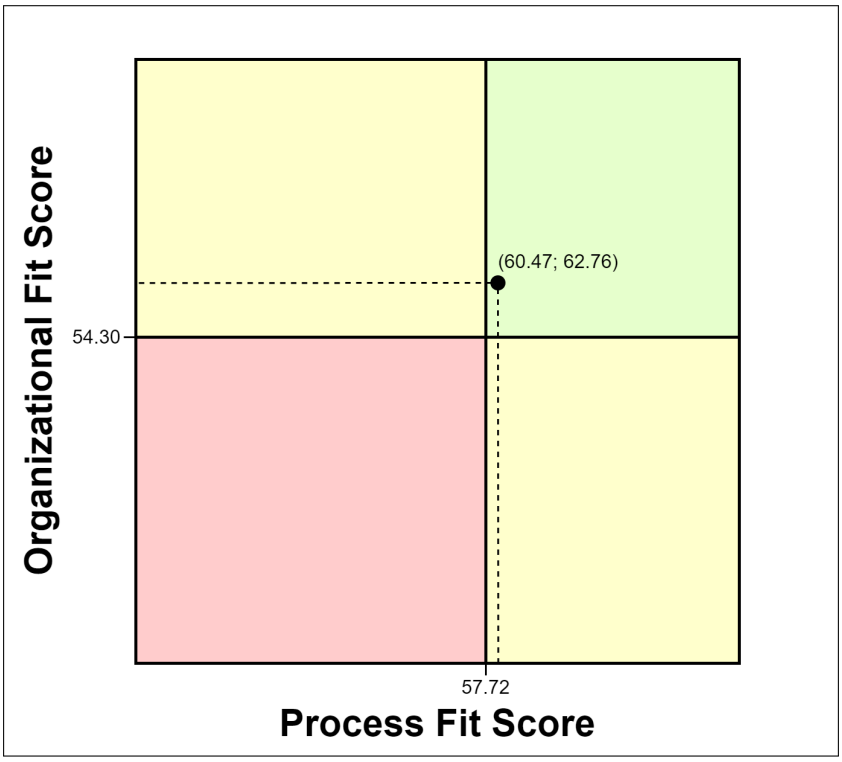


Figure 4.6: Blockchain Fit Analysis Output

High-Level Blockchain Design

The company's inputs for this element of the blockchain assessment framework are presented in Appendix C.3. The inputs required for this step, as shown in Table C.4, are simply requirements for the different process criteria identified in Section 3.2.2.3 and an importance weighting for each of the process criterion.

Using the importance weightings assigned to each process criterion by the company, scores can be calculated for each consensus mechanism based on the criteria relevant to them and each options performance in each of those relevant criteria as identified in Table 3.14. The importance weightings are first adjusted according to Equation 8, using Table 3.18 to identify the process criteria associated with the identified use case (Smart Contracts). It should be noted that the importance weightings for each consensus mechanism will then differ based on their performance ratings. Values can then be assigned to the performance ratings, as stated in the second last paragraph of Section 3.2.2.3. Finally, Equation 7 can be used to calculate the scores for each consensus mechanism, noting that the sum of the weightings is the sum of the adjusted importance weightings for each consensus mechanism. Similarly, using the company's inputs for their required performance of each process criterion and the importance weighting of each process criterion, a score can be calculated identifying the company's ideal consensus mechanism solution. The scores for each consensus mechanism and the ideal solution are shown in Table 4.1 below.

Table 4.1: Blockchain High-Level Design Consensus Mechanism Scores

Consensus Mechanism	Score	Distance to Ideal
Proof-of-Work	2.52	1.49
Proof-of-Stake	3.82	0.19
Delegated-Proof-of-Stake	4	0.01
Proof-of-Elapsed-Time	3.71	0.3
Practical Byzantine Fault Tolerance	4.07	0.06
Ideal Solution	4.01	0

Again, using the importance weightings assigned to each process criteria by the company, scores can be calculated for each blockchain type based on the process criteria relevant to them and each options performance in each of those relevant process criteria as

identified in Table 3.15. The assigned importance weightings are first adjusted according to Equation 8, using Table 3.18 to identify the process criteria associated with the identified use case (Smart Contracts). Now, the importance weightings for the different blockchain types will differ based on their performance in the respective process criteria. Values are assigned to the performance ratings, as stated in the second last paragraph of Section 3.2.2.3. Lastly, Equation 7 can be used to calculate the scores for each blockchain type. Similarly, the company's inputs for their required performance of each process criterion and the importance weighting of each process criterion can be used to calculate the score for the company's ideal blockchain type solution. The scores for each blockchain type and the ideal solution are shown in Table 4.2 below.

Table 4.2: Blockchain High-Level Design Blockchain Type Scores

Blockchain Type	Score	Distance to Ideal
Public Permissionless	2.59	1.1
Public Permissioned	3.37	0.32
Private Permissioned	3.70	0.01
Private Permissionless	3.05	0.64
Ideal Solution	3.69	0

The results from Table 4.1 and Table 4.2 indicate the best available solutions for the consensus mechanism and blockchain type. A private permissioned blockchain using DPoS is suggested based on the company's process criteria preferences. With these design parameters determined, the blockchain assessment may continue with the "Blockchain Adoption Approach".

Blockchain Adoption Approach

Due to this element of the framework and the proceeding element, "Blockchain Value Analysis", being conceptual elements, they rely on similar inputs to allow conceptualization of the relevant process and the subsequent completion of the relevant element. Thus, the inputs for this element, as well as the next, are jointly presented in Appendix C.4. While these inputs are not explicitly required from the user for these steps, they have been included to provide context of the process and allow the study to make meaningful deductions for the final two elements of the assessment framework.

The first step of this element allows the optimal strategic approach for blockchain adoption to be identified according to Figure 3.6. The identified strategic approach

according to the company's inputs is highlighted in green in Figure 4.7 below.

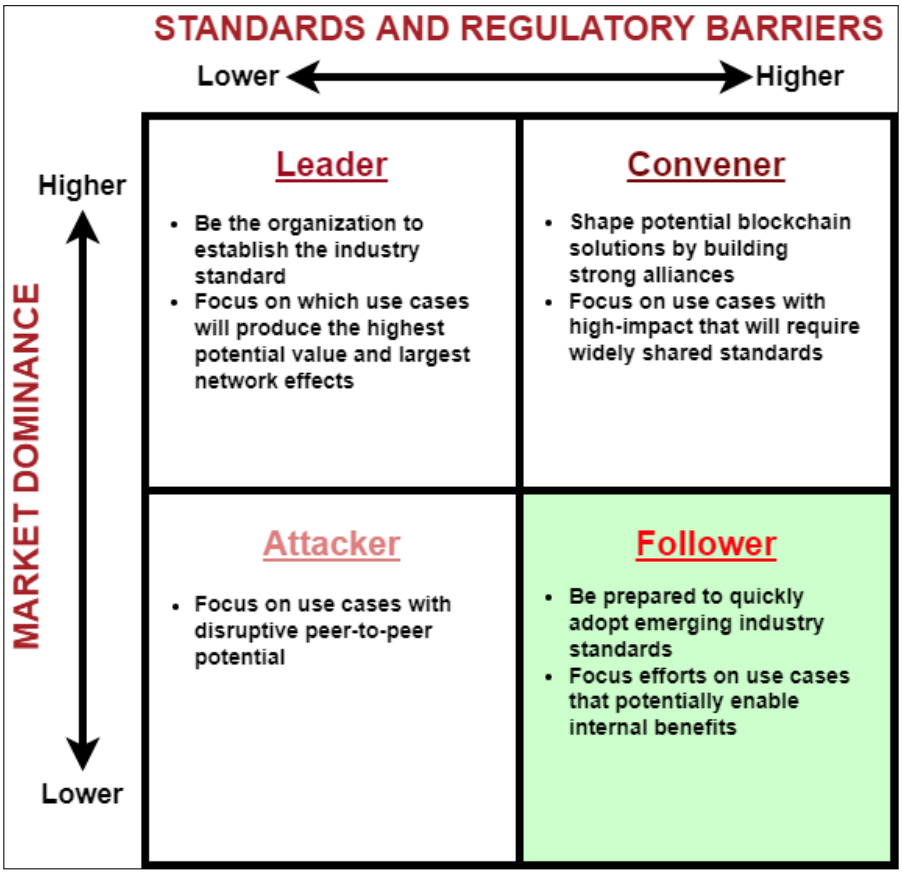


Figure 4.7: The Company's Optimal Blockchain Adoption Strategy

The final step of this element is using the framework presented in Figure 3.7 to identify the relevant consideration during the blockchain solution's lifecycle and in each enterprise layer. Due to the lack of knowledge on the process and organization, the reference framework from Figure 3.8 will be adopted and adjusted where possible to more closely fit the company's specific use case. Figure 4.8 presents the adjusted framework, with green considerations indicating high importance, red indicating low importance and yellow indicating a middle ground between the two.

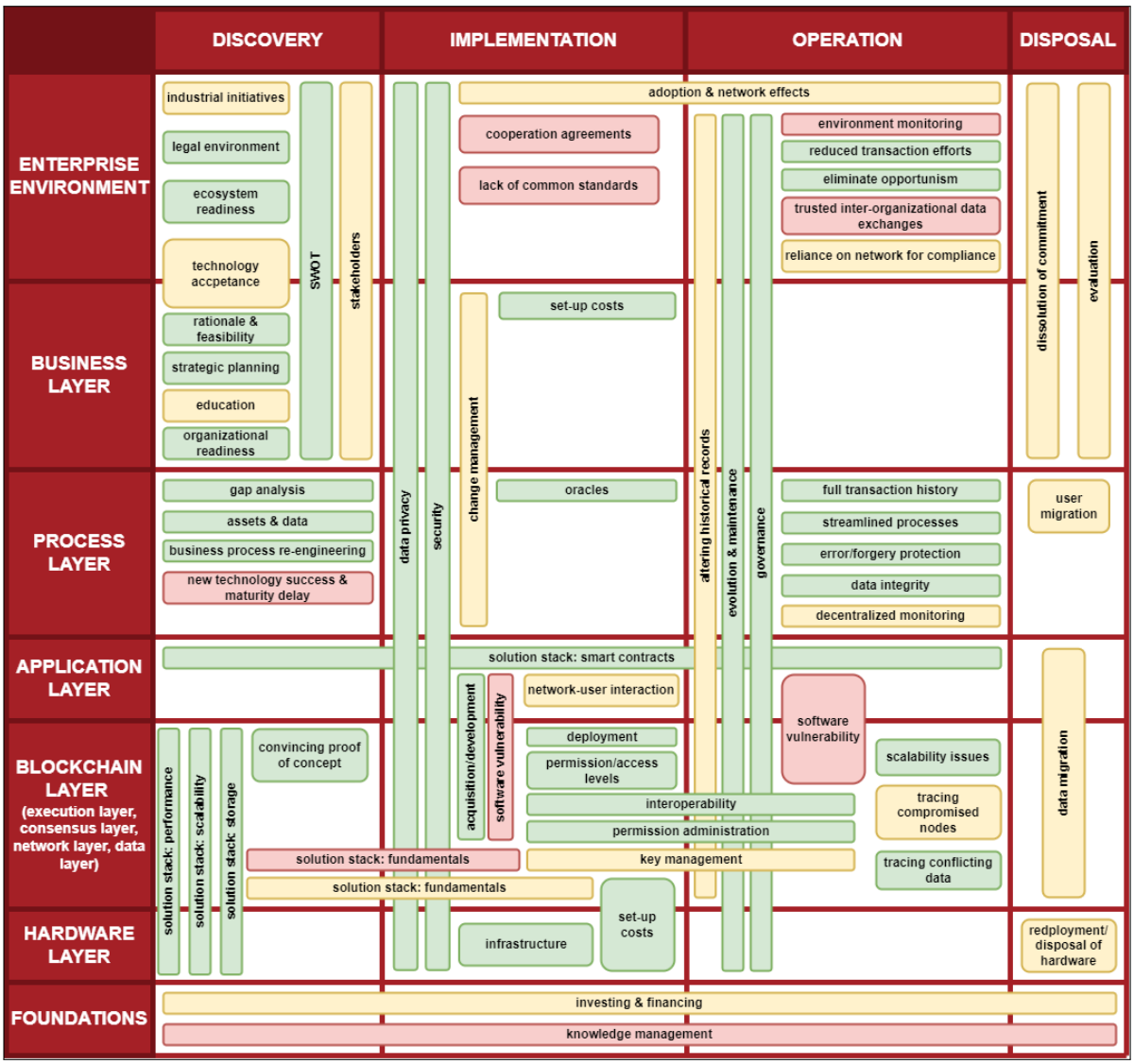


Figure 4.8: The Company's Blockchain Adoption Consideration Framework

Finally, with the inputs and outputs from the first two elements of the "Solution Scope" phase obtained, the final element may be undertaken. The "Blockchain Value Analysis" relies on the outputs of these first two elements to conceptualize the cost and performance metrics of a blockchain solution more effectively.

