Univerza *v Ljubljani*
Fakulteta *za gradbeništvo*
in geodezijo

MUAMMER SEMIH SONKOR

COLLABORATIVE BIM ENVIRONMENTS: MITIGATING CYBERSECURITY THREATS IN THE DESIGN PHASE

SODELOVALNA OKOLJA BIM: BLAŽENJE KIBERNETSKIH VARNOSTNIH GROŽENJ V FAZI NAČRTOVANJA

BIM A+ European Master in Building Information Modelling

Master thesis No.:

Supervisor:
Prof. Žiga Turk, PhD.

Ljubljana, 2020

Co-funded by the Erasmus+ Programme of the European Union

ERRATA

Page	Line	Error	Correction

»This page is intentionally blank«

BIBLIOGRAFSKO – DOKUMENTACIJSKA STRAN IN IZVLEČEK

UDK: **004.056.53:69.01(043.3)**

Avtor: **Muammer Semih Sonkor**

Mentor: **prof. dr. Žiga Turk**

Somentor:

Naslov: **Sodelovalna okolja BIM: Blaženje kibernetskih varnostnih groženj v fazi načrtovanja**

Tip dokumenta: **magistrsko delo**

Obseg in oprema: **74 str., 23 sl., 4 pregl.**

Ključne besede: **BIM, dizajn, kibernetska varnost, veriženje blokov, sodelovanje, skupna podatkovna okolja, IPD, decentralizirana hramba**

Izvleček:

Gradbeništvo je sredi digitalne preobrazbe. Ključno vlogo pri njej ima gradbeniško informacijsko modeliranje (BIM). Omogoča bolj povezano, sodelovalno in učinkovito okolje za vse faze graditve objektov. Vendar izboljšano sodelovanje in enostaven dostop do podatkov povečujeta tveganje napadov na kibernetsko varnost s strani notranjih in zunanjih povzročiteljev, kar ogroža občutljive informacije o projektu. Ta študija se osredotoča na fazo načrtovanja, saj vprašanja kibernetske varnosti v okoljih BIM v tej fazi dosegajo vrhunec zaradi velikega števila udeležencev in velikega obsega novih informacij.

Čeprav obstajajo številni okvirji kibernetske varnosti, ki jih postavljajo mednarodne in nacionalne organizacije po vsem svetu, se nobeden od njih posebej ne osredotoča na fazo načrtovanja v gradbeništvu. Zato ta študija obravnava štiri splošne dokumente o kibernetski varnosti, da bi izbrala najprimernejšo možnost za BIM okolja. Izbran je Okvir za ocenjevanje kibernetske varnosti Nacionalnega centra za kibernetsko varnost (NCSC), ki je v nadaljevanju prilagojen orodjem, postopkom in zainteresiranim deležnikov iz faze načrtovanja. Opredeljena so glavna vprašanja kibernetske varnosti v kontekstu načrtovanja v BIM okolju in podana priporočila. Proti koncu študije je predlagana kibernetsko varna arhitektura izmenjave podatkov, ki uporablja tehnologijo veriženja podarkovnih blokov (blockchain) in decentraliziran pristop za shranjevanje podatkov. Prav ta decentralizirani mehanizem za shranjevanje podatkov in uporaba blockchaina tehnologije v predlagani arhitekturi pristop razlikuje od drugih študij.

»This page is intentionally blank«

BIBLIOGRAPHIC– DOCUMENTALISTIC INFORMATION AND ABSTRACT

UDC: **004.056.53:69.01(043.3)**

Author: **Muammer Semih Sonkor**

Supervisor: **Prof. Žiga Turk, PhD.**

Cosupervisor:

Title: **Collaborative BIM Environments: Mitigating Cybersecurity Threats in the Design Phase**

Document type: **Master Thesis**

Scope and tools: **74 p., 23 fig., 4 tab.**

Keywords: **BIM, Design, Cybersecurity, Blockchain, Cybersecurity Assessment, Collaboration, CDE, IPD, Decentralised Storage**

Abstract:

The construction industry is going through a digital transformation, and Building Information Modelling (BIM) has a vital role in the digitalisation process. It creates a more connected, collaborative, and efficient environment for all phases of construction. However, improved collaboration and easy access to data increase the risk of cybersecurity attacks from internal and external threat agents against sensitive project information. This study focuses on the design phase since cybersecurity issues in BIM environments peak in this stage with the increasing number of stakeholders involved and intensive information creation.

Even though there are many cybersecurity frameworks published by international and national organisations around the world, none of them particularly focuses on the design phase of construction projects. Therefore, this study reviews four generic cybersecurity documents to select the most suitable option for adapting into the BIM environment. As a result of the review, Cyber Assessment Framework from the National Cyber Security Centre (NCSC) is selected to proceed with the adaptation considering the tools, processes, and stakeholders involved in the design phase. As a result of this adaptation, the main cybersecurity issues in the BIM-design context are identified, and suggestions are provided. In the last part of the study, a data sharing architecture that makes use of Blockchain Technology (BCT) and decentralised storage approach is proposed to manage some of the addressed cybersecurity problems. Decentralised data storage mechanism and the use of Blockchain (BC) in the proposed architecture differentiates it from previous studies.

»This page is intentionally blank«

ACKNOWLEDGEMENTS

I would like to express my gratitude to my thesis supervisor, Prof. Dr. Žiga Turk, for his support during the development of my research. Also, I would like to thank all our professors who have put great effort during the coursework. I would also like to thank Layla Mendes for her guidance on research methodology.

Last but not least, I would like to thank my family and friends for their love and support. It would not be possible to complete my studies without their endless support and motivation during the COVID-19 pandemic and quarantine.

»This page is intentionally blank«

TABLE OF CONTENTS

INDEX OF TABLES

INDEX OF FIGURES

INDEX OF ACRONYMS

AECO	Architecture, Engineering, Construction and Operations
AI	Artificial Intelligence
AIA	The American Institute of Architects
BASIR	The Built Asset Security Information Requirements
BASM	Built Asset Security Manager
BASMP	The Built Asset Security Management Plan
BASS	The Built Asset Security Strategy
BbCN	BIM-based Construction Networks
BC	Blockchain
BCT	Blockchain Technology
BEP	BIM Execution Plan
BIM	Building Information Modelling
BSI	The British Standards Institution
BYOD	Bring Your Own Device
CDE	Common Data Environment
CIA	Confidentiality, Integrity, and Availability
CISA	The Cybersecurity and Infrastructure Security Agency
CMAA	The Construction Management Association of America
CMAR	Construction Management at Risk
CPS	Cyber-Physical System
DB	Design-Build
DBB	Design-Bid-Build
DDoS	Distributed Denial of Service
DoS	Denial of Service
DPoS	Delegated Proof of Stake
ECDSA	Elliptic Curve Digital Signature Algorithm
ENISA	The European Union Agency for Cybersecurity
GTAG	Global Technology Audit Guide
ICT	Information and Communication Technologies
IEC	The International Electrotechnical Commission
IET	The Institute of Engineering and Technology
IFC	Industry Foundation Classes
IIA	The Institute of Internal Auditors
IoC	Indicators of Compromise
IoT	Internet of Things
IPD	Integrated Project Delivery
IPFS	InterPlanetary File System
ISO	The International Organization for Standardization
IT	Information Technology
JSON	JavaScript Object Notation
ML	Machine Learning
MSP	Membership Service Provider
NBS	National Building Specification
NCSC	The National Cyber Security Centre
NIST	The National Institute of Standards and Technology
P2P	Peer-to-Peer

PAS	Publicly Available Specification
PBFT	Practical Byzantine Fault Tolerance
PC	Personal Computer
PoET	Proof of Elapsed Time
PoS	Proof of Stake
PoW	Proof of Work
RIBA	The Royal Institute of British Architects
SB/IMP	The Security Breach/Incident Management Plan
SFA	Single-Factor Authentication
SGX	Software Guard Extensions
SHA	Secure Hash Algorithm
STEP	Standard for the Exchange of Product model data
SWOT	Strengths, Weaknesses, Opportunities, Threats
UK	The United Kingdom
UPS	Uninterruptable Power Supply
USA	The United States of America
XML	Extensible Markup Language

1 INTRODUCTION

This chapter provides an overview of the thesis by going through focus points and giving highlights. It concisely describes the background of the research and the current situation of the industry from building information modelling and cybersecurity perspectives. The problem statement, main goals and objectives, the methodology followed to obtain findings and results, and the structure of the thesis are presented in this chapter.