Blockchain Value Analysis

Similarly to the previous element, this element does not rely on explicit inputs, but rather on the knowledge and experience of the user. Due to limited time with the company's representatives, the inputs presented in Appendix C.4 are used to complete this element of the assessment framework. The cost influencer choices presented in Table C.5 are used in conjunction with the outputs of the "High-Level Blockchain Design" and

"Blockchain Adoption Approach" elements so that the costs during the different phases of blockchain implementation may be identified with more certainty. These costs are presented in Table 4.3 below, along with the relevant implementation phase.

Table 4.3: Blockchain Value Analysis Relevant Cost Elements

Blockchain Implementation Phase	Relevant Cost Element
Consulting Phase	Consultant fees
Design Phase	White paper cost
	Prototype development
Development Phase	Agency development fees
	Smart contract creation and implementation
	Mobile application development
	Website interface development
Quality Assurance	Cybersecurity
	Legal costs
	Agency quality assurance costs
Deployment, Operation and Maintenance	Third-party cloud node hosting costs
	System migration
	Maintenance and upgrading
	Continuous integration
	Storage costs
	Energy costs
	Infrastructure
	Project management

Furthermore, using the inputs of Appendix C.4, the relevant performance metrics can be identified. These performance metrics, along with their required values, if any, are presented in Table 4.4 below.

Table 4.4: Blockchain Value Analysis Relevant Performance Metrics

Relevant Performance Metric	Required Value
Throughput	N/A
Latency	<500 ms
Scalability	1500 users

These performance metrics place constraints on the solution scope and make it easier to identify a relevant blockchain solution. Finally, the identified costs and performance metrics can be used to identify potential cost reductions for the specific process. These potential cost reductions are listed below.

- Verification costs
- Improved settlement speeds
- Enhanced security and data integrity
- Policing and enforcement costs
- Transaction costs
- Bargaining costs
- Search and information costs
- Debugging costs
- Automation
- Networking costs

All of these items provide a potential way in which a blockchain solution may reduce costs for the company. With the outputs of the "Solution Scope" phase complete, any required performance or cost adjustments can be introduced by beginning the phase again and being aware of any criteria that will affect the required metric wanting to be altered. With all the outcomes of each element of the assessment framework completed, the assessment may finish with a final conclusion based on these obtained outcomes.

4.2.3 Case Study Conclusion

While each element provides an outcome that in itself provides valuable information, the true value of the blockchain assessment framework comes from using the outcomes in conjunction with one another to truly assess the value and feasibility of a blockchain solution. The "Blockchain Critical Assessment" indicates that a blockchain solution is definitely applicable in the company's specific case, with only two factors not satisfied. The reason being is that the company is the intermediary and prides itself in being a trusted facilitator of asset management, thereby creating an environment in which there is trust between parties. This does not mean that a blockchain solution is not useful, it rather indicates that there are certain functionalities of a blockchain solution that will not be used, which in this case is it's ability to create trust in a trustless environment. As long as there are other functionalities that a blockchain solution provides that may not be provided by an alternative solution, a blockchain solution can still be a good investment.

Thus, the assessment continues with the "Blockchain Fit Analysis". While the company scored higher than the threshold value for both fit scores, the scores are not exactly remarkable and thus the company finds themselves just within the top right quadrant of the fit analysis graph. The "Organizational Fit Score" is promising and indicates that the organization is just about ready for blockchain adoptions, but education could go a long way in informing potential users of the use of blockchain and its many potential benefits and fostering competency among these potential users. Furthermore, simplifying certain operations to reduce the different kinds of data that are transferred between systems would greatly increase blockchain's suitability.

The "Process Fit Score" is more marginal and while it is indicating that blockchain is a good fit for the company's process, caution should be exercised and the process should constantly be evaluated once more information is known on a potential blockchain solution's implementation to ensure that the process remains suitable. Once again, simplifying the process by standardizing interfaces for different users, reducing the number of data formats, and reducing the number of different processes using the same data or incorporating processes to rely on one distributed system will increase the suitability of blockchain for this process, as well as navigating the regulatory environment well or waiting for another organization to lead the way to determine the best approach. Regardless of the improvements that can be made, blockchain is still a plausible solution for this organization and its specific process and thus a high-level blockchain solution can be designed.

Analysing the scores of each consensus mechanism and the ideal solution's score from the "High-Level Blockchain Design", there are two consensus mechanisms that stand out: Delegated-Proof-of-Stake and Practical Byzantine Fault Tolerance. While DPoS scores closer to the ideal, either solution would provide the needed requirements. There are many factors that may influence this decision and research into each consensus mechanism would be beneficial. For example, DPoS requires the staking of tokens and thus the blockchain solution will have to be developed with this in mind, and determining who then gets these tokens and how much they will get may introduce complexities that the company is not interested in. Furthermore, pBFT is used with some common development platforms, such as Hyperledger Fabric, and thus considering that the company is planning on using a development platform, pBFT may be the more obvious choice. However, DPoS can be used to foster a more decentralized environment by giving all users a say in how the blockchain solution is run by staking their assigned coins. This clearly indicates that while the blockchain assessment framework recommends DPoS over pBFT, the assessment does not contain an exhaustive list of factors and thus the scores should only be used as a guideline to help the company narrow their choices, where the final choice is ultimately their own.

The second and final output of the "High-Level Blockchain Design" is the blockchain type. This selection is more straightforward and indicates that a private permissioned blockchain is the best blockchain type to implement. This choice lines up well with the company's preferences of wanting to select the validators and permit who may transact and view the blockchain solution's history. None of the other options would be as suitable and this is reflected in their scores.

With a high-level design in mind, more conceptual assessments may begin. Firstly, the "Blockchain Adoption Approach" recommends that the company takes a follower role by allowing industry standards to first be established, but being prepared to swiftly adopt a blockchain solution if the time is right. This recommendation is based on the company's market position and the barriers present due to regulations and standards. The last outcome of this element is the considerations framework. No extra considerations were added or removed from the reference considerations framework presented in Section 3.2.2.4, but the considerations were ranked by importance, with green indicating high importance, red indicating low importance and yellow being the middle ground between the two. The high importance items are focused on considerations that will indicate whether the blockchain solution will be capable of providing certain functionality that the process will require and how these functionalities will be incorporated and the potential

benefits that a blockchain solution will introduce during operation. The yellow items are more secondary considerations that will eventually need to be properly considered but they may not be at the forefront of the company's interest at this stage because they are not directly related with what blockchain provides. The red items are the considerations that cannot be heavily influenced and are thus just considerations to be aware of rather than acting upon them at this stage. As the company's journey with blockchain progresses, the importance of these considerations will shift and items that are high importance now can either be completed or not so important later and lower importance items will become more important as the finer details are planned and implemented.

The final element, the "Blockchain Value Analysis", allows the user to conceptualize the type of costs that will be implemented during the implementation of blockchain. Using the quoting system provided by Leewayhertz (2019) and the company's development preferences identified in Appendix C.4, different estimations for a small scale blockchain solution for one process can be made below.

- Development Time: approximately 23 weeks
- Development Cost: R1 332 000 - R2 094 000
- Consulting and Design Costs: R145 000 - R160 000
- Monthly Cloud Costs: approximately R28 500

Furthermore, it can be seen from Appendix A.1 that a permissioned blockchain using pBFT can operate with 100 000 users at 0.16s latency and 200tps, well above what is required by the company. Due to the lack of sources available, DPoS performance is more difficult to quantify. However, it should be noted that the performance of a particular solution may vary wildly depending on its specific configuration. Regardless, it is clear that a solution which meets the company's requirements is possible and further research into the exact cost reductions that can be expected, as well as their values, will allow the company to accurately decide whether blockchain is a wise investment that can yield returns against their current solution. It can be noted that most cost reductions are brought about through time reductions and thus determining the time of certain processes with and without a blockchain solution will be imperative in reaching a decision.

The blockchain assessment framework has indicated that blockchain is a plausible solution. The company may now either break their role as follower and attempt to

create a disruptive use case for blockchain in their industry or wait for blockchain to gain more traction and standards and then implement it. Regardless of the approach taken, the company will need to put in a lot more time in determining the exact solution they will require and the exact gains that can be expected, the approach will just dictate the urgency with which this should be done. Remaining a follower will mean that a more relaxed approach can be adopted and there is no rush to analyse blockchain further, while the opposite is true if the company decides to break their follower role.

4.3 Validation

The following section is focused on validating the blockchain assessment framework through the use of expert analyses. The section begins by explaining the method being used, followed by the feedback that was received. The section ends with the insights that are drawn from the feedback received.

4.3.1 Validation Method

Considering that this study is design-oriented research focused on the initial design of a blockchain assessment framework, it is crucial to validate the framework by ensuring that the design requirements of Section 3.1 were met during the design phase, with the ultimate aim of accepting the hypothesis presented in Section 4.1. The outcome of this study is validated using the case study of Section 3.2 in conjunction with an expert analysis.

The company's representatives have been involved in this study since before the design phase began, providing input on what a successful assessment framework would incorporate into its design. Using these recommendations and the literature review of Chapter 2, the design of the assessment framework commenced. As each element of the blockchain assessment framework was designed, a meeting would be setup with the company's representatives to explain the element and obtain the necessary inputs from the company, while simultaneously using the meeting to encourage feedback on the particular element. The feedback was then used to make any required adjustments to the element of the framework.

Once every element was completed and their respective inputs were obtained, the elements were joined together to create the final blockchain assessment framework. The demonstration of the framework could then begin and the final outputs of it were

obtained for the company's specific case provided. The results of the assessment were analysed as presented in Section 4.2.3.

A presentation was prepared to present the final framework and the results to the representatives of the company. The aim of the presentation was twofold: ensure the company was satisfied with the insight the results enable and to gather feedback on the framework itself. The presentation promoted feedback on the framework by adopting a semi-structured interview approach. This approach was taken to ensure that the company representatives never felt pressured into giving feedback on topics they had not fully thought about, while also allowing the author to guide the conversation to receive the feedback required. Prompting and probing were used to extract more direct answers where necessary, ultimately promoting useful feedback that would validate the framework. An overview of the semi-structured interview is shown in Table 4.5.

Table 4.5: Semi-Structured Interview Overview

Aspect	Overview
Interview Strategy	Framework validation
Method	Semi-structured interview
Objective	Validate the quality and usefulness of the designed blockchain assessment framework.
Input	– Blockchain assessment framework and elements – Blockchain assessment framework demonstration outcomes
Output	– Blockchain assessment framework feedback – Validated framework – Improvement and future work hints
Interviewees	– Company's Head of Product Development – Company's Divisional Manager

The experts are from two different areas of expertise to promote feedback from two different perspectives. The divisional manager provides input from a manager's perspective, considering all the elements that would be required to make an insightful decision and how the organization would would react to the implementation of the technology. The head of product development is continually involved with complex information systems and is thus able to provide input from a more technical standpoint.

The combination of the inputs and feedback from these experts provides a holistic perspective from which to validate the framework.

Certain key points of feedback were identified to ensure that the blockchain assessment framework conforms with both the functional and user requirements of Section 3.1.2 and 3.1.3, while satisfying the boundary conditions of Section 3.1.4 and the design restrictions of Section 3.1.5. Table 4.6 identifies the different feedback topics introduced during the presentation.

Table 4.6: Feedback Topic Overview

Topic	Evaluation Question
Framework Need	Is the need for creating the blockchain assessment framework for organizations clear?
Element Clarity	Are the different elements of the framework clear?
Element Completeness	Are there any elements that can be added or removed from the framework? Why would this be necessary?
Framework Usability	What is your opinion on the usability and flow of the elements of the framework?
Decision Aid	Do the outcomes of the blockchain assessment framework aid with decision-making regarding blockchain implementation?
General	Are there any areas in which more research is required or are there elements of the framework that could be improved? How?

4.3.2 Validation Feedback

As mentioned previously, the feedback was obtained using a semi-structured interview approach combined with a presentation. The presentation began by explaining the identified research opportunity and how the study aims to address this knowledge gap. Secondly, it gave an overview of the case study provided to ensure that all participant's perspectives were correctly aligned. The blockchain assessment framework was then introduced, indicating the flow between the different elements and how they are used in conjunction with one another. Then each element of the framework was explained more in-depth, along with the inputs required and the outcome of the element based on the company's inputs. Recommendations for the company were then provided based on the outcomes of the elements. Finally, any feedback that was not given during the bulk of the presentation was prompted from the company's representatives at the end. The

feedback is presented in Table 4.7 below, where the feedback from both of the comapny's representatives is combined to give overall feedback for each topic identified in Table 4.6.

Table 4.7: Validation Feedback

Topic	Feedback
Framework Need	Yes. The framework really helps to decide whether it is worthwhile for the company to invest in analysing blockchain at a deeper level. While it is not a detailed analysis that will indicate whether blockchain will be successful and what gains can be expected, it works great as a starting point to generate momentum and guide the organization with the next potential steps of blockchain exploration. Furthermore, the framework joins different aspects of blockchain into one framework, showing the connection between them and provides a way of thinking to ensure that no aspects are left out and that all major considerations have been thought about. Lastly, it shows where a blockchain solution can add value and how its functional characteristics achieve this where other solutions cannot.
Element Clarity	Yes. All of the elements, and the purpose of each, is abundantly clear and the order of them is logical and the flow of information between them makes sense.
Element Completeness	No. The elements that are present are sufficient for a satisfactory analysis of blockchain to take place.
Framework Usability	The framework flows well and allows the correlation between different elements to be identified. The framework is easy to use and does not require a lot of inputs and time compared to the outcomes that are obtained through using it. The sequence and separation of the different elements help to structure meaningful discussions and pinpoint where different barriers to adoption may lie.

Continued on next page

Continued from previous page

Topic	Feedback
Decision Aid	Yes. The outcomes give a good indication as to whether blockchain is a viable solution that should be analysed further and thus aids with decision making regarding further blockchain analysis. It helps with presenting concrete results that can be used to ensure that all stakeholders have the same perspective on the advantages and disadvantages of a blockchain solution. However, the framework does not help decide whether blockchain should be implemented, rather it helps decide whether more research should be done on it or not. Further along in blockchain exploration, the framework will not be as useful and will require more quantitative indications comparing the benefit of implementing blockchain and not implementing it.
General	Yes. To be more useful to the user, a more detailed design of a blockchain solution would help immensely. Furthermore, the "Blockchain Value Analysis" element could be more quantitative, indicating actual values for the expected costs, performance and cost reductions. Also, the "Blockchain High-Level Design" inputs are subjective to the user and a way of incorporating more objectivity could be beneficial. The framework could be used iteratively to gain deeper understanding with each pass or as more information becomes available.

4.3.3 Feedback Insights

Insights can be drawn based on the feedback from the presentation, which was focused on the topics highlighted in Table 4.6. These insights are summarized in Table 4.8 and are used as the basis for recommendations on potential future research or are incorporated into the final iteration of the blockchain assessment framework.

Table 4.8: Feedback Insights

Insight	Action
Add quantitative values to indicate the costs during the different phases of blockchain implementation based on the solution's design and expected implementation approach.	*Future Research:* current research lacks the data to estimate costs based on design features and the implementation approach.
Add quantitative values to indicate the cost reductions that can be experienced compared to a traditional solution based on the blockchain solution's design.	*Future Research:* current research lacks the data to estimate cost reductions based on design features.
Provide quantitative values to indicate the performance of a chosen solution.	*Future Research:* current research lacks the data to estimate the performance of a blockchain solution based on its configuration.
Add more design features to make the blockchain design step more detailed and specific to the user.	*Future Research:* the current literature review does not allow the comparison of different design choices based on the effect they would have on the criteria identified in Section 3.2.2.3.
Indicate the trade-offs between the different design criteria when identifying a relevant design choice.	*Future Research:* more research is required to determine the interaction of the different design criteria and how they could affect each other.
Include more objectivity into the high-level design step of the blockchain solution.	*Future Research:* more research would be required to add filters to create more objectivity, such as the definition of a relevant use case that is already present.
Indicate the value of doing multiple passes with the framework to gain a better understanding with each iteration.	*Final Framework Iteration:* the final iteration includes a decision gate after the "Blockchain Value Analysis" that promotes more iterations for better accuracy.

4.4 Chapter Summary and Discussion

This chapter began with brief descriptions of how the blockchain assessment framework would be demonstrated using a case study and validated through expert analysis with the use of a semi-structured interview, and how these would be used to enhance the design of the framework for the final iteration. The first section revisits the problem statement and ultimately what the framework is expected to accomplish and formalizes this through the creation of a hypothesis. Although there are improvements that can be made, the hypothesis is accepted based on the feedback received from the company representatives.

The next section begins with an overview of the case study used to demonstrate the use of the framework and continues with the demonstration, completing each element and discussing the insights that can be drawn from the outcomes. The final discussion indicates that blockchain is a suitable solution for the company, but the company must rather wait for more advances to be made within their industry before they commit major resources to exploring it further.

These outcomes were then presented to the company's representatives, along with a description of the framework and each element. This presentation was coupled with a semi-structured interview to form the basis of the feedback received from the company's representatives that would be used for validation. A variety of feedback topics were broached and insights could subsequently be drawn from the discussion that took place. The main points of feedback can be summarized as follows:

- It conglomerates a collection of blockchain knowledge to advance the understanding and application of it in organizations.
- It covers the main aspects of an assessment and ensures nothing is left out, ultimately providing important outcomes and guidelines.
- It helps with generating momentum regarding blockchain exploration and the future steps to be taken.
- The framework elements are clear, purposeful and complete, while flowing smoothly and being easy to use and understand.
- The framework aids with efficient decision making regarding further blockchain analysis.

- There are improvements that can be made to make the framework more helpful with blockchain implementation, rather than just indicating whether further analysis is worthwhile or not.

This feedback was then used to enhance the design of the framework and also provide insight into recommendations for potential future research. This unified framework addresses a need and although there are improvements that can be made, it aids with assessing blockchain and kickstarts the blockchain exploration process.

4.5 Chapter Conclusion

In conclusion, this chapter demonstrated the use of the framework through the use of a case study, showing how each element works and the outcomes to be expected and the insights that can be drawn. The outcomes were presented to the subjects of the case study and feedback was received from them, allowing the validity of the framework to be proven, showing that the need for such a framework is clear and that the current framework addresses these needs well, with some minor improvements that can be included. The feedback received from the expert analysis was used to either make enhancements to the framework or provide recommendations for potential future research. Chapter 4 answered the following research questions identified in Section 1.3.2: SO7.3, SO7.4, SO8.2, SO8.3, and SO8.4. The next chapter presents the conclusions of this research and suggests possible areas for future research, as well as the limitations of the study.

5 CONCLUSION

This final chapter concludes the study by providing a brief summary of the research, followed by the major findings and how each research question was addressed during the study. This is followed by a reflection on these findings. Then the limitations of the study are discussed and the chapter concludes with future research recommendations.

5.1 Research Summary

The final outcome of this study is a blockchain assessment framework that can be used to assess blockchain's feasibility within a particular process within an organization. The aim of the framework is to assess how well a blockchain solution fits within an organization and the chosen process based on the characteristics of a blockchain solution and the characteristics of the organization and process. Following this, a high-level blockchain solution is designed, providing a first look at what a suitable solution might look like for the organization's process. This leads to a framework that is used to determine the major considerations during the solution's lifecycle and in each layer of an enterprise's architecture. The final element uses the knowledge of the previous elements to identify the potential costs that could be incurred during implementation, the required performance of a blockchain solution, and the cost reductions that the solution may introduce.

The study began with identifying the opportunity that the current academic literature presents. The research method for addressing this opportunity was then presented, where the research objectives and research questions were identified. This then lead into the design of the ensuing research and how the necessary knowledge would be obtained and the scope within which the research would take place.

Following this, a comprehensive literature review was undertaken to obtain the knowledge required to design the final framework. This focused on gathering information on blockchain and its operation and different components. This was followed by identifying the characteristics of blockchain, the challenges it is faced with and how it compares to traditional databases. The different types of use cases that blockchain provides value in was looked at. Then the different factors that depict how suitable blockchain is for a given circumstance were identified and split into relevant domains. Adoption of blockchain was then looked at, focusing on the lifecycle of blockchain and the considerations that must be thought of and what adoption strategies can be used. Then the metrics that can be used to compare blockchain solutions with one another

and with more traditional solutions are identified. Finally, the different aspects that are present in a variety of blockchain assessments were identified to help determine the aspects that should be included in a comprehensive blockchain assessment.

This chapter is then followed by the design methodology and design of a relevant blockchain assessment framework. This chapter begins with identifying the different design requirements of an assessment framework. This is followed by presenting the chosen design methodology and the eventual design of the framework. The design begins by designing each element of the framework independently and then incorporating them into the final blockchain assessment framework.

The framework was then demonstrated using a case study in Chapter 4. The results of the demonstration were then presented and used to gain feedback by expert analysis through the use of a semi-structured interview. This feedback was used to validate the framework and to identify possible enhancements to the framework, as well as potential future research areas. A summary of the study is shown in Figure 5.1 below.

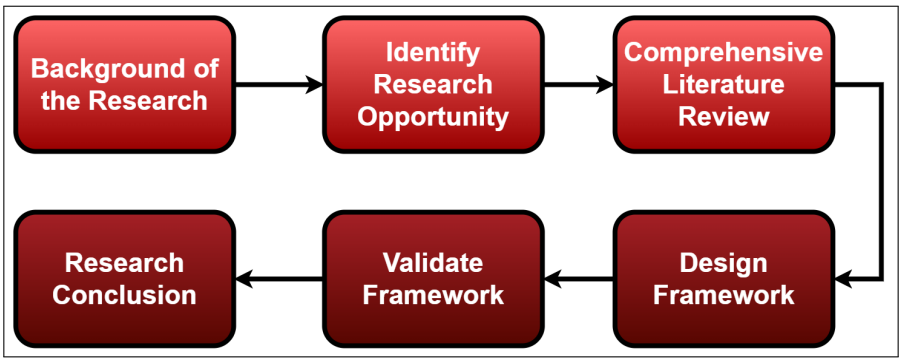


Figure 5.1: Study Summary

5.2 Research Findings and Reflection

This section highlights the key findings of the study by investigating how each research question, identified in Section 1.3.2, was answered. Based on these research findings, a reflection of the study will be made.

The aim of this study was to create a blockchain assessment framework to assess the potential use of blockchain within an organization. The framework was created to address an opportunity identified in Section 1.2, based on the following information:

- Blockchain is a nascent technology with major disruptive potential.

- Blockchain's characteristics are expected to introduce groundbreaking functionality to databases, such as end-to-end transparency, trust, immutability, and distribution.
- Successful implementation of blockchain solutions are few and far between because of the lack of knowledge on it and experience with it.
- Blockchain assessment literature is scattered and not particularly generic.

There was no generic approach that could be used to assess blockchain for a particular process. This was highlighted by a literature review and through collaboration with industry experts. This study attempted to address this by identifying relevant research questions to be answered, presented in Table 1.2. The findings for each research question are discussed below.

5.2.1 Research Question Findings

The research questions identified in Section 1.3.2 are answered to address the research sub-objectives identified in Section 1.3.1, which are in turn required to be satisfied in order to realize the main objective of the study. The answer, or where the answer is situated, for each research question is explored below.

SO1.1: What is blockchain technology?
One of the biggest barriers to blockchain adoption is the misunderstanding of the technology and so creating a deeper understanding of how it operates and what it consists of is the first step in a successful assessment of the technology. Section 2.1 of this study deals with this, explaining how blockchain works and the major components it consists of.

SO1.2: What are the fundamentals of blockchain technology?
Again looking to create a deeper understanding of blockchain, the fundamentals of the technology will help with understanding it while ensuring the research does not get too technical. Section 2.1 is focused on identifying and explaining these fundamentals of blockchain.