1.1 Research Background

Disruptive technologies in the last decades have accelerated the digital transformation and automation in all industries, including Architecture, Engineering, Construction and Operations (AECO) industry. Some examples for recently developing and trending technologies are Artificial Intelligence (AI), Internet of Things (IoT) and Machine Learning (ML), and they are mostly data-driven technologies that require the establishment of databases and data exchange networks. A key technology for the digitalisation of the AECO industry is Building Information Modelling (BIM). It enables a more connected, collaborative, and efficient working environment for design, construction, and operation stages. These advances in digitalisation in the construction industry result in significant savings in time, cost, and quality.

In a world of communication, internet-connected devices, networks, and data storage systems; information becomes more accessible than ever, and in some cases, for unauthorised third parties by malicious attacks. Cybersecurity aims to defend such systems from attacks and to minimise the risk of security compromises by utilising additional measures and suggesting best practices for users. There have been many studies defining information security principles, and the most prominent and widely accepted one is CIA triad which stands for confidentiality, integrity, and availability [1]. Even though CIA triad covers the main aspects of information security, there are more comprehensive models developed in years. One of these alternative models, developed by Parker, is Parkerian Hexad which adds three more attributes on top of CIA triad: authenticity, possession/control, and utility [2].

Models mentioned above help to analyse systems—from a cybersecurity perspective —in a more organised way and within a framework; therefore, this research employs these information security models in order to disclose possible vulnerabilities in BIM environment. Especially for large scale and sensitive projects, good security can provide a competitive advantage to design and construction companies as well as taking part in the international construction market [3]. Finding possible solutions to improve security and to mitigate cyber threats is the main objective of this research considering the significance of information security for companies competing for high profile construction projects.

1.2 Problem Statement

Collaborative nature of BIM requires the use of centralised networks, ideally providing uninterrupted data exchange and robust communication between stakeholders. The utilisation of centralised networks during the life cycle of construction and inevitable need to share data with subcontractors, vendors and client brings the risk of being attacked by external and internal threat agents or having systems failures [4], and a potential interruption in BIM workflow as a result. Moreover, an unauthorised third party accessing to the shared repository and BIM data might cause loss or theft of confidential data of sensitive facilities such as prisons, embassies and army bases, and most of the Critical National Infrastructure as stated by the Institute of Engineering and Technology (IET) [5].

The use of Common Data Environments (CDE) consolidates the collaborative aspect of BIM working environment. National Building Specification (NBS) defines the CDE as "a central repository where construction project information is housed" [6, Para. 1]. Having all the project information including 3D models, time schedules, cost calculations, contracts, and quality documents in digital formats, stored in a central repository, enables all stakeholders to access information—that they are authorised to—conveniently. Centralising the data does not only provide easy access but also increases exposure, which requires additional measures to apply. According to PAS 1192-2:2013 [7], the information originator owns the information. Keeping the authenticity of the information as well as integrity is essential for providing a tamper-proof data flow. Detailed analysis of CDE from a security point of view is executed in Chapter 2 in order to point out the weak spots.

Design is the phase that frequent changes made to geometry and metadata of models in a collaborative BIM environment through CDE. In this environment, sharing design documents with required stakeholders becomes effortless compared to the conventional systems used in the construction industry; however, it also brings additional concerns related to data ownership, change tracking, and unauthorised access to sensitive information. During the design phase of BIM-enabled construction projects; use of various modelling software by different disciplines, the involvement of many designers and other stakeholders, and frequent changes made to models increase the complexity of information security assurance.

There are many international and national information security guidelines, frameworks, and methods published by various organisations across the world. Eighty-six of them are listed in the guidelines published by the European Union Agency for Cybersecurity (ENISA) in November 2018 [8]. Even though some of the documents listed in the ENISA guidelines are industry-specific, there is no framework, particularly pointing out the cybersecurity issues confronted during construction projects.

1.3 Objectives

In this thesis, the following objectives are targeted to be achieved:

- To review cybersecurity threats, actors, and motivations, and to investigate possible solutions to improve security in the design phase of construction projects considering the use of CDEs and BIM tools.
- To define prominent factors in the design stage that should be considered in the cybersecurity risk assessment.
- To review various generic cybersecurity methods and frameworks to select the most convenient option for adaptation into the BIM environment.
- To develop a cybersecurity assessment framework for the design phase of BIM-enabled construction projects based on the selected non-industry specific framework.
- To review Blockchain Technology (BCT) as a solution for ensuring a robust data network, availability of reliable information, and enhanced data integrity and confidentiality.
- To develop a data exchange architecture for the design phase in BIM environment by employing BCT and decentralised storage approach.

1.4 Research Methodology

Research is defined in many different ways by many authors. Kothari [9, p. 1] defines it as “an art of scientific investigation”, Kumar [10] sees it as a way of thinking, and Thomas [11] describes it as “disciplined, balanced inquiry, conducted in a critical spirit”. In this research, considering these definitions, a rigorously disciplined approach for investigation was employed to achieve research objectives.

One of the common research methodology classifications is qualitative vs quantitative research [9]. This thesis employs a qualitative methodology since there are no quantity-based studies and analysis included. For this research, initially, an exhaustive literature review was conducted to gather information from previous research on “cybersecurity”, “cybersecurity in BIM”, “collaboration in BIM environment”, “design workflows in BIM”, and “blockchain technology”. The literature review helped to identify cybersecurity issues from BIM and design perspectives.

After the literature review, cybersecurity methods, standards, and frameworks mentioned in the guideline from ENISA were investigated to find the most suitable ones to review. Considering four months of duration assigned for this master’s thesis, documents to be reviewed were narrowed down to four from eighty-six options in ENISA guidelines. Selected documents were carefully reviewed to find the best matching option for the requirements of this study. The cyber assessment framework from the National Cyber Security Centre (NCSC) is selected to adapt to the BIM and design contexts. For the

adaptation, the main categories of the original framework were kept the same, and each category was handled in three parts: Original, Adaptation, and Discussion. Original gives a summary of the base framework from NCSC; Adaptation tailors the generic concerns to construction design and BIM contexts; Discussion provides suggestions about the adapted cybersecurity concerns.

Lastly, for the proposed architecture in Chapter 4, concepts related to BCT were investigated to develop ideas as a solution to cybersecurity issues in BIM environments. As a result of the investigation, the following concepts and technologies were found useful to employ in the proposed architecture besides BCT:

- Decentralised data storage,
- Hashing by using secure hash algorithms (SHA-2 was used in this study),
- Merkle tree,
- Super-peer networks,
- Public-key cryptography.

It should be noted that the abovementioned concepts and approaches cannot be considered separately since some of them make use of others as a part of their working mechanism.

1.5 Overview of the Thesis

This thesis is structured in 5 chapters, as explained below:

- **Chapter 1 – Introduction:** This chapter provides a concise overview of the thesis by pointing out the objectives, stating problems, and justifying objectives of the research. Background of the research is presented together with the objectives. Research methodologies followed to reach the goals of the thesis are explained.

- **Chapter 2 – Literature Review:** Previous research is reviewed from the perspective of the thesis objectives. It briefly gives general information about concepts, approaches, and methods employed in the research. Integrated Project Delivery (IPD) approach and Common Data Environments (CDE) are scrutinised from a cybersecurity point of view. Design workflows and stakeholders involved in the design phase are indicated, as well as cybersecurity principles and main threats. The working mechanism of BCT, consensus mechanisms in blockchains (BC), and the related concepts are reviewed to provide background information for the analysis in Chapter 4. This chapter has an intrinsic value in terms of providing detailed knowledge before proceeding with the analysis chapters.

- **Chapter 3 – Cybersecurity Risk Assessment in the Design Phase:** This chapter presents a cybersecurity assessment framework for the design phase of construction projects. A

generic cyber assessment framework is chosen to adapt it to the requirements of the design phase. Providing summarised versions of criteria from the original framework, adapted versions of these criteria, and a discussion on these issues in the BIM-design context is the main objective of this chapter. As a result, main concerns pertaining to the security issues in collaborative BIM environments are addressed.

- **Chapter 4 – Managing Security Issues in the Design Phase With Blockchain Technology:** In this chapter, a data exchange architecture utilising BCT and decentralised storage approach is proposed to manage related security issues addressed in Chapter 3. BIM-design workflows, involved stakeholders, technology tools, and utilised network and database systems are taken into consideration for the development of the schema. It is aimed to see, to what extent BCT can be the solution for enhanced security. A SWOT analysis is performed to show the advantages and disadvantages of the proposed architecture.

- **Chapter 5 – Conclusion:** In this chapter, conclusions made as a result of findings and analysis are stated. It makes a connection between the literature review and the analysis in Chapters 3 and 4. A table showing which cybersecurity concerns indicated in Chapter 3 are solved in Chapter 4 by the proposed architecture and which concerns are remaining. Recommendations for future work are indicated.