SO2.1: What are the different types of blockchain and how do they differ?
A major decision to be made regarding blockchain design are the types of blockchain solutions that can be implemented. Thus, Section 2.1.6 deals with identifying the different types of blockchain and how they are different to one another.

SO2.2: What is currently known about the potential of blockchain within organizations?

There would not be a purpose in having an assessment framework for organizations if there was no potential for blockchain within these organizations. Section 2.3 highlights the different use cases in which a blockchain solution has proven to be beneficial for organizations.

SO2.3: How can blockchain enable organizations to create value within their processes?

Section 2.2.1 investigates the characteristics of blockchain and how these may provide certain functionalities to organizations that other solutions might not. Section 2.3 highlights the main areas where blockchain solutions have proven successful and therefore gives an indication as to how these functionalities are used to create value. Lastly, Section 2.6.2 highlights certain cost reductions that may be introduced through the use of a blockchain solution, indicating the value it brings in terms of time saving and cost reduction.

SO2.4: What are the different elements of blockchain, what choices do they present and how do they differ?

Section 2.1 deals with the different components that blockchain consists of and thus certain design choices that need to be made. This study focuses on the consensus mechanisms presented in Section 2.1.5 and the blockchain types presented in Section 2.1.6 and therefore compares the different choices of these elements comprehensively. Elements that do not directly affect a solutions performance are still presented as long as they add value to the study, but are not explored as in-depth, merely describing the different choices and the difference between them on a surface level.

SO3.1: How does blockchain compare against traditional solutions?

Section 2.2 investigates the characteristics of blockchain and how these introduce functionalities that other solutions cannot replicate. The section ends by comparing how blockchain solutions compare against traditional databases.

SO4.1: What are the aspects of blockchain assessment that need to be incorporated into the design of a generic blockchain assessment approach for organizations?

Section 2.7 investigates the assessment approaches that are used in current literature and identifies how common each aspect is and combines them to identify the aspects that should be included in a generic blockchain assessment framework.

SO4.2: What are the strengths and weaknesses of the currently available blockchain assessment approaches of these relevant aspects?

The weakness of these approaches is often that they do not incorporate all the elements necessary for a full assessment or they are focused on assessing particular use cases rather than creating generic assessment approaches. Section 2.7 highlights the strengths and weaknesses of the current assessment approaches, while Section 3.2 highlights the strengths that are taken from these different approaches to create a generic blockchain assessment framework.

SO4.3: Which of these aspects can be quantified and how can they be measured?

Section 3.2.2 shows which elements of the framework can be quantified. The fit analysis is quantified based on the organization and process' characteristics and is measured relative to a threshold score. The design element uses the user's preferences to quantify their ideal solution, which can then be compared to the choices values to identify the best solution. Finally, the value analysis has the potential to be quantified but requires more research to accurately incorporate quantitative measures.

SO5.1: What are the strengths that can be taken from each blockchain assessment approach for each element to be used in a single, cohesive blockchain assessment approach?

Section 3.2 and Section 3.3 indicate the strengths that are taken from the different approaches and ultimately incorporated into the final elements of the blockchain assessment framework, which is informed by the strengths identified in Table 2.22.

SO6.1: What are the shortcomings present in the created blockchain assessment approach and how can they be identified?

Section 4.2 and Section 4.3 are focused on demonstrating the use of the framework by using a case study and validating the framework by expert analysis through the use of a semi-structured interview. Both these sections allowed the shortcomings of the framework to be identified by drawing insights from the results of the sections.

SO6.2: How can the shortcomings of the framework be addressed?

Section 4.3.3 briefly explains how the identified shortcomings of the framework can be addressed: either through enhancing the framework design or recommending areas of future research.

SO7.1: What are the required outcomes of a blockchain assessment approach that supports decision-making regarding blockchain implementation in organizations?

Section 3.1 identifies the outcomes that would support decision-making regarding blockchain in organizations. Section 4.4 validates these outcomes and recommend improvements to make the outcomes more useful.

SO7.2: What does a blockchain assessment approach for organizations look like?

Section 3.1 identifies what is required of a blockchain assessment framework and Section 3.3 presents what this solution might look like, while Section 4.3 validates the flow and logic of the framework.

SO7.3: Are the outcomes insightful results that clearly indicate the suitability, feasibility and impact of a blockchain solution?

Section 4.3 validates the outcomes of the framework, indicating that they are insightful in determining whether further blockchain exploration is worthwhile. However, the feasibility and impact of a blockchain solution is not as insightful as it ought to be and the introduction of more quantitative values indicating costs, performance and cost reductions could be beneficial.

SO7.4: Does the tool meet its requirements?

Section 4.2 and Section 4.3 ensure that the tool has met the design requirements of Section 3.1, excluding the functional requirement F1 and the boundary condition B5. F1 is mostly satisfied, but as noted in Section 4.3.3, the framework is not as useful in the later decision-stages of blockchain implementation and thus the requirement could be changed from "...in the decision-stages of blockchain implementation..." to "...in the early decision-stages of blockchain implementation...". Considering that only one use case was used to demonstrate and validate the framework, the boundary condition B5 cannot be validated until more case studies using the framework have taken place.

SO8.1: What are the scope and limitations of this approach based on the data it was created from?

The scope of the created framework is addressed in Section 1.3.4, while the limitations are presented in Section 5.3.

SO8.2: How can the feasibility and validity of the blockchain assessment approach be demonstrated and validated?
Section 4.2 and 4.3 deal with demonstrating the use of the tool using a case study and ensuring its validity through the use of a semi-structured interview.

SO8.3: Will this approach help with a complete assessment of blockchain implementation for organizations within the scope?
As mentioned in Section 4.3.3, the framework helps with decision-making during blockchain exploration and becomes less useful during later stages of blockchain implementation, but the assessment is well-rounded and provides much needed momentum for blockchain exploration. Furthermore, more case studies are required to ensure that the framework is useful for other organizations within the scope.

SO8.4: Is the approach able to support decision-making in organizations considering blockchain implementation?
Through the validation of Section 4.3, it is noted that the framework helps organizations with decision-making during the early stages of blockchain exploration, indicating whether further analysis on the technology would be beneficial or not.

5.2.2 Reflection

Based upon the research findings of the previous section and the outcome of this study, reflection of the research can take place. This reflection focuses on the main outcome of this study, the blockchain assessment framework, but briefly reflects on other aspects such as the research process and certain choices made during the study.

Validity of the study was ensured by collecting data from multiple sources throughout the study. The main source of knowledge being the existing literature on blockchain, but this knowledge and the deductions made from it were complemented by using a demonstrative case study and expert analysis. Furthermore, the need for an assessment approach was identified during the research opportunity identification and the author's perspective can affect the way this need is addressed. Thus, subjectivity and bias were avoided by systematically translating the gap of knowledge into literature topics to be explored to enable the realization of requirements and elements of the blockchain assessment framework, ultimately enabling the replication of the logic of this research. The actual design of the framework is subject to the author's perspective, but by describing the design methodology and the choices made, other researchers that take similar steps to address the same research opportunity would design a similar framework. Finally, the

choice to design a framework with tangible outcomes, as opposed to a decision-making model or discussion format, is to provide practical value to the users of the framework.

Reflecting on the actual outcome of this study, the blockchain assessment framework, it can be noted that the framework ended being more high-level than originally intended. Initially the framework was being designed with the intention of providing an organization with the necessary outcomes to fully determine whether blockchain should or should not be implemented within their organization. However, as the design progressed and feedback was received, it quickly became obvious that the framework was not detailed or quantitative enough to provide meaningful insight as to whether blockchain should or should not be implemented. This is not to say that the framework is useless, rather the framework has proven to be extremely helpful during the early stages of blockchain exploration instead of during the later stages of blockchain implementation as intended. The framework is extremely useful for initiating the blockchain exploration journey and determining whether further analysis is worthwhile. The framework helps to identify what the next steps of the blockchain exploration journey should be and whether embarking on that journey could be worth the effort. Furthermore, this research and the outcome of this research provide a solid foundation upon which future work on blockchain assessment approaches can be built upon which fully indicate whether to implement blockchain. The study has gathered a variety of relevant knowledge to allow further exploration on the topic of blockchain assessment, providing a strong base from which future research can take place.

5.3 Limitations

Blockchain is still a very new technology and consequently there is not ample amounts of research on the topic of blockchain assessment. As such, the study is limited by the blockchain research that is available. Furthermore, blockchain's novelty means there is a lack of standards with regards to a variety of blockchain aspects. One of these aspects is the measurement of blockchain performance, where different studies use different metrics to indicate performance. This lack of standards limits the way in which research can be compared against one another to produce useful insights.

This study has been limited to businesses within South Africa because of the use of a South African company for validation. Furthermore, the framework's validity has not been proven in multiple South African industries, and is consequently limited due to this until it has proven its value through further validation in other industries. A further

limitation is the exclusion of other design features in the high-level blockchain design element because of the lack of data that links these potential features with how they affect blockchain performance. Lastly, the assessment framework makes use of a variety of subjective inputs and is thus limited by the biases and perspective of potential users.

5.4 Future Research Recommendations

The insights drawn from this study can be used to identify potential areas of future research that could enhance academic literature on blockchain assessment and enable more thorough studies to be completed. The recommendations for future research are presented below:

- ***Blockchain Development and Implementation Costs.*** Gather empirical data on the cost of developing and implementing blockchain solutions to enable the creation of cost models that can be used to more accurately predict blockchain costs.
- ***Different Blockchain Configuration Performances.*** Gather empirical data on the performance of different blockchain solution configurations based on a wide variety of performance metrics to enable more accurate predictions of blockchain solution performance.
- ***Blockchain Cost Reductions.*** Create mathematical models that can be used to estimate the cost savings introduced by a blockchain solution based on the time it saves during different operations.
- ***Blockchain Design Choices.*** Investigate how different design features and their relevant options will affect the performance of different process criteria of a blockchain solution.
- ***Design Criteria Trade-offs.*** Investigate how the different process criteria identified in Section 3.2.2.3 affect each other and the relationship between them.
- ***Introduce Objectivity into the Framework.*** Investigate how more objective inputs can be used within the blockchain assessment framework to reduce the biases of potential users and increase the accuracy of results. Further investigate how different multi-criteria decision-making methods affect the results produced by the assessment framework and which produces the most accurate results.

Bibliography

Al-Breiki, H., Rehman, M.H.U., Salah, K. and Svetinovic, D. (2020). Trustworthy Blockchain Oracles: Review, Comparison, and Open Research Challenges. *IEEE Access*, vol. 8, pp. 85675–85685.

Ali, M.S., Dolui, K. and Antonelli, F. (2017). IoT Data Privacy via Blockchains and IPFS. In: *Proceedings of the seventh international conference on the internet of things*, pp. 1–7.

Allessie, D. (2017). Blockchain Technology for Governmental Processes: The Design of a Blockchain Assessment Tool: a Design Science Approach.

Alqahtani, S. and Demirbas, M. (2021). Bottlenecks in Blockchain Consensus Protocols. In: *2021 IEEE International Conference on Omni-Layer Intelligent Systems (COINS)*, pp. 1–8. IEEE.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y. *et al.* (2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In: *Proceedings of the thirteenth EuroSys conference*, pp. 1–15.

Angelis, J. and da Silva, E.R. (2019). Blockchain adoption: A value driver perspective. *Business Horizons*, vol. 62, no. 3, pp. 307–314.

Ar, I.M., Erol, I., Peker, I., Ozdemir, A.I., Medeni, T.D. and Medeni, I.T. (2020). Evaluating the feasibility of blockchain in logistics operations: A decision framework. *Expert Systems with Applications*, vol. 158, p. 113543.

Atlam, H.F., Alenezi, A., Alassafi, M.O. and Wills, G.B. (2018). Blockchain with Internet of Things: Benefits, Challenges, and Future Directions. *International Journal of Intelligent Systems & Applications*, vol. 10, no. 6.

Atzori, M. (2015). Blockchain Technology and Decentralized Governance: Is the State Still Necessary? *Available at SSRN 2709713*.

Bains, P. (2022). Blockchain Consensus Mechanisms: A Primer for Supervisors. *FinTech Notes*, vol. 2022, no. 003.

Bamakan, S.M.H., Motavali, A. and Bondarti, A.B. (2020). A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Systems with Applications*, vol. 154, p. 113385.