2 LITERATURE REVIEW

This chapter presents a detailed literature review focusing on the issues to be investigated in the following chapters. It is aimed to create a foundation with various sources and thoughts of different authors for the assessments and analysis in Chapters 3 and 4. It looks into the use of CDEs and the IPD approach from the perspective of their impacts on collaboration. To make a comprehensive cybersecurity assessment in Chapter 3; workflows and stakeholders involved in the design phase, and main principles of cybersecurity, as well as possible security threats, are pointed out.

2.1 Collaboration and the Design Phase in BIM Environment

With the advent of the Internet and more extensive use of it in years, technologies that support collaboration continue to proliferate in the construction industry [5]. These disruptive technologies have entirely changed the way companies operate. One of the processes that are mostly affected by these innovations is the data exchange process, which is directly pertinent to the subject of this thesis. Enhanced way of exchanging data between stakeholders not only improves the working efficiency but also increases the cybersecurity vulnerabilities. Main elements of data exchange that should be considered in a security context are; people involved in the process and the organisation within the project, the technology used for data exchange, and sensitivity of the shared information.

In BIM-enabled construction projects, work is performed by BIM-based Construction Networks (BbCN), which consists of specialised professionals from various disciplines, performing BIM-related works [12]. The success of BbCN is dependent on the appropriate transmission of information and robust communication between stakeholders [13], which is also critical in maintaining collaboration. In order to provide uninterrupted communication between stakeholders—from different locations in some cases—utilising shared databases for data exchange becomes an inevitable need [14]

BIM targets to enable stakeholders to collaborate at all stages of construction by allowing them to add, remove, modify, or update data when needed [14]. However, from a cybersecurity perspective, one of the primary considerations is people involved in collaborative working environments. In PAS 1192-5:2015, it is indicated as “The employer or asset owner shall appreciate that in respect of a built asset, a holistic approach needs to address security around the aspects of people and process, as well as physical and technological security” [3, p. 7]. Therefore, while enhancing the collaboration between stakeholders, it is crucial to place importance on data governance, which refers to the management of the availability, integrity, and security of data used within an Enterprise [15].

Another aspect of collaboration and data exchange, from cybersecurity lense, is the technology utilised during the project lifecycle. Oraee et al. [12] propose a framework that synthesises five antecedents of collaboration; Context, Team, Process, Task, and Actor. Oraee et al. [12] also present a

study, which demonstrates the percentages of these antecedents focused on by selected previous papers. According to the study, Process has the majority (66%) in terms of being targeted by authors; and it mostly refers to information communication technologies – tools and software, and networks. This result shows the vital importance of technology to support collaboration in BIM environment.

Cloud computing is one of the emerging technologies spawned by the widespread use of the Internet. Microsoft defines cloud computing as "the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale." [16, Para. 1]. It provides an efficient way of data exchange in BIM-enabled projects which accelerates its integration in the AECO industry [17]. On the other hand, the use of cloud computing requires the utilisation of an elaborate security framework, which will provide main elements of information security such as availability, confidentiality, integrity, and authenticity for data [18].

Exchanged data can be sensitive either because of the information type—being related to commercial information, pricing or key negotiating positions—or because of the project itself being sensitive—construction of facilities such as banks, prisons, embassies, army bases [3], [5]. PAS 1192-5:2015 [3] also points out the need for additional security measures in case of having a sensitive built asset near the construction site. Therefore, in collaborative working environments, while dealing with sensitive information either about the project or about involved companies, security procedures become of paramount importance.

In the following sections, two main concepts and approaches are reviewed; Common Data Environment (CDE) and Integrated Project Delivery (IPD). This review not only explains these concepts but also addresses the impacts of them on collaboration in BIM-enabled projects – considering cybersecurity aspects.

2.1.1 Common Data Environment (CDE)

An increasing number of digital documents in BIM environment requires a shared repository to exchange information while avoiding duplications and respecting the ownership of data. The concept of Common Data Environment (CDE) emerged as a result of this need. PAS 1192-2:2013 defines CDE as "Single source of information for any given project, used to collect, manage and disseminate all relevant approved project documents for multi-disciplinary teams in a managed process" [7, p. 3]. This definition indicates the importance of CDE for collaboration in a multi-disciplinary working environment. Moreover, it shows that a single source of information is necessary to manage all the input received from stakeholders more efficiently. Figure 1 is a graphical representation of the concept of CDE.

In a collaborative process, digital models are created with the contribution of several disciplines, which use different BIM-authoring tools. Preidel & Borrmann [19] point out the fact that several guidelines, including PAS 1192-2:2013 [7], suggest the use of discipline-specific modelling, instead of one single model for all disciplines. In this approach, each discipline has complete access only to their sub-model, and this way, it is easier to manage responsibilities and ownership of each discipline's model. The overall federated model consists of these sub-models, which are still owned and maintained by separate disciplines. Sharing and coordination of these sub-models and managing the federated model require a common digital platform, which is defined as CDE by PAS 1192-2:2013 [7].

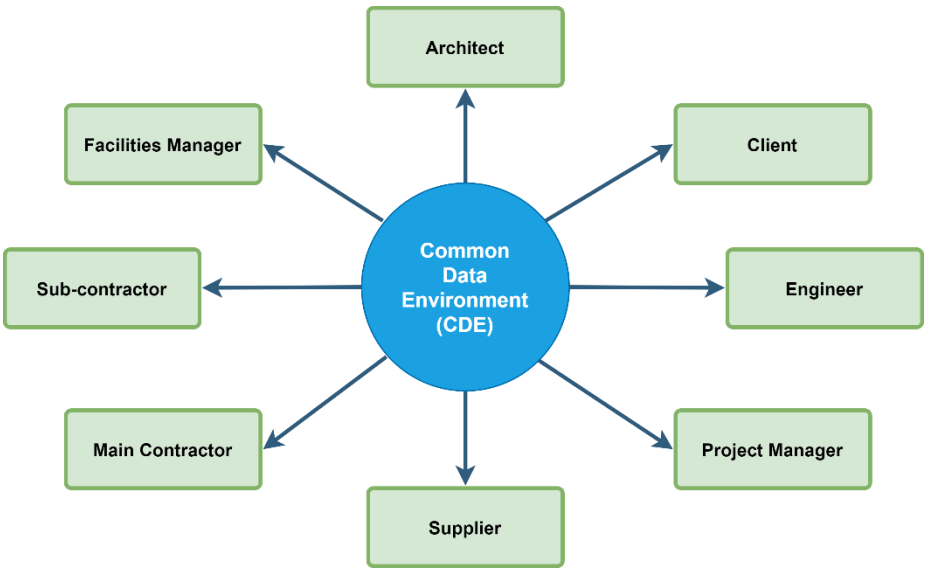

Figure 1: The concept of Common Data Environment (CDE)

Cloud computing is another emerging concept studied by researchers as a solution to collaboration issues in BIM environment. It is defined as on-demand Internet-based resources providing data storage, networks, servers, computing power or software [20]. Cloud computing paradigm and the CDE concept has an intersection because a CDE can use an extranet, a project server, or a cloud-based system as infrastructure [7]. Therefore, the term CDE covers all platforms and infrastructure systems—not only cloud services—as soon as they provide a shared repository to house project documents. Figure 2 shows the relation between CDE and generic cloud storage, and the hardware requirement.

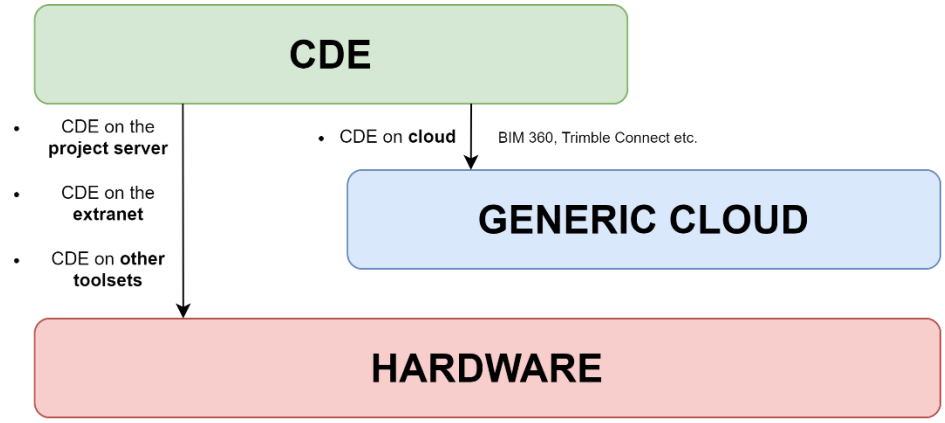

Figure 2: The relation between CDE and generic cloud storage, and the hardware requirement

Allowing various stakeholders to share a common data environment creates uncertainties and vulnerabilities [21]. According to Smith et al. [22], the most significant threats as a result of possible data breaches are loss of intellectual property and confidentiality, which might potentially result in strategic actions taken by competitors. Secure collaboration is still new and developing in the AECO industry [17]. A more detailed analysis of CDE from a cybersecurity perspective is presented in Chapter 4.

2.1.2 Integrated Project Delivery (IPD) for Construction

Integrated Project Delivery (IPD) is another concept that has emerged to minimise project inefficiencies and waste. Many articles have been published researching the benefits of IPD; standards and frameworks have been written as guidelines for implementation [23]. The American Institute of Architects (AIA) published a guide in 2007, "Integrated Project Delivery: A Guide", and defined IPD as "a project delivery approach that integrates people, systems, business structures and practices into a process that collaboratively harnesses the talents and insights of all participants to optimise project results, increase value to the owner, reduce waste, and maximise efficiency through all phases of design, fabrication, and construction" [24, Para. 1]. As indicated in the definition, IPD targets to make the most out of resources—people, material, systems—by innovatively structuring the organisation of the project.

Successful implementation of the IPD approach on a construction project mostly relies on the collaboration of project participants [25]. Therefore, the employment of the IPD approach may not directly lead to more enhanced collaboration. However, the collaborative attitude of the project team supports the success of integrated delivery. Ma et al. [26] argue that the majority of IPD collaboration, in a construction project, happens during the design phase since all stakeholders need to review and understand the design before the construction starts. Moreover, myriad design changes and optimisations increase the complexity of collaboration [26]. This argument justifies the reason for explicitly focusing on the design stage in this thesis.

Ilozor and Kelly [27] remark that there are different opinions as to the relationship between the IPD approach and BIM. Becerik-Gerber and Kensek [28] conducted an extensive survey with professionals from the industry and researchers; as a result, they identified one of the future research themes as "rethinking of IPD as a method to promote BIM" [28, p. 142]. On the other hand, AIA [24] declares that BIM is a tool—not a delivery method—which supports IPD. The majority opinion about this matter is that BIM is a tool which makes the IPD process more robust and efficient [27].

In IPD, there are three main parties of the project: owner, designers, and constructors [24], as shown in Figure 3. This approach involves the constructors in earlier phases of the project, starting from the design stage. This way, constructors' responsibility increases since they are involved from the beginning. They are expected to provide continuous estimates with the changes in the design [24]. IPD targets to remove the boundaries between different disciplines by having shared goals; however, on the other hand, the roles and responsibilities, and the work scope of each team and discipline are well defined [24].

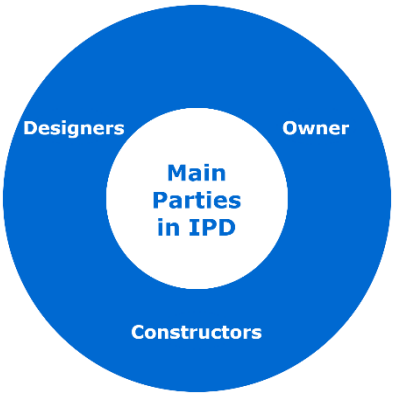

Figure 3: Main parties in IPD according to [24]

IPD approach requires a more careful selection of project participants since there is more information sharing at all stages of the project. Having a large amount of information shared increases concerns regarding confidentiality. Especially in the design phase, where more frequent changes made, cybersecurity aspects become of great importance. Security aspects of IPD will be scrutinised in greater detail in Chapter 4.

2.1.3 Design Phase in Building Information Modelling (BIM)

Construction projects have three main lifecycle phases: design, construction, and operations [29]. Royal Institute of British Architects (RIBA) divides pre-construction phase into five stages: strategic definition, preparation and briefing, concept design, spatial coordination, and technical design in "RIBA Plan of Work" [30] as shown in Figure 4. BIM is a developing and promising process that helps architects, engineers, and constructors at all stages of construction projects, including design stages

[31]. BIM transforms the design process by providing collaborative platforms and tools for efficient workflows [32].

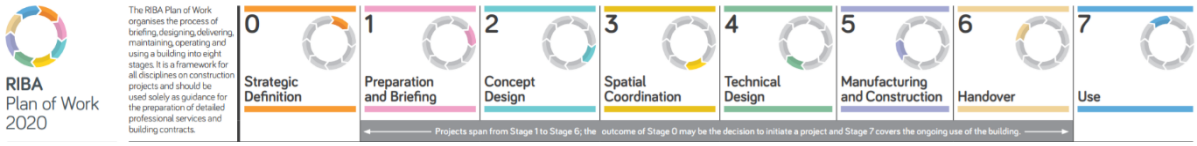

Figure 4: RIBA Plan of Work – Stages of Construction Projects [31]

There are numerous benefits of BIM in the design phase that are stated by various authors in previous research. Azhar [31] investigates the benefits of BIM in his research and shows that the implementation of BIM results in cost and time savings, especially in design stages. Eastman et al. [21] mention these benefits in their influential book, BIM Handbook: A Guide to Building Information Modeling for Owners, Managers, Designers, Engineers, and Contractors, as follows:

- Enhanced design visualisation
- Automating small corrections in case of design changes
- Being able to produce accurate 2D drawings at any stage of the project
- Improved collaboration between different design teams
- Enabling checks against design purposes
- Generating cost estimations in the design stage
- Enhanced sustainability aspects

Figure 5 demonstrates the importance of collaboration in the earlier stages of the project. Shifting the complete collaboration to early stages enables earlier actions in design; therefore, collaborators have the chance to make better decisions resulting in cost efficiency [33]. On the other hand, Figure 5 also shows that the most damage due to cyber-attacks may occur in the earlier stages if collaborative design effort is shifted to the earlier phases of the project.

Even though BIM is not software—it is a process of collaboration, communication, and representation [34]—, advancements in technology play a crucial role in its development. Eastman et al. state that "BIM is not a thing or a type of software but a human activity that ultimately involves broad process changes in construction" [21, p. vii]. Parametric modelling is one of the methods empowered by the development of information technologies in design [35]. It allows representing objects without being constrained to fixed geometry and non-geometry properties while designing, and this way, automatic adaptation of the model to changing contexts becomes possible [21]. Software developing companies have contributed to a great extent to the progress of BIM-enabled design. Autodesk Revit, ArchiCAD, Tekla, Sketchup, Vectorworks, and Rhino are some of the leading BIM modelling software commonly used in the design stages of projects [36].

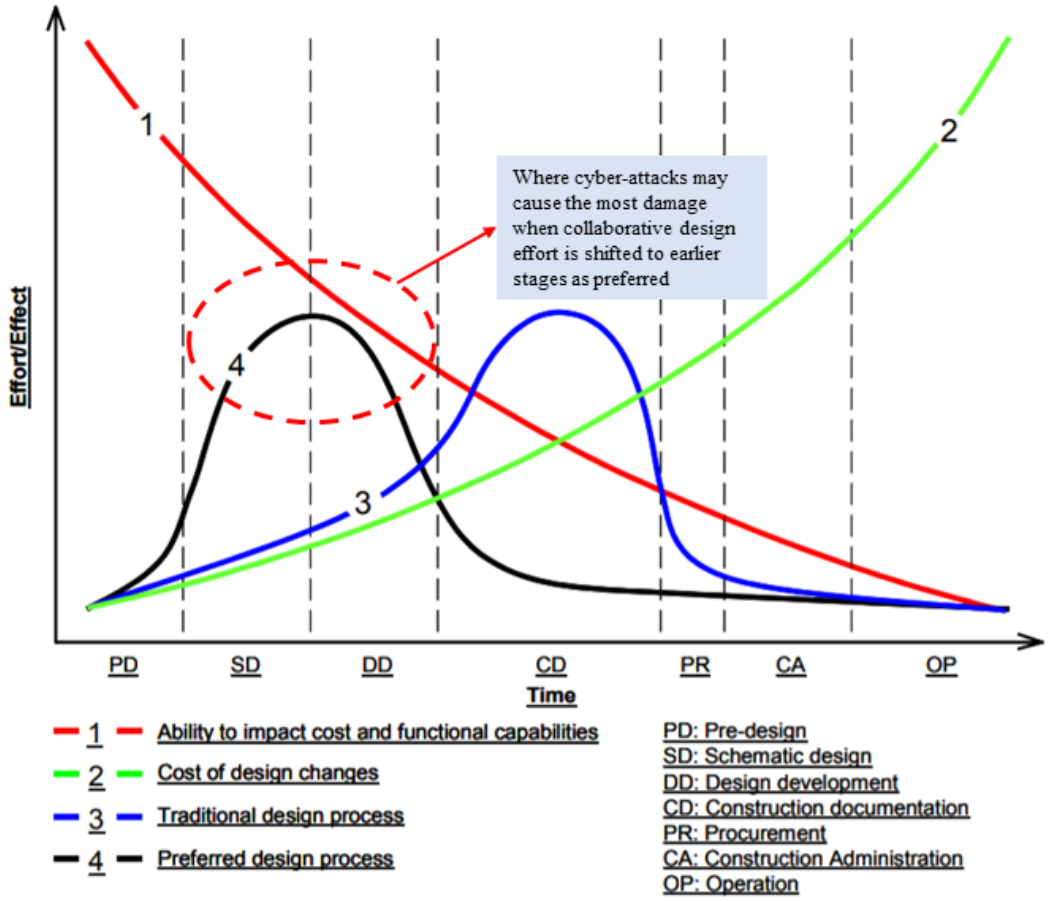

Figure 5: Effort/Effect Curve by Patrick Macleamy [33] with the comment about cyber-attack damage

While BIM offers an advanced collaboration in the design phase, it brings some challenges as well. One of the significant challenges faced during the design phase —in a BIM-enabled project—is interoperability [21]. Open and international standards, such as IFC, are utilised to overcome interoperability issues of data exchange [37] between different disciplines using various BIM authoring tools. IFC is an ISO standard developed for building information exchange [21] and can be encoded in several formats such as JSON, STEP, and XML [37].