Barua, A., Konana, P., Whinston, A.B. and Yin, F. (2004). Assessing Internet Enabled Business Value: An Exploratory Investigation. *MIS Quarterly*, vol. 28, no. 4, pp. 585–620.

Bastiaan, M. (2015). Preventing the 51%-Attack: a Stochastic Analysis of Two Phase Proof of Work in Bitcoin.

Bauer, I., Zavolokina, L., Leisibach, F. and Schwabe, G. (2019). Exploring Blockchain Value Creation: The Case of the Car Ecosystem. In: *Proceedings of the 52nd Hawaii International Conference on System Sciences*.

Bechard, M. (2021). People lucky enough to have a job can expect 5.5% salaray rise in 2022.
Available at: `https://bit.ly/3PYgi9E`

Beck, R. and Müller-Bloch, C. (2017). Blockchain as Radical Innovation: A Framework for Engaging with Distributed Ledgers.

Bellini, E., Ceravolo, P. and Damiani, E. (2019). Blockchain-Based E-Vote-as-a-Service. In: *2019 IEEE 12th International Conference on Cloud Computing (CLOUD)*, pp. 484–486. IEEE.

Beniiche, A. (2020). A Study of Blockchain Oracles. *arXiv preprint arXiv:2004.07140*.

Bergman, S., Asplund, M. and Nadjm-Tehrani, S. (2020). Permissioned blockchains and distributed databases: A performance study. *Concurrency and Computation: Practice and Experience*, vol. 32, no. 12, p. e5227.

Bonneau, J., Clark, J. and Goldfeder, S. (2015). On Bitcoin as a public randomness source. *IACR Cryptol. ePrint Arch.*, vol. 2015, p. 1015.

Braun, C. and Winter, R. (2007). Integration of IT Service Management into Enterprise Architecture. In: *Proceedings of the 2007 ACM symposium on Applied computing*, pp. 1215–1219.

Brilliantova, V. and Thurner, T.W. (2019). Blockchain and the future of energy. *Technology in Society*, vol. 57, pp. 38–45.

Brockmöller, A.A.C. (2008). Knowledge sharing in expert-apprentice relations.

Bucher, T., Fischer, R., Kurpjuweit, S. and Winter, R. (2006). Analysis and Application Scenarios of Enterprise Architecture: An Exploratory Study. In: *2006 10th IEEE International Enterprise Distributed Object Computing Conference Workshops (EDOCW'06)*, pp. 28–28. IEEE.

Bürer, M.J., de Lapparent, M., Pallotta, V., Capezzali, M. and Carpita, M. (2019). Use cases for Blockchain in the Energy Industry Opportunities of emerging business models and related risks. *Computers & Industrial Engineering*, vol. 137, p. 106002.

Buterin, V., Reijsbergen, D., Leonardos, S. and Piliouras, G. (2020). Incentives in Ethereum's hybrid Casper protocol. *International Journal of Network Management*, vol. 30, no. 5, p. e2098.

Carson, B., Romanelli, G., Walsh, P. and Zhumaev, A. (2018). Blockchain beyond the hype: What is the strategic business value. *McKinsey & Company*, pp. 1–13.

Casino, F., Dasaklis, T.K. and Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and informatics*, vol. 36, pp. 55–81.

Castro, M. and Liskov, B. (2002). Practical Byzantine Fault Tolerance and Proactive Recovery. *ACM Transactions on Computer Systems (TOCS)*, vol. 20, no. 4, pp. 398–461.

Castro, M., Liskov, B. *et al.* (1999). Practical Byzantine Fault Tolerance. In: *OsDI*, vol. 99, pp. 173–186.

Cavalcante, J. and Gzara, L. (2018). Product-Service Systems lifecycle models: literature review and new proposition. *Procedia CIRP*, vol. 73, pp. 32–38.

Chen, W., Botchie, D., Braganza, A. and Han, H. (2022). A transaction cost perspective on blockchain governance in global value chains. *Strategic Change*, vol. 31, no. 1, pp. 75–87.

Chowdhury, M.J.M., Colman, A., Kabir, M.A., Han, J. and Sarda, P. (2018). Blockchain versus Database: A Critical Analysis. In: *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pp. 1348–1353. IEEE.

Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V. *et al.* (2016). Blockchain Technology: Beyond Bitcoin. *Applied Innovation*, vol. 2, no. 6-10, p. 71.

Dabbagh, M., Choo, K.-K.R., Beheshti, A., Tahir, M. and Safa, N.S. (2021). A survey of empirical performance evaluation of permissioned blockchain platforms: Challenges and opportunities. *computers & security*, vol. 100, p. 102078.

Dabbagh, M., Kakavand, M., Tahir, M. and Amphawan, A. (2020). Performance Analysis of Blockchain Platforms: Empirical Evaluation of Hyperledger Fabric and Ethereum. In: *2020 IEEE 2nd International Conference on Artificial Intelligence in Engineering and Technology (IICAIET)*, pp. 1–6. IEEE.

Dattani, J. and Sheth, H. (2019). Overview of Blockchain Technology. *Asian Journal of Convergence in Technology*, vol. 5, no. 1, pp. 1–3.

Davenport, T.H. (1993). *Process innovation: reengineering work through information technology*. Harvard Business Press.

Davies, A. (2021). How much blockchain cost for software development? Available at: `https://www.devteam.space/blog/how-much-blockchain-cost-for-software-development/`

De Filippi, P. and Loveluck, B. (2016). The invisible politics of Bitcoin: governance crisis of a decentralized infrastructure. *Internet policy review*, vol. 5, no. 4.

Dieter, G.E., Schmidt, L.C. *et al.* (2013). *Engineering Design*, vol. 5. McGraw-Hill Higher Education Boston.

Dong, W.M. and Wong, F.S. (1987). Fuzzy Weighted Averages and Implementation of the Extension Principle. *Fuzzy sets and systems*, vol. 21, no. 2, pp. 183–199.

Duarte, A.I.M. and Costa, C.J. (2012). Information Systems: Life Cycle and Success. In: *Proceedings of the Workshop on information systems and design of communication*, pp. 25–30.

El Ioini, N. and Pahl, C. (2018). A Review of Distributed Ledger Technologies. In: *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*, pp. 277–288. Springer.

Erol, I., Ar, I.M., Ozdemir, A.I., Peker, I., Asgary, A., Medeni, I.T. and Medeni, T. (2020). Assessing the feasibility of blockchain technology in industries: evidence from Turkey. *Journal of Enterprise Information Management*.

Evans, D.S. (2014). Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms. *University of Chicago Coase-Sandor Institute for Law & Economics Research Paper*, , no. 685.

Eyal, I., Gencer, A.E., Sirer, E.G. and Van Renesse, R. (2016). {Bitcoin-NG}: A Scalable Blockchain Protocol. In: *13th USENIX symposium on networked systems design and implementation (NSDI 16)*, pp. 45–59.

Eyal, I. and Sirer, E.G. (2014). Majority Is Not Enough: Bitcoin Mining Is Vulnerable. In: *International conference on financial cryptography and data security*, pp. 436–454. Springer.

Fabrizio, N., Rossi, E., Martini, A., Anastasovski, D., Cappello, P., Candeago, L. and Lepri, B. (2019). Invoice Discounting: A Blockchain-Based Approach. *Frontiers in Blockchain*, vol. 2, p. 13.

Fernández Caramés, T.M. and Fraga Lamas, P. (2020). Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE access*, vol. 8, pp. 21091–21116.

Garcia-Torres, S., Albareda, L., Rey-Garcia, M. and Seuring, S. (2019). Traceability for sustainability–literature review and conceptual framework. *Supply Chain Management: An International Journal*.

Garzik, J. *et al.* (2015). Public versus Private Blockchains Part 1: Permissioned Blockchains White Paper. *BitFury Group*.

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C. and Santamaria, V. (2018). To blockchain or not to blockchain: That is the question. *IT Professional*, vol. 20, no. 2, pp. 62–74.

Gervais, A., Karame, G.O., Wüst, K., Glykantzis, V., Ritzdorf, H. and Capkun, S. (2016). On the Security and Performance of Proof of Work Blockchains. In: *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pp. 3–16.

Gopalakrishnan, P.K., Hall, J. and Behdad, S. (2021). Cost analysis and optimization of Blockchain-based solid waste management traceability system. *Waste Management*, vol. 120, pp. 594–607.

Gourisetti, S.N.G., Mylrea, M. and Patangia, H. (2019). Evaluation and Demonstration of Blockchain Applicability Framework. *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1142–1156.

Hao, Y., Li, Y., Dong, X., Fang, L. and Chen, P. (2018). Performance Analysis of Consensus Algorithm in Private Blockchain. In: *2018 IEEE Intelligent Vehicles Symposium (IV)*, pp. 280–285. IEEE.

Hassani, H., Huang, X. and Silva, E. (2018). Banking with blockchain-ed big data. *Journal of Management Analytics*, vol. 5, no. 4, pp. 256–275.

He, Y., Li, H., Cheng, X., Liu, Y., Yang, C. and Sun, L. (2018). A Blockchain Based Truthful Incentive Mechanism for Distributed P2P Applications. *IEEE access*, vol. 6, pp. 27324–27335.

Hedman, J. and Kalling, T. (2003). The business model concept: theoretical underpinnings and empirical illustrations. *European journal of information systems*, vol. 12, no. 1, pp. 49–59.

Hon, W.K., Palfreyman, J. and Tegart, M. (2016). Distributed Ledger Technology & Cybersecurity. *European Union Agency For Network And Information Securit (ENISA)*.
Available at: `https://www.enisa.europa.eu/publications/blockchain-security`

IBM (2022). What is EAM?
Available at: `https://www.ibm.com/topics/enterprise-asset-management#:~:text=Enterpriseassetmanagement(EAM)is,uptimeandreduceoperationalcosts.`

Janssen, M. (2009). Framing Enterprise Architecture: A Metaframework for Analyzing Architectural Efforts in Organizations. *Coherency Management: Architecting the Enterprise for Alignment, Agility and Assurance*, pp. 107–126.

Jen, L.-r. and Lee, Y.-j. (2000). IEEE recommended practice for architectural description of software-intensive systems. In: *IEEE Architecture*. Citeseer.

Joannou, D., Kalawsky, R., Martínez-García, M., Fowler, C. and Fowler, K. (2020). Realizing the Role of Permissioned Blockchains in a Systems Engineering Lifecycle. *Systems*, vol. 8, no. 4, p. 41.

Jonkers, H., Lankhorst, M., Van Buuren, R., Hoppenbrouwers, S., Bonsangue, M. and Van Der Torre, L. (2004). Concepts for Modeling Enterprise Architectures. *International Journal of Cooperative Information Systems*, vol. 13, no. 03, pp. 257–287.

Jonkers, H., Lankhorst, M.M., ter Doest, H.W., Arbab, F., Bosma, H. and Wieringa, R.J. (2006). Enterprise architecture: Management tool and blueprint for the organisation. *Information systems frontiers*, vol. 8, no. 2, p. 63.

Kamal, M.M. (2006). IT innovation adoption in the government sector: identifying the critical success factors. *Journal of Enterprise Information Management*.

Karafiloski, E. and Mishev, A. (2017). Blockchain solutions for big data challenges: A literature review. In: *IEEE EUROCON 2017-17th International Conference on Smart Technologies*, pp. 763–768. IEEE.

Khan, D., Jung, L.T., Hashmani, M.A. and Cheong, M.K. (2022). Empirical Performance Analysis of Hyperledger LTS for Small and Medium Enterprises. *Sensors*, vol. 22, no. 3, p. 915.

Khan, M.I., Faisal, F., Azam, S., Karim, A., Shanmugam, B. and De Boer, F. (2019). Using blockchain technology for file synchronization. In: *IOP Conference Series: Materials Science and Engineering*, vol. 561, p. 012117. IOP Publishing.

Kharitonov, A. (2017). A Framework for Strategic Intra-and Inter-Organizational Adoption of the Blockchain Technology. *SSRN 3005343*.

Kochhar, R., Kochar, B., Singh, J. and Juyal, V. (2018). Blockchain and its impact on telecom networks.

Koens, T. and Poll, E. (2018). What Blockchain Alternative Do You Need? In: *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, pp. 113–129. Springer.

Kombe, C., Dida, M. and Sam, A. (2018). A review on healthcare information systems and consensus protocols in blockchain technology.