Another challenge in BIM integration in the design phase is providing a sufficient level of cybersecurity [38]. The need for employing security measures grows, especially with the increasing number of stakeholders in a collaborative working environment [39]. Boyes [5] suggests the assessment of the design to make sure that there are no unanticipated and new risks. For this reason, Chapter 3 is solely focusing on the security risk assessment of the design phase to identify possible threats and vulnerabilities.

2.1.3.1 Design Workflow and Involved Stakeholders in BIM

Project members involved at each stage are directly related to the delivery method employed in a project [24], and accordingly, design workflow varies from one delivery method to another. There are four major project delivery methods mentioned by The Construction Management Association of America (CMAA) [40]: Design-Bid-Build (DBB), Construction Management at Risk (CMAR), Design-Build (DB), and Integrated Project Delivery (IPD). The most prevalent method employed in construction projects is DBB, which comprises three separate stages: the designer provides the design service; owner selects a contractor according to the bids received; the contractor constructs the facility [40]. Despite this fact, the design workflow for the IPD approach is demonstrated in this section since DBB method limits the use of BIM for enhanced coordination [41].

There are six groups of stakeholders, according to Autodesk's [41] workflow shown in Figure 6: owner, architect, subconsultants, contractor, suppliers, and trade contractors. There are three design-related stages shown in Figure 6, which are conceptualisation, criteria design, and detailed design [41]. In the original workflow, published by Autodesk [41], there are four more project phases, which are implementation documents, agency coordination/final buyout, construction, and facility management. However, these stages are not shown in this section since they are not directly pertinent to the design phase.

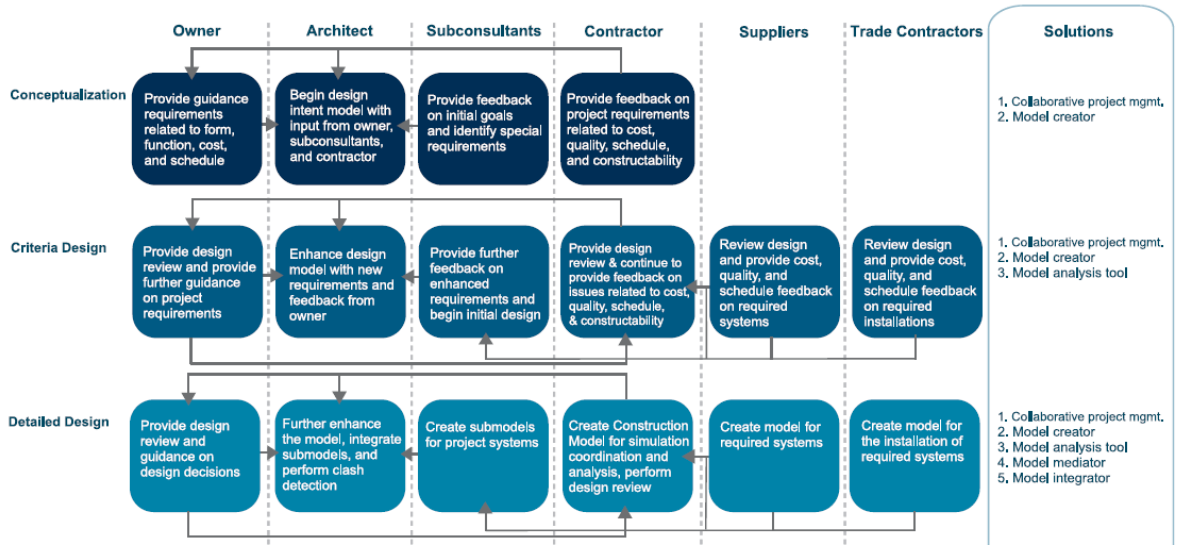

Figure 6: Design workflow and involved stakeholders in BIM-enabled IPD implemented projects [41]

AIA [24] and Autodesk [41] define three abovementioned design stages as follows:

- **Conceptualisation (Conceptual Design):** Planning the project by producing ideas to decide what is going to be built, who will construct it, and how is the construction going to be executed. The preliminary schedule is determined, cost estimations are made, and performance

targets are set. BIM enables these estimations to be more accurate compared to conventional construction projects. The constructor is involved in this stage in the IPD approach to provide constructability analysis as well as cost information.

- **Criteria Design (Schematic Design):** Evaluation is made to narrow down significant options. Cost estimations, schedule and project scope are finalised to continue to the following stages with higher confidence. In the IPD approach, integrated project coordinator forms the project teams, distribute responsibilities, and coordinates the schedule. The constructor continues giving feedbacks on constructability and cost.

- **Detailed Design (Design Development):** All critical decisions regarding the design are concluded. All ambiguities are removed, and all elements and systems are defined. The precision of cost estimations and schedule is improved to a higher level compared to previous stages.

2.2 Overview of Cybersecurity

Advancements in information and communication technologies (ICT) in recent years is resulting in digital transformation in most of the industries. This transformation—widely known as Industry 4.0—enables the adaptation of related technologies, such as cloud-based design systems and the IoT; however, it may not be possible to achieve the real potential of digitalisation without addressing cybersecurity challenges appropriately [42]. Many governments have started founding their cybersecurity agencies and centres over the last few years. One of them is the Cybersecurity and Infrastructure Security Agency (CISA)—formed by the USA government in 2018—, and they define cybersecurity as "the art of protecting networks, devices, and data from unauthorised access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information" [43, Para. 1]. Another one is the National Cyber Security Centre (NCSC)—formed by the UK government in 2016—, and they make the following definition: "Cybersecurity is how individuals and organisations reduce the risk of cyber attacks" [44, Para. 1].

One of the terms often mentioned in cybersecurity definitions is "cyber environment"—sometimes used as "cyberspace". It refers to the environment where computer-based electronic devices communicate over interconnected network systems [5]. Another term to be defined is "information security", which is frequently used interchangeably with cybersecurity, even though there are some differences [45]. The International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) define information security as "the protection of information from a wide range of threats in order to ensure business continuity, minimise business risk, and maximise return on investments and business opportunities" [46, Para. 17]. It is also mentioned that information can be either printed/written on a paper or in digital format [46]. Therefore, while cybersecurity covers

the security of everything—information and devices—in the cyber realm, information security covers the security of all kinds of information regardless of the format and environment. Venn diagram in Figure 7 shows the relationship between cybersecurity and information security visually.