Konashevych, O. (2020). General Concept of Real Estate Tokenization on Blockchain. *European Property Law Journal*, vol. 9, no. 1, pp. 21–66.

Krause, W. and Schutte, C.S.L. (2015). A Perspective on Open Innovation in Small- and Medium-sized Enterprises in South Africa, and Design Requirements for an Open Innovation Approach. *South African Journal of Industrial Engineering*, vol. 26, no. 1, pp. 163–178.

Kroll, J.A., Davey, I.C. and Felten, E.W. (2013). The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. In: *Proceedings of WEIS*, vol. 2013. Washington, DC.

Kuzlu, M., Pipattanasomporn, M., Gurses, L. and Rahman, S. (2019). Performance Analysis of a Hyperledger Fabric Blockchain Framework: Throughput, Latency and Scalability. In: *2019 IEEE international conference on blockchain (Blockchain)*, pp. 536–540. IEEE.

Lapointe, C. and Fishbane, L. (2019). The Blockchain Ethical Design Framework. *Innovations: Technology, Governance, Globalization*, vol. 12, no. 3-4, pp. 50–71.

Lashkari, B. and Musilek, P. (2021). A Comprehensive Review of Blockchain Consensus Mechanisms. *IEEE Access*, vol. 9, pp. 43620–43652.

Laurent, P., Chollet, T., Burke, M. and Seers, T. (2018). The tokenization of assets is disrupting the financial industry. are you ready. *Inside magazine*, vol. 19, pp. 62–67.

Leewayhertz (2019). Blockchain App Development Calculator.
Available at: `https://leewayhertz.outgrow.us/Blockchain-Cost-Calculator`

Li, C. and Zhang, L.-J. (2017). A Blockchain Based New Secure Multi-Layer Network Model for Internet of Things. In: *2017 IEEE international congress on internet of things (ICIOT)*, pp. 33–41. IEEE.

Lielacher, A. (2019). Blockchain consultants: How much do they charge?
Available at: `https://www.bitcoinmarketjournal.com/blockchain-consultants/#:~:text=HourlieRatesVaryGreatly,rateof$61to$80`

Litke, A., Anagnostopoulos, D. and Varvarigou, T. (2019). Blockchains for Supply Chain Management: Architectural Elements and Challenges Towards a Global Scale Deployment. *Logistics*, vol. 3, no. 1, p. 5.

Lo, S.K., Xu, X., Chiam, Y.K. and Lu, Q. (2017). Evaluating Suitability of Applying Blockchain. In: *2017 22nd International Conference on Engineering of Complex Computer Systems (ICECCS)*, pp. 158–161. IEEE.

Lu, Q. and Xu, X. (2017). Adaptable blockchain-based systems: A case study for product traceability. *Ieee Software*, vol. 34, no. 6, pp. 21–27.

Lukáš, P. (2017). Metrics for Evaluating Information Systems. *Posterus: Portál pre odborné publikovanie*. ISSN 1338-0087.

Maharjan, P.S. (2018). *Performance Analysis of Blockchain Platforms*. Ph.D. thesis, University of Nevada, Las Vegas.

Matthes, F., Buckl, S., Leitel, J. and Schweda, C.M. (2008). *Enterprise Architecture Management Tool Survey 2008*. Techn. Univ. München München.

Mattila, J. (2016). The Blockchain Phenomenon. *Berkeley Roundtable of the International Economy*, vol. 16.

Mendling, J., Weber, I., Aalst, W.V.D., Brocke, J.V., Cabanillas, C., Daniel, F., Debois, S., Ciccio, C.D., Dumas, M., Dustdar, S. *et al.* (2018). Blockchains for Business Process Management-Challenges and Opportunities. *ACM Transactions on Management Information Systems (TMIS)*, vol. 9, no. 1, pp. 1–16.

Miraz, M.H. and Ali, M. (2020). Blockchain Enabled Smart Contract Based Applications: Deficiencies with the Software Development Life Cycle Models. *arXiv preprint arXiv:2001.10589*.

Monrat, A.A., Schelén, O. and Andersson, K. (2020). Performance Evaluation of Permissioned Blockchain Platforms. In: *2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, pp. 1–8. IEEE.

Morabito, V. (2017). Business Innovation Through Blockchain. *Cham: Springer International Publishing*.

Morrow, M.J. and Zarrebini, M. (2019). Blockchain and the Tokenization of the Individual: Societal Implications. *Future Internet*, vol. 11, no. 10, p. 220.

Mougayar, W. (2016). *The Business Blockchain: promise, practice, and application of the next Internet technology*. John Wiley & Sons.

Mühlberger, R., Bachhofner, S., Castelló Ferrer, E., Ciccio, C.D., Weber, I., Wöhrer, M. and Zdun, U. (2020). Foundational Oracle Patterns: Connecting Blockchain to the Off-chain World. In: *International Conference on Business Process Management*, pp. 35–51. Springer.

Murthy, C.V.B., Shri, M.L., Kadry, S. and Lim, S. (2020). Blockchain Based Cloud Computing: Architecture and Research Challenges. *IEEE Access*, vol. 8, pp. 205190–205205.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, p. 21260.

Nguyen, C.T., Hoang, D.T., Nguyen, D.N., Niyato, D., Nguyen, H.T. and Dutkiewicz, E. (2019). Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. *IEEE Access*, vol. 7, pp. 85727–85745.

Nguyen, G.-T. and Kim, K. (2018). A survey about consensus algorithms used in blockchain. *Journal of Information processing systems*, vol. 14, no. 1, pp. 101–128.

Niranjanamurthy, M., Nithya, B.N. and Jagannatha, S.J.C.C. (2019). Analysis of Blockchain technology: pros, cons and SWOT. *Cluster Computing*, vol. 22, no. 6, pp. 14743–14757.

Nofer, M., Gomber, P., Hinz, O. and Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, vol. 59, no. 3, pp. 183–187.

Nowiński, W. and Kozma, M. (2017). How can blockchain technology disrupt the existing business models? *Entrepreneurial Business and Economics Review*, vol. 5, no. 3, pp. 173–188.

Oliveira, L., Zavolokina, L., Bauer, I. and Schwabe, G. (2018). To Token or not to Token: Tools for Understanding Blockchain Tokens.

Oliveira, T. and Martins, M.F. (2011). Literature Review of Information Technology Adoption Models at Firm Level. *Electronic Journal of Information Systems Evaluation*, vol. 14, no. 1, pp. pp110–121.

Panuparb, P. (2019). *Cost-benefit Analysis of a Blockchain-based Supply Chain Finance Solution*. Ph.D. thesis, Massachusetts Institute of Technology.

Peck, M.E. (2017). Do You Need a Blockchain? this chart will tell you if the technology can solve your problem. *IEEE Spectrum*, vol. 54, no. 10, pp. 38–60.

Performance, H. and Group, S.W. (2018). Hyperledger Blockchain Performance Metrics. *Whitepaper. https://www. hyperledger. org/wpcontent/uploads/2018/10/HL_Whitepaper_Metrics_PDF_V1*, vol. 1.

Pilkington, M. (2016). Blockchain technology: principles and applications. In: *Research handbook on digital transformations*. Edward Elgar Publishing.

Privitera, M.B. (2015). Developing Insights. *Contextual Inquiry for Medical Device Design*, p. 141.

Proudlock, M., Phelps, B. and Gamble, P. (1999). IT adoption strategies: Best practice guidelines for professional SMEs. *Journal of Small Business and Enterprise Development*.

Queralta, J.P. and Westerlund, T. (2021). Blockchain for mobile edge computing: Consensus mechanisms and scalability. In: *Mobile Edge Computing*, pp. 333–357. Springer.

Rehmani, M.H. (2021). Blockchain Technology and Database Management System. In: *Blockchain Systems and Communication Networks: From Concepts to Implementation*, pp. 15–22. Springer.

Risius, M. and Spohrer, K. (2017). A Blockchain Research Framework. *Business & Information Systems Engineering*, vol. 59, no. 6, pp. 385–409.

Romiti, M., Judmayer, A., Zamyatin, A. and Haslhofer, B. (2019). A deep dive into bitcoin mining pools: An empirical analysis of mining shares. *arXiv preprint arXiv:1905.05999*.

Ruan, P., Dinh, T.T.A., Loghin, D., Zhang, M., Chen, G., Lin, Q. and Ooi, B.C. (2021). Blockchains vs. Distributed Databases: Dichotomy and Fusion. In: *Proceedings of the 2021 International Conference on Management of Data*, pp. 1504–1517.

Ruokolainen, T., Ruohomaa, S. and Kutvonen, L. (2011). Solving Service Ecosystem Governance. In: *2011 IEEE 15th International Enterprise Distributed Object Computing Conference Workshops*, pp. 18–25. IEEE.

Scriber, B.A. (2018). A Framework for Determining Blockchain Applicability. *IEEE Software*, vol. 35, no. 4, pp. 70–77.

Seibold, S. and Samman, G. (2016). Consensus: Immutable Agreement for the Internet of Value. *KPMG¡ https://assets. kpmg. com/content/dam/kpmg/pdf/2016/06/kpmgblockchain-consensus-mechanism. pdf*.

Sikorski, J.J., Haughton, J. and Kraft, M. (2017). Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Applied Energy*, vol. 195, pp. 234–246.

Simon, D., Fischbach, K. and Schoder, D. (2013). An Exploration of Enterprise Architecture Research. *Communications of the Association for Information Systems*, vol. 32, no. 1, p. 1.

Singhal, B., Dhameja, G. and Panda, P.S. (2018). *Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions*. Springer.

Smetanin, S., Ometov, A., Komarov, M., Masek, P. and Koucheryavy, Y. (2020). Blockchain Evaluation Approaches: State-of-the-Art and Future Perspective. *Sensors*, vol. 20, no. 12, p. 3358.

Sukhwani, H., Martínez, J.M., Chang, X., Trivedi, K.S. and Rindos, A. (2017). Performance Modeling of PBFT Consensus Process for Permissioned Blockchain Network (Hyperledger Fabric). In: *2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)*, pp. 253–255. IEEE.

Sukhwani, H., Wang, N., Trivedi, K.S. and Rindos, A. (2018). Performance Modeling of Hyperledger Fabric (Permissioned Blockchain Network). In: *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*, pp. 1–8. IEEE.

Sultan, K., Ruhi, U. and Lakhani, R. (2018). Conceptualizing Blockchains: Characteristics & Applications.

Swan, M. (2015). *Blockchain: Blueprint For A New Economy*. " O'Reilly Media, Inc.".

Swan, M. (2017). Anticipating the economic benefits of blockchain. *Technology innovation management review*, vol. 7, no. 10, pp. 6–13.

Swanson, T. (2015). Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems. *Report, available online*.

Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. *First monday*.

Takyar, A. (2019). How to Determine the Cost of Blockchain Implementation? Available at: `https://www.leewayhertz.com/cost-of-blockchain-implementation/`

Taskinsoy, J. (2019). Blockchain: A Misunderstood Digital Revolution. Things You Need to Know about Blockchain.

Thanujan, T., Rajapakse, R.A.C.P. and Wickramaarachchi, D. (2020). A Review of Blockchain Consensus Mechanisms: State of the Art and Performance Measures. In: *Kotelawala Defence University International Research Conference 2020*, pp. 315 – 326.

Toufaily, E., Zalan, T. and Dhaou, S.B. (2021). A framework of blockchain technology adoption: An investigation of challenges and expected value. *Information & Management*, vol. 58, no. 3, p. 103444.

Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM*, vol. 59, no. 11, pp. 15–17.

van Aken, J.E. and Berends, H. (2018). *Problem Solving in Organizations: A Methodological Handbook for Business and Management Students*. 3rd edn. Cambridge University Press.

Vaughan, W., Bukowski, J. and Wilkinson, S. (2016 June). Chainpoint: A scalable protocol for anchoring data in the blockchain and generating blockchain receipts.

Veinović, M. *et al.* (2021). Comparative Analysis of Consensus Algorithms in Blockchain Networks. In: *Sinteza 2021-International Scientific Conference on Information Technology and Data Related Research*, pp. 128–133. Singidunum University.

Versteeg, G. and Bouwman, H. (2006). Business architecture: A new paradigm to relate business strategy to ICT. *Information systems frontiers*, vol. 8, no. 2, pp. 91–102.

Vo, H.T., Kundu, A. and Mohania, M.K. (2018). Research Directions in Blockchain Data Management and Analytics. In: *EDBT*, pp. 445–448.