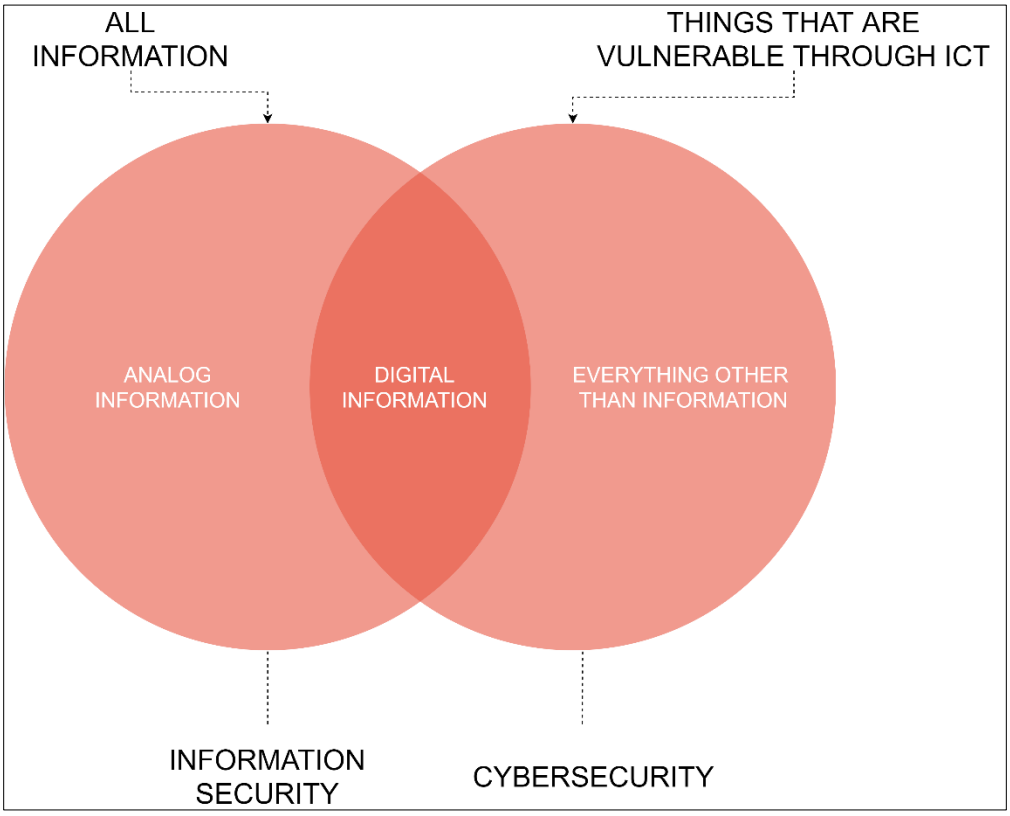

Figure 7: Relationship between information security and cybersecurity [47]

Digitalisation in the AECO industry—often called Construction 4.0—increases the use of ICT and, as a result, having more connected systems throughout the lifecycle of construction projects become possible [48]. One of the main advantages of digitalisation is being able to utilise the data. However, a considerable amount of data produced during big scale construction projects—such as bidding information, pricing, employee identification information, and cost/revenue data—can be classified as confidential and sensitive [48]. Therefore, the need to address the cybersecurity vulnerabilities arises [3]. There are two main actions to maintain security: identifying possible threats and employing measures to mitigate them [5].

Another commonly used term to be mentioned in the context of cybersecurity is “cyber-physical system (CPS)”. In a few words, “they are computer-based systems that monitor and control physical processes” [49, p. 1]. Network agents are the main parts of most CPSs, which mostly consist of sensors, actuators, and communication devices [49]. Since CPSs depend to a large extent on ICT, advancements in them can be seen as positively correlated [50]. CPS can also be seen as an approach to overcome

challenges in the implementation of IoT and smart devices in buildings [51]; therefore ensuring the security of CPSs is a paramount concern from both ICT and construction perspectives.

In the following sections, principles of cybersecurity are described by considering BIM and design-related issues. Possible cyber threats are scrutinised to point out the types of threats, main motivations, possible outcomes of attacks, and practices to minimise the adverse effects of such malevolent intentions.

2.2.1 Main Principles of Cybersecurity

Most of the definitions for both information security and cybersecurity comprise three main principles: confidentiality, integrity, and availability—also called as CIA triad [52]. The scope and interpretation of these three principles vary depending on the industry needs, organisational needs, and laws in place [53]. In years, security experts have developed novel and more comprehensive models by extending these three security principles. One of the pre-eminent security models—proposed by Donn B. Parker—is Parkerian Hexad which augments the CIA triad by adding three more attributes: possession/control, authenticity and utility [2]. Boyes [54] indicates that two more facets on top of Parkerian Hexad are required for addressing security issues of CPSs: safety and resilience. Figure 8 shows these eight security facets. Definitions of these security principles and their importance in the context of BIM is indicated below.

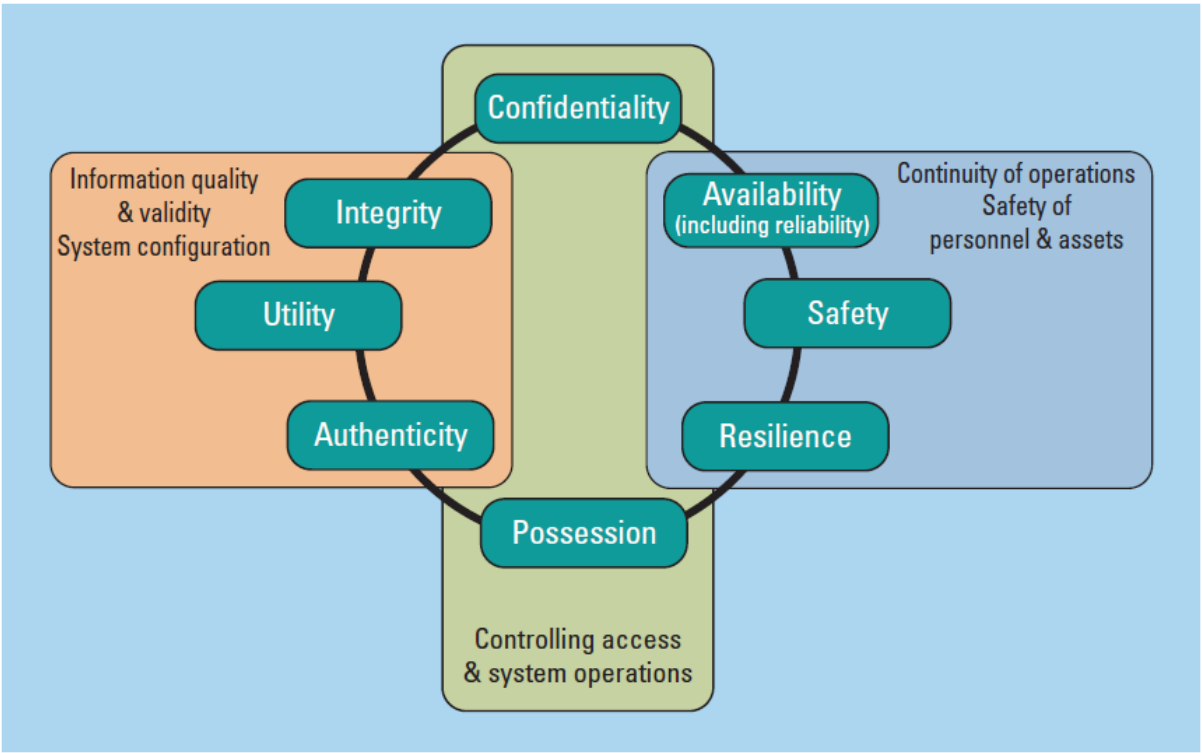

Figure 8: Augmented Parkerian Hexad [54]

- **Confidentiality** is having control of access to information and preventing unauthorised access to data that might cause damage to the organisation when disclosed [3], [55]. From construction and BIM point of view, an inadequate level of confidentiality might cause:

    - o disclosure of commercial data, which might lead to a disadvantageous position in a competitive tendering process;
    - o compromise of the facility's security information, which might cause malevolent parties to break into the security system with less effort when the facility is in operation;
    - o loss of intellectual property, which might contain valuable information as to design calculations, construction techniques, and specific know-how [38].

Confidentiality can be ensured by encrypting data and putting restrictions to limit access to data repositories [55]. It is also crucial to mention that some of the data alone may not be sensitive or cause damage if compromised; however, combining this data with others may create sensitive information [38]. Therefore, controlled access should be provided to each team member according to their roles and responsibilities.

- **Integrity** can be concisely defined as preventing unauthorised alterations to information and retaining consistency [3]. Integrity is disrupted when an authorised user or an unauthorised third party modify or delete some information [55]. As a result, receivers think that information is as originated, which is misleading. Therefore, in BIM-enabled construction projects—where the number of users might go up to thousands—, change tracking and configuration management become of paramount significance [38]. Additionally, recovery measures should be taken against possible integrity compromises, such as having regular backup procedures that are already practised [38].

- **Availability** is the accessibility and usability of information, services and systems by authorised parties at any time [3], [55], [56]. Systems used for data sharing should have a sufficient level of resilience to accomplish desired availability [3]. If a rival party can compromise the availability of information, it may provide an immense competitive advantage to them [56]. From BIM perspective, the following critical issues should be addressed—by considering the significance of time during design and construction phases—:

    - o If the project is utilising a cloud-based CDE, risks of the availability of that specific cloud service should be understood thoroughly;
    - o Compatibility between various BIM authoring software utilised by design teams might be an issue of availability during the project lifecycle.

  - Another concern might be the compatibility between different versions of the same modelling software used at different stages of the project. Even though new versions of modelling software support files produced by the old versions, there might be losses in embedded comments, diagrams and calculations, which leads to disrupted integrity.

- **Possession/Control** is defined as "holding, controlling, and having the ability to use information" by Parker [57] from an information security perspective. It can be provided by taking preventive actions as to the control of information and preventing unauthorised interference [3]. From a CPS perspective, it can be seen as losing control of making changes or losing the ability to monitor operations [54]. While the loss of confidentiality is caused by the disclosure of confidential and secret information; loss of possession may occur whether the information is confidential or not. Loss of possession/control may lead to loss of confidentiality; however, they must be treated separately to identify protective actions to both individually [57].

- **Authenticity** is ensuring the genuineness of the data and transactions [55]. It is crucial to understand the difference between integrity and authenticity clearly. If there is a transaction between parties A and B, integrity means that there is no unauthorised change or modification in the data during the transaction. On the other hand, authenticity means that data received by B is genuinely sent by its purported sender, A. Due diligence in ensuring the authenticity of the information during the design phase—where vast numbers of subcontractors are involved—is needed to prevent notable differences between the original design and the as-built asset [54].

- **Utility** can be briefly defined as the usefulness of the data [57]. From a construction point of view, it can be explained as keeping the asset information usable during the lifecycle of an asset from design to maintenance [3]. Considering the total lifecycle of built assets being much longer than modelling software, the utility of BIM documents become of high priority [54]. Opening proprietary formats can be an issue, even after a decade of creating the file with previous versions of modelling software. However, the pertinent data must remain useful during the extended maintenance periods of built assets. Therefore, it is prudent to take necessary actions starting from the design stage, such as using non-proprietary formats.

- **Safety** is one of the attributes added by Boyes [54] on top of Parkerian Hexad to cover the security aspects of built assets comprehensively. Since the failure of CPS operations may lead to serious safety issues—even causing to physical injuries or death—, it is reasonable to include it within the security facets.

- **Resilience** is the ability of a system to go back to its normal state or recover promptly when an adverse event occurs [3]. It is of paramount importance to be able to isolate the

negatively affected parts of the system from unaffected parts [54]. Moreover, projects and organisations must understand which information is critical and sensitive, so that resilience can start to be created from these points [58].

2.2.2 Cybersecurity Threats

According to Alguliyev et al. [59], cybersecurity threats affect the following aspects of a system: the confidentiality, by disclosing sensitive information; the integrity, by altering the data without authorisation; the availability, by causing interruptions in the system; the reliability, when there is a need to validate both communicating parties are the ones they pretend to be; the authenticity, when it is required to confirm the identity of the originator of information; the non-repudiation, by distorting proof of actions executed by involved parties; the accountability, by disabling tracking of an entity's actions. Figure 9 shows these threats from a CPS point of view. Communication and computing branches of the diagram can be applied to the design and construction phases of a BIM-enabled project as well.

Figure 9: Tree of cyber threats and attacks on CPSs [59]

In Figure 10, it is illustrated that threats exploit vulnerabilities, and they result in exposures which are risks. Risks can be mitigated by safeguards which protect assets. Finally, assets are menaced by threats [60]. This cycle can be used to see the relationship between risk elements and to understand the mitigation process.

Figure 10: Risk elements [60]

Some of the significant cybersecurity threats are listed below [61]:

- **Denial of Service (DoS) and Distributed Denial of Service (DDoS):** Attacks that create a high volume of traffic to prevent the system from legitimately working are called DoS attacks. If numerous zombied computer systems (botnets) are utilised for the attack, it is called a DDoS attack [60].

- **Insider data theft:** These are attacks that involve people who have authorised access to data and systems [62].

- **Email-based fraud:** They include phishing, spear-phishing or other types of spoofing by e-mails [61].

- **Social engineering:** It is performed by gaining the trust of someone working in a project or a company to deceive them and making them reveal information that they are not supposed to reveal [60].

- **Trojan attacks:** These attacks utilise programs that pretend to be useful, but on the other hand, including malicious codes [63].

- **Code injection techniques:** It happens when malicious codes inject themselves into trusted software and operating systems and thus bypassing antivirus software [60].

- **Advanced persistent threats:** These attacks aim to infiltrate systems and stay there for an extended period to monitor activities and steal data [64].

- **Zero-day attacks:** Attacks that occur on the same day a vulnerability is discovered in the software are called zero-day attacks [65].

- **External software, including malware:** Introducing software including malware and adware to a system [61].

Cyber threats can interrupt the BIM workflow at every stage of a project [4]. Therefore, the causes and outcomes of cybersecurity threats must be understood by organisations. There are three elements of threats, which are agent, motive, and results [66]. Cybersecurity threat agent types, potential malevolent groups and their motivations, possible adverse outcomes of attacks, and actions to minimise the effects of these attacks are reviewed in this section from BIM perspective.

2.2.2.1 Threat Agent Types

Threat agents are the sources of attacks causing damages to systems by intention or by accident [50]. It is crucial to understand that threats may emanate from anywhere [60], and because of that, threat sources must be reviewed in a few different categories. Boyes [38] divides threat agents into three main groups: external threat agents, internal threat agents, and systems and business failures.

- **External threat agents:** These are malicious outside groups, intending to access internal data, steal intellectual property, disclose sensitive information, and interrupt workflows by jeopardising the availability and integrity of systems [4]. Outsiders are not connected to the owner, and they do not have the authorisation to access project data [67]. They can be hackers, competitors, terrorists who are trying to reach BIM data for having a competitive advantage, organising a crime to the constructed facility, or leaking confidential information [38].

- **Internal threat agents:** These are people who have authorised access to the project information, and they use their privileged access for causing harm [67]. They cause undesired results for the project or the organisation by intention or by mistake [60]. Therefore, they can be categorised as either “malicious insiders” or “non-malicious insiders” [5]. Malicious insiders may be motivated by the feeling of revenge or just personal benefit, and they use their access to cause damage or compromise information [62]. Non-malicious insiders usually lack sufficient training and cause a cybersecurity incident by mistake [62]; however, the incident may occur due to negligence or error even though employees have received training [66]. Both malicious and non-malicious threat agents must be a part of the risk assessment.

- **Systems and businesses failures:** These failures may occur due to several reasons such as natural events, system failures or business failures [38]. Natural causes might include extreme weather conditions—thunderstorms, floods, sandstorms, heavy snowfall—or animal-related incidents [4]. These natural risks must be elaborately examined before being dismissed. For instance, there might be no risk of flood in an area; however, a broken main can still cause a flood and damage the hardware [66]. System failures may happen due to human-made mistakes such as the imprudent installation of systems, lack of maintenance, or damaging equipment due to negligence [68]. Business failures such as bankruptcies may affect the availability of data and disrupt access [38].

2.2.2.2 Cyber-Attack Motivations and Types of Cyber-Actors

There are several cyber-actor groups vary depending on their motivations and background. These actors can be grouped into three main categories according to their intentions [69]:

- **White hats** are usually hired by companies to assess the security level of the company and maintain or increase the robustness of existing security, according to the definition of Dunn Cavelty [70]. They have the legitimate right to access data within the boundaries set by their company.

- **Black hats** are the ones who break into systems without authorisation and tamper with the data [69]. Even though they use similar tools with white hats, they intend to cause harm, system malfunction, sabotage, or various other damages to target systems [39].

- **Grey hats** have the purpose of finding security vulnerabilities of systems without having authorised access. By contrast with black hats, they have the intention of patching and improving security instead of causing harm [69]. Hacktivists—will be explained in more detail in the following section—also fall into this category since they act by the motivation of supporting a good cause and doing justice [39]. It should be taken into account that a "good cause" for one party can have the opposite meaning for another, that is why this category cannot be labelled as "black" or "white".

Abovementioned categories outline three main groups of cyber-actors; however, there are various taxonomies developed for defining them in a more specific context. Parker [71] developed a categorisation of seven groups: pranksters, hacksters, malicious hackers, personal problem solvers, career criminals, extreme advocates, and malcontents, addicts, and irrational individuals. Later in 2005, Marcus Rogers developed an eight-level taxonomy: novice, cyber-punks, internals, petty thieves, virus writers, old guard hackers, professional criminals, and information warriors [72]. The taxonomy used

by Pärn and Edwards [39] to address various motivations behind cyber-attacks is utilised in this section to define each group:

- **Hacktivists** are the people who hack for a specific reason, which can be social, patriotic, or political, and they usually defend the freedom of speech, equal share of wealth, and anti-censorship [73]. The word "hacktivist" is formed by the combination of the words "hacker" and "activist". They usually act with groups such as Anonymous, Lulzsec, and Internet Feds and organise large-scale attacks to draw attention to particular issues [60].

- **Script kiddies** are the ones who download programs, run scripts, and follow explicit instructions to commit a cyber-attack since they lack sufficient programming knowledge to create their attacks [60]. They may be grouped under any of the main categories mentioned before—black hat, white hat and grey hat—according to their intentions and the consequences of their acts [39]. They usually want to be a hacker or see themselves as hackers, and they can only attack systems with apparent security vulnerabilities [74].