Vujičić, D., Jagodić, D. and Ranđić, S. (2018). Blockchain Technology, Bitcoin, and Ethereum: A Brief Overview. In: *2018 17th international symposium infoteh-jahorina (infoteh)*, pp. 1–6. IEEE.

Vukolić, M. (2015). The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. In: *International workshop on open problems in network security*, pp. 112–125. Springer.

Wang, H., Chen, K. and Xu, D. (2016). A maturity model for blockchain adoption. *Financial Innovation*, vol. 2, no. 1, pp. 1–5.

Wang, W., Hoang, D.T., Hu, P., Xiong, Z., Niyato, D., Wang, P., Wen, Y. and Kim, D.I. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. *Ieee Access*, vol. 7, pp. 22328–22370.

Weill, P. and Vitale, M. (2001). *Place to Space: Migrating to eBusiness Models*. Harvard Business School Publishing Corporation.

Winter, R. and Fischer, R. (2006). Essential Layers, Artifacts, and Dependencies of Enterprise Architecture. In: *2006 10th IEEE International Enterprise Distributed Object Computing Conference Workshops (EDOCW'06)*, pp. 30–30. IEEE.

Wüst, K. and Gervais, A. (2018). Do You Need A Blockchain? In: *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pp. 45–54. IEEE.

Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A.B. and Chen, S. (2016). The Blockchain as a Software Connector. In: *2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)*, pp. 182–191. IEEE.

Yaga, D., Mell, P., Roby, N. and Scarfone, K. (2019). Blockchain Technology Overview.

Yang, W., Garg, S., Huang, Z. and Kang, B. (2021). A decision model for blockchain applicability into knowledge-based conversation system. *Knowledge-Based Systems*, vol. 220, p. 106791.

Yu, Z., Liu, X. and Wang, G. (2018). A Survey of Consensus and Incentive Mechanism in Blockchain Derived from P2P. In: *2018 IEEE 24th international conference on parallel and distributed systems (ICPADS)*, pp. 1010–1015. IEEE.

Zarvić, N. and Wieringa, R. (2014). An Integrated Enterprise Architecture Framework for Business-IT Alignment. *Designing Enterprise Architecture Frameworks: Integrating Business Processes with IT Infrastructure*, vol. 63, no. 9.

Zhai, S., Yang, Y., Li, J., Qiu, C. and Zhao, J. (2019). Research on the Application of Cryptography on the Blockchain. In: *Journal of Physics: Conference Series*, vol. 1168, p. 032077. IOP Publishing.

Zhang, C., Wu, C. and Wang, X. (2020). Overview of Blockchain Consensus Mechanism. In: *Proceedings of the 2020 2nd International Conference on Big Data Engineering*, pp. 7–12.

Zhao, J.L., Fan, S. and Yan, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue.

Zheng, P., Zheng, Z., Luo, X., Chen, X. and Liu, X. (2018*a*). A Detailed and Real-time Performance Monitoring Framework for Blockchain Systems. In: *2018 IEEE/ACM 40th International Conference on Software Engineering: Software Engineering in Practice Track (ICSE-SEIP)*, pp. 134–143. IEEE.

Zheng, Z., Xie, S., Dai, H.-N., Chen, X. and Wang, H. (2018*b*). Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375.

Appendix A: Additional Information

A.1 Performance Metrics

Table A.1 presents the performance metric values for a range of blockchain solutions and performance metrics. It should be noted that the solutions presented are more nuanced than what they may seem, which explains the reason for the discrepancies that may be present between seemingly identical solutions.

Table A.1: Performance Metric Values for Specific Blockchain Configurations

Configuration and Source	Throughput	Latency	Scalability	Success Rate	TPC	TPMS	TPDIO	TPND
Hyperledger Fabric: permissioned, pBFT (Kuzlu *et al.*, 2019)	200 tps	0.16 s	100 000					
	40 tps (read and write) or 220 tps (read)	1.4 s (read and write) or 0.3 s (read)						
Hyperledger Fabric: permissioned, pBFT (Sukhwani *et al.*, 2018)	800 blocks per hour	16.5 ms	100					
Hyperledger Fabric 1.4.4: permissioned, pBFT (Dabbagh *et al.*, 2020)	28 tps	1.2 s		100%				

Continued on next page

Continued from previous page

Configuration and Source	Throughput	Latency	Scalability	Success Rate	TPC	TPMS	TPDIO	TPND
Ethereum 1.2.1: permissionless, PoW (Dabbagh *et al.*, 2020)	17 tps	4.8 s		100%				
Ethereum: permissioned, PoW (Monrat *et al.*, 2020)	82 tps	120 s	24					
Hyperledger Fabric: permissioned, pBFT (Monrat *et al.*, 2020)	200 tps	5 s	12					
Hyperledger Fabric: permissioned, pBFT (Zheng *et al.*, 2018*a*; Kombe *et al.*, 2018)	600 tps				2.65	4.28	0.14	0.101
Ethereum: permissionless, PoW (Zheng *et al.*, 2018*a*; Kombe *et al.*, 2018)	5.6 tps				0.002	0.011	0.27	0.222
Hyperledger Fabric: permissioned, pBFT (Maharjan, 2018)	300 tps							

Continued on next page

Continued from previous page

Configuration and Source	Throughput	Latency	Scalability	Success Rate	TPC	TPMS	TPDIO	TPND
Hyperledger Fabric: permissioned, pBFT (Bergman *et al.*, 2020)		424 ms	20					
Hyperledger Fabric: permissioned, pBFT (Ruan *et al.*, 2021)	1294 tps	3500 ms						
Hyperledger Fabric: permissioned, pBFT (Khan *et al.*, 2022)	31.7 tps	19.66 s						
Permissioned, pBFT (Alqahtani & Demirbas, 2021)	600 tps	160 ms						
Tendermint: PoS (Alqahtani & Demirbas, 2021)	150 tps	460 ms						
PoW (Litke *et al.*, 2019)	3 - 60 tps	2 - 60 min						
DPoS (Litke *et al.*, 2019)	4000 - 9000 tps	6 min						
PoS (Litke *et al.*, 2019)	5 - 1000 tps	2 s - 5 min						

Continued on next page

Continued from previous page

Configuration and Source	Throughput	Latency	Scalability	Success Rate	TPC	TPMS	TPDIO	TPND
pBFT (Litke *et al.*, 2019)	10 000 tps	15 - 20 s						
Hyperledger Fabric: permissioned, pBFT (Hao *et al.*, 2018)	534.87 tps	78.36 s						
Ethereum: permissionless, PoW (Hao *et al.*, 2018)	129.62 tps	1296.73 s						

A.2 Cost Metrics

The costs below are the estimated average costs for certain cost elements identified from Table 2.19 obtained from Gopalakrishnan *et al.* (2021), Takyar (2019), and Lielacher (2019). All costs were identified and obtained in United States Dollar (USD) and have been converted to South African Rand (ZAR) using the average exchange rate of 15.814 (ZAR/USD) for the month of June 2022 and the final value is rounded to the nearest ten to be succinct. Furthermore, older data is adjusted by using the simple interest formula presented in Equation 9 with an average inflation rate of 5.5% as identified in Bechard (2021).

$$A = P \cdot (1 + i \cdot t) \tag{9}$$

Where A is the final amount, P is the original amount, i is the inflation rate, and t is the time in years since the estimate.

Table A.2: Blockchain Cost Ranges

Cost Element	Cost Range
Consultant fees	R920/hr - R3680/hr (minimum of 10 hours)
White paper cost	R27 630 - R921 170
Prototype development	R552 700
Freelance Blockchain Developer	R1490/hr - R1840/hr
Smart contract development	R55 270 - R552 700
User interface development	R9210 - R644 820
Cryptocurrency/Tokens creation (existing or new)	R184 230 - R921 170
Security (sales, cyber)	R1 105 400
Legal costs	R184 230
Quality assurance agency costs	R110 540
Quality assurance individual costs	R21 560
Public blockchain deployment (3rd party services)	R0.18/transaction + R13 820/month
Private blockchain deployment (3rd party services)	R27 630/month

With a focus on blockchain solutions for organizations, the scenarios in Table A.3 below focus on private blockchain solutions. The quotes were obtained from Leewayhertz (2019) and all costs are converted from USD to ZAR using the average exchange rate of 15.814 (ZAR/USD) for the month of June 2022 and the final value is rounded to the nearest ten to be succinct.

Table A.3: Cost of Different Blockchain Implementation Scenarios

Scenario 1 – new blockchain platform, private, financial transactions, complex cloud computation, mobile application, website interface, administrator interface, immediate development, no PoC (straight to deployment), 10 user types
Development Costs – R2 933 500 to R4 609 780 Estimated Time – 53 weeks Consulting and Design Costs – R318 490 to R352 020 Third-party Monthly Cost – R62 860
Scenario 2 – integrate with existing product (development platform), private, no financial transactions, no cloud computation, administrator interface, normal development speed, PoC, 1 user type
Development Costs – R586 700 to R921 960 Estimated Time – 11 weeks Consulting and Design Costs – R63 700 to R70 400 Third-party Monthly Cost – R12 570
Scenario 3 – integrate with existing product (development platform), private, financial transactions, third-party services used, mobile application, website interface, administrator interface, normal speed of development, PoC, 4 user types
Development Costs – R1 737 960 to R2 731 080 Estimated Time – 31 weeks Consulting and Design Costs – R188 690 to R208 560 Third-party Monthly Cost – R37 240

Continued on next page

Continued from previous page

Scenario 4 – new blockchain platform, private, no financial transactions, third-party services used, administrator interface, website interface, mobile application, normal development speed, PoC, 4 user types
Development Costs – R1 295 170 to R2 035 260 Estimated Time – 23 weeks Consulting and Design Costs – R140 620 to R155 420 Third-party Monthly Cost – R27 750
Scenario 5 – integrate with existing product (development platform), private, no financial transactions, third-party services used, mobile application, website interface, administrator interface, normal development speed, PoC, 4 user types
Development Costs – R1 184 470 to R1 861 310 Estimated Time – 21 weeks Consulting and Design Costs – R128 600 to R142 140 Third-party Monthly Cost – R25 380

Appendix B: Framework Design

B.1 Framework Design Iterations

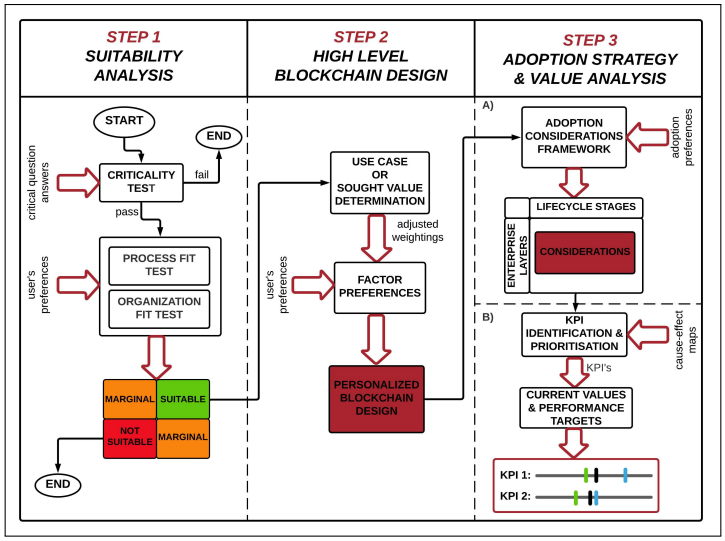


Figure B.1: Blockchain Assessment Framework First Iteration

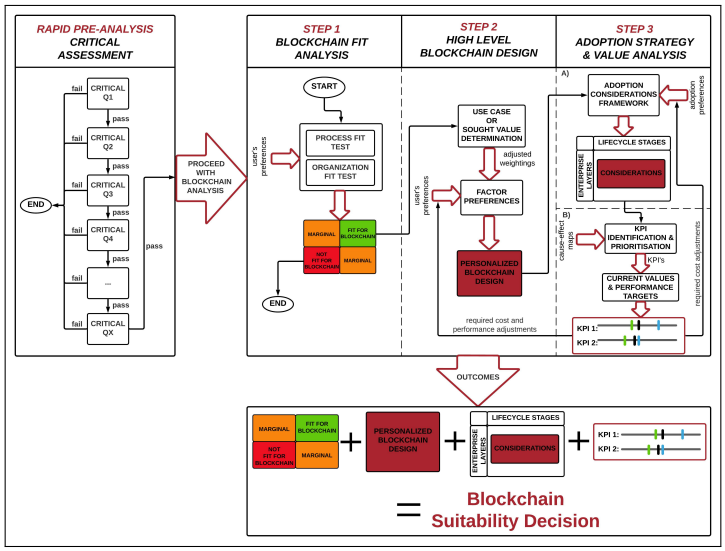


Figure B.2: Blockchain Assessment Framework Second Iteration

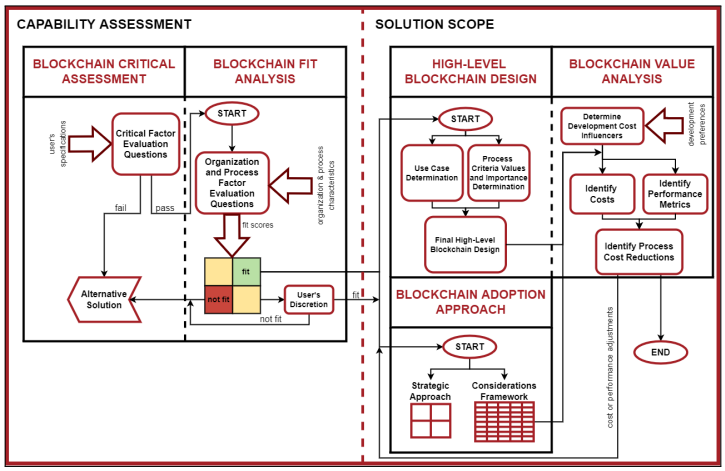


Figure B.3: Blockchain Assessment Framework Third Iteration

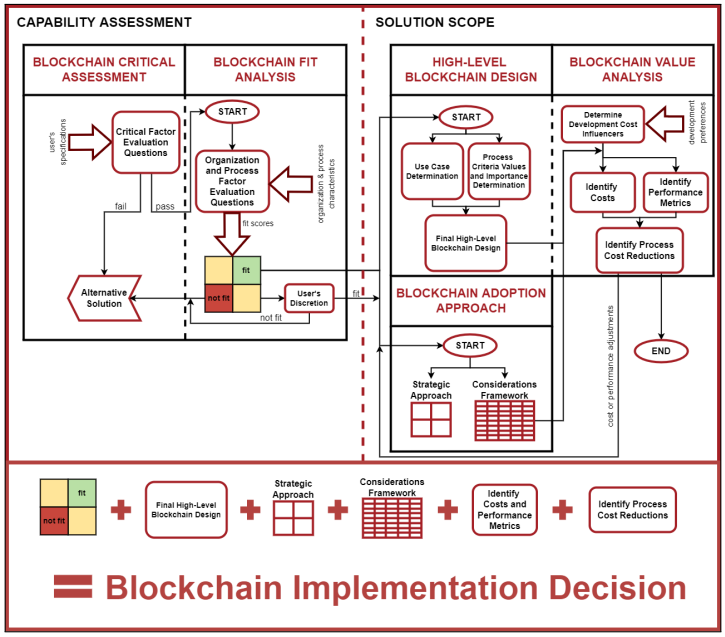


Figure B.4: Blockchain Assessment Framework Fourth Iteration

Appendix C: Framework Inputs

C.1 Blockchain Critical Assessment Inputs

Table C.1: Blockchain Critical Assessment Inputs

Critical Factor	Evaluation Question	Company Answer
Data Store/Exchange	Do you need to store or exchange data?	Yes
Multiple Distributed Parties	Are there multiple parties inputting, updating, and reading information from distributed locations?	Yes
Validated Transactional Data	Are exchanges/transactions involved or is the data transactional and must these transactions be validated?	Yes
Lack of Trust	Is there a lack of trust or conflicting interests among involved parties?	No
Lack of a Trusted Intermediary	Is there a lack of a trusted intermediary or need/want to remove them?	No
Consistent Set of Rules	Can a consistent set of rules help achieve the process outcome?	Yes
Consistent Governing Rules	Will the governing rules be consistent over time?	Yes
Interrelated Transaction History	Is transactions history required and are transactions dependent or interrelated?	Yes
Mapping Party Transactions	Must parties be mapped to their transactions or do transactions have increased value when claimed by a participant?	Yes
Transparency Importance	Is transparency of the transactions a beneficial feature?	Yes
Immutability and Auditability Importance	Is an immutable, auditable record of transactions beneficial?	Yes
Censorship or Attack Reduction	Can a distributed infrastructure reduce the risk of censorship or attack?	Yes

C.2 Blockchain Fit Analysis Inputs

Table C.2: Organizational Fit Analysis Inputs

Domain	Organizational Factor	Evaluation Question/Statement	Company Answer
Critical	Administrative Authority Support	The administrative authority supports blockchain experimentation.	70
	Financial Support	The financial means are available for blockchain experimentation and implementation.	60
	Legal/ Regulatory Framework	The legal/regulatory framework allows for blockchain experimentation and implementation within this industry/organization.	75
Core Expertise	Managerial Capabilities	The managerial capabilities are available for blockchain experimentation and implementation.	60
	Blockchain Complexity	The organization comprehends blockchain's complexity.	50
	Risk Aversity	The organization is risk averse with IT innovation experimentation and implementation.	60
	IT Capabilities	The organization has the IT capabilities or the ability to outsource for blockchain experimentation and implementation.	80
	Blockchain Enthusiast	Is there a blockchain enthusiast within the organization that understands blockchains and is willing to experiment with and implement it?	Yes

Continued on next page

Continued from previous page

Domain	Organizational Factor	Evaluation Question/Statement	Company Answer
Core Expertise	Technological Uncertainty	The organization is capable of handling technological uncertainty linked with blockchain applications.	70
Operation	Interoperability	The organization does not use a particular set of data in multiple different network systems.	30
	Decentralized Characteristics	The organization is willing to decentralize data storage.	60
Willingness	Top-management Dedication	The organization's top-management is dedicated to blockchain experimentation and implementation.	50
	Collaborating Parties Willingness	Potential stakeholders are willing to participate in blockchain experimentation and implementation that is led by the organization.	70
	Inter-organizational Trust	Potential stakeholders trust the organization to facilitate data exchange/registration.	80
	External Influence to Adopt	There are external influences on the organization to adopt blockchain (pressure, incentives, penalties, etc.).	40
Industry	Similar Use Cases in the Market	Are there existing use cases similar to the one being explored?	Yes
	Collaborating Parties Competencies	Potential stakeholders are competent to experiment with and implement blockchain.	50

Continued on next page

Continued from previous page

Domain	Organizational Factor	Evaluation Question/Statement	Company Answer
Industry	Fraud Prevalence	Is fraud prevalent in your industry or organization?	No

Table C.3: Process Fit Analysis Inputs

Domain	Process Factor	Evaluation Question	Company Answer
Users	Predictable Actor Behaviour	How predictable is the data input and behaviour of potential actors in the network?	60
	Limited Trust in Current Process	Do current actors lack trust in the current process?	30
	Desired User Control Over Data	Will potential stakeholders want to store their data locally for better control in the process?	65
	High Importance of User Experience	What is the level of importance for the user's experience and ease of use in the process?	80
	Transparency Required	Is it required for transparent data to exist between potential stakeholders involved in the network?	70
Process Facilitation	Peer-to-Peer Potential	Is there potential for the process to be facilitated by peer-to-peer interactions?	Yes

Continued on next page

Continued from previous page

Domain	Process Factor	Evaluation Question	Company Answer
Process Facilitation	Low Interest of Organization Being Intermediary	Is there a low interest of the organization being the intermediary in this process?	No
	High Availability of Bandwidth	Does the network have enough available bandwidth and computing power for the required specifications?	80
	Low Throughput of Data	What is the frequency of transactions experienced?	Medium
	Current Laborious Human Facilitations	Is human labour required to facilitate the process?	Yes
	Workflow Simplification	Will distributed ledger technology help simplify the workflow of the process?	60
Hardware/ Software	Legacy Systems in Place	What is the level of the legacy systems that are currently in place?	Brownfield
	Interface Differentiation	Do all involved parties have their own interfaces for the process or are all interfaces standardized?	Multiple
Control	Low Institutionalized Environment	Is there a lack of bureaucracy in place for this process?	30
	Network Ability to Implement Technology Standards	Do the potential stakeholders adapt well to new technology standards?	Yes

Continued on next page

Continued from previous page

Domain	Process Factor	Evaluation Question	Company Answer
Control	Importance of Control Over the Infrastructure	How reasonable is it to have a lack of control over the infrastructure of the network?	70
Data	Data Complexity	Are there multiple data formats involved in the process?	Multiple
	Low Trust in Current Data Storage	Is there a lack of trust or information asymmetry in the data storage of the current system?	No
	Traceability Required	Is it required to be able to trace who has accessed and created data in the network?	80
	Data Integrity	What level of data integrity is required for the process?	90
	Interoperability Possibility	Is the data from the current process involved in other processes? Is there one or many different uses of the data?	Multiple
	Inter-organizational Information Exchange	Is there data exchange between multiple organizations or distributed branches of the same organization?	Yes
	Transaction Dependency	Are there interactions between the transactions created by the potential stakeholders of the network?	Yes
	Asset Digitization Potential	How much potential is there for the assets involved in the transactions/exchanges to be digitized?	80
	Privacy of Sensitive Data	Is there process information that is privacy sensitive?	50

C.3 High-Level Blockchain Design Inputs

Table C.4: Blockchain High-Level Design Inputs

Process Characteristic	Answer	Importance Rating
Use Case	Smart Contracts	N/A
Energy Efficiency	3	0.5
Latency Performance	4	0.9
Throughput Performance	4	1.0
Hardware Dependence	3	0.6
Centralization	3	0.8
Scalability (validating nodes)	4	0.8
Scalability (client nodes)	5	0.8
Security/Fault Tolerance	5	1.0
Settlement Finality	Deterministic	1.0
Incentivization	No	0.5
Consensus Participation	Permissioned	0.7
Data Accessibility (read)	Private	1.0
Data Accessibility (write)	Private	1.0
Actor Identity (clients)	Known	1.0
Actor Identity (validators)	Known	1.0
Organization Control	3	0.8
External Transparency	1	1.0
Immutability	5	1.0

C.4 Blockchain Adoption Approach and Value Analysis Inputs

Table C.5: Blockchain High-Level Design Inputs

Analysis Item	Description	Answer
Development Resources	How would you address developing the blockchain solution (agency, in-house, freelancers)?	Agency
Development Platform	Will the blockchain solution be built from scratch or integrated with a current system or using a blockchain development platform (e.g. Ethereum or Hyperledger Fabric)?	Development Platform
Network-User Interaction	How will users of the network interact with it (web interface, mobile application, admin interface, or combination)?	Mobile Application and Web Interface
Proof of Concept	Will the blockchain solution require a proof of concept?	Yes
Operation Complexity	Will the blockchain solution be its own IS or will it be required to interact with multiple IS's outside itself?	Multiple
Blockchain Deployment	How will the blockchain solution be deployed (on-premises, third-party cloud, or hybrid)?	Third-party Cloud
Financial Transactions	Will the selected process require the use of financial transactions and the subsequent exchange of value between parties?	No
Development Speed	What is the urgency with which the blockchain solution needs to be developed?	Normal development speed

Continued on next page

Continued from previous page

Analysis Item	Description	Answer
Number of User Types	How many different types of users will be using the solution?	Up to four
Market Dominance	Would you consider the organization to have higher or lower market dominance with its current position in the market?	Lower
Standards and Regulatory Barriers	Would you consider the standards and regulatory barriers to be higher or lower within your industry?	Higher
System Changeover	What system changeover method would be employed for system migration or replacement (phased implementation, parallel running, or direct changeover)?	Phased Implementation
Performance Metrics	What performance metrics are relevant to the organization's use case?	Throughput, latency (<500ms), scalability (1500 users), simultaneous transactions, and queue length
Cost Items	What cost items would be relevant to the organization's use case?	Consulting, development, design, quality assurance, deployment and migration, project management, infrastructure, storage costs, continuous integration, and maintenance and upgrading
Cost Reductions	What cost reductions would be relevant to the organization's use case?	networking costs, transaction costs, policing and enforcement costs, verification costs, debugging costs, automation, and search and information costs