- **Cyber insiders** are the employees who have the authorisation to access systems and information of the company and pose a threat to the security [62]. They may have motivations such as revenge, greed, or self-satisfaction [73]. They target known vulnerabilities of the systems for self-benefit [61]. Even though they appear friendly, they may cause the most significant damage to organisations since their co-workers or managers do not usually suspect them. They may sell intellectual property, company secrets, and commercial information to competitors [74].

- **Cyber terrorist** is defined as "an individual who uses computer/network technology to control, dominate, or coerce through the use of terror in furtherance of political or social objectives" [75, p. 78]. After the attacks in the US on September 11th, 2001, media started to use the term "cyberterrorism" frequently, and not always in the correct context; however, this term should not be used unless the perpetrator aims to cause fear and panic in the general public, with a specific intention [73]. These groups may look for support from a government as well as organised crime groups, which allows them to utilise advanced tools to augment the impact of the attack [5].

- **Malware author** term covers people creating malicious programs such as viruses, worms, and Trojans [73]. Their motivations may vary from individual to individual, such as personal satisfaction, financial benefit, or hatred against a target [39].

- **Organised cybercriminals** are sophisticated groups of people who usually utilise advanced attacking methods, aiming to generate financial benefits [61]. Some of the cybercriminal activities are theft of intellectual property, theft of money from bank accounts,

blackmailing to gain profit, and DDoS attacks on large scale companies [5]. They may be interested in accessing BIM documents related to sensitive facilities such as embassies, prisons, or banks [67].

- **Patriot hackers** are the supporters of a state, acting on their own initiative and targeting the enemies of their country or the countries conflicting with theirs [76]. Some of their motivations are defending their state, patriotism, and occasionally religious reasons [76].

- **Cyber militias** refer to cyber-actors informally supported by governments to provide protection and attack the enemies of the state when necessary [77]. They differ from patriot hackers mentioned above since they organise their activities with the support of the government—even informally—while patriot hackers work by their own will.

2.2.2.3 Possible Outcomes of Cyber-Attacks

As a result of abovementioned cybersecurity threats and cyber-attacks, adverse outcomes may occur, which must be taken into account by organisations to produce solutions for possible incidents and minimise undesired effects. These outcomes are summarised in this section; however, it should be kept in mind that they are not considered independent from each other [5].

- **Financial losses:** Even though other outcomes may also have indirect financial effects; direct financial losses are summarised under this category. Some of the possible financial outcomes are:

    - Recovery costs—mainly if there is physical damage to hardware—to make the system functional again,
    - Costs related to inspections by security specialists to analyse the incident—particularly possible in case of forensic investigations,
    - Costs for mitigation
    - Costs related to possible changes in the contracts with service providers as a result of the cyber incident [5].

- **Loss or disclosure of intellectual property or sensitive information:** Attackers aim to access information—such as intellectual property and confidential information—that they cannot access in normal conditions [62]. Intellectual property for construction projects may include “trade secrets, proprietary processes, technical specifications and detailed calculations or methodologies” according to PAS 1192-5:2015 [3]. Possession of intellectual property by malevolent parties may have significant consequences, particularly at the design and construction phases since most of the technical methods and options are discussed and decided at these phases [5].

- **Data corruption:** If perpetrators acquire the key for the communication system of the company, they can alter the real data, which is called "integrity attack" [59]. Corruption of data is one of the attacks against CPSs, as shown in Figure 9 as a part of communication and computing branches of the "tree of attacks".

- **Disclosure of personal identity information:** Retrieval of personal identity information may lead to further cyber incidents since it will provide attackers hints to use social engineering or to conduct phishing attacks [3].

- **Reputation damage:** It is caused by the disclosure of sensitive or personal information, or the malfunctions occur as a result of cyber-attacks [5]. The level of reputation damage increases as the scale of involved company or project grows.

- **Disruption of business operations:** It may happen as a result of several malevolent attacks such as overwhelming the communication network of the company to halt internal exchange of information, or corrupting PC operating systems of employees to hinder the workflow [62].

2.2.2.4 How to Minimise the Consequences of Cyber-Attacks

Potential cyber-attackers, their motivations and possible outcomes of cyber-attacks are scrutinised in the previous sections since it is of paramount importance to understand the threats in order to mitigate adverse effects. NCSC [62] addresses the steps to reduce the impacts of cyber-attacks, from a general cybersecurity perspective, as a part of the white paper published in January 2016. According to NCSC [62], there are four main stages of an attack: survey, delivery, breach, affect. Definitions of them and the mitigation methods to employ at these stages are as follows:

- **Survey** (also called as hostile reconnaissance) is the stage where attackers collect information to expose vulnerabilities of the target system [3]. Personnel mistakes and negligence often play a vital role in the event of a cyber incident [38]. Therefore, training employees against security issues and creating security awareness within the organisation are the essential mitigation methods for the survey stage [62].

- **Delivery** is the process of reaching the point of exploitation [62]. Some of the mitigation practices to employ at the delivery stage are utilising regularly updated malware protection, use of firewalls and proxy servers, and having a strict password policy in place [62].

- **Breach** is the stage where a security system is bypassed by attackers [60]. Effectively patching the known vulnerabilities of software, utilising a malware protection system for the

internet gateway, implementing robust access control, and tracking all network activities to detect possible suspicious activities reduce the possibility of vulnerability exploitations [62].

- **Affect** stage covers all the activities performed by attackers after the breach stage has occurred [62]. In case of an attacker accessing the network of the organisation despite all mentioned mitigation methods, a defence-in-depth approach can be beneficial to employ [62]. Defence-in-dept approach can be described as having several defence mechanisms so that if one of the mechanisms fail to protect the system, other ones being in place to fight against the attack [78].

From a digital built environment point of view, cyber deterrence suggestions provided by the British Standards Institution (BSI) [3] in PAS 1192-5:2015 can be useful for design, construction, and facility management companies [39]. Following measures are suggested:

- Having a holistic approach for security that encompasses people, technology tools, and processes.
- Applying the suggested security triage process to define the level of security required for the built asset.
- Identifying the sensitivity of the constructed built asset as well as the neighbouring built assets.
- Employing a security-minded approach for developing the policies and processes of the project.
- Appointing a built asset security manager, and developing a built asset security strategy, a built asset security management plan, a security breach/incident management plan, and built asset security information requirements [3].

2.3 Blockchain Technology

Due to the addressed issues related to the collaborative environment in the design phase and proliferating cybersecurity concerns because of digitalised building processes, researchers and industry professionals have been on the quest for practical solutions. Blockchain Technology (BCT) is one of these potential solutions that have been investigated in recent years for the management of security issues in the AECO industry. This section aims to give background information about the previous related work, the working mechanism of BCT, and related concepts.

Blockchain (BC) is a database system that stores all executed transactions in records called *blocks* in a decentralised fashion to prevent tampering and unauthorised revisions [79]. It was initially used as the mechanism behind Bitcoin, which was developed by S. Nakamoto in 2008 and published in a whitepaper [80]. Providing transparency, secured transactions between users, and enabling trusted financial transactions are the prominent selling points of BCT [79]. The success of BCT in supporting

cryptocurrencies like Bitcoin opened the way for utilising it in other industries and various applications [81]. While the finance industry has made the most use of BCT so far [79], other uses such as smart contracts [4] increased its areas of implementation.

2.3.1 Fundamentals of Blockchain

The concept of BC was initially developed by a group of researchers in 1991 to create timestamped transactions to prevent tampering [82]. Later in 2008, it was adapted by S. Nakamoto to develop the first cryptocurrency, Bitcoin [80]. Four main steps explain how the BC system works:

- A transaction occurs;
- A network of computers verifies the transaction;
- The transaction is stored in a block;
- The block is given a *hash* as well as the hash of the latest block added to the BC [83].

Once all these four steps are completed, and the block is hashed, it can be added to the BC [83]. A more detailed schema of BC is illustrated in Figure 11. In order to understand the architecture and working system of BC, the following terms shall be defined:

- **Hash** is the encrypted value generated by mathematical functions with the input of letters and numbers [84].
- **Blocks** are the units of information that forms a BC [85]. The first block in a BC that does not have any hash value from the previous block is called *genesis block* [81]. Blocks are formed by two main components: *block header* and *block body* [86]. The block header constitutes:
    - Block version: It shows which block validation rules to be followed [86].
    - Merkle tree root hash: A *Merkle tree* (a simplified example is illustrated in Figure 12) is a data structure helping to encode data efficiently, and the hash at the top is called *root hash* [87].
    - Timestamp: A time stamp that shows the seconds passed since January 1st, 1970 [86]. This system used is called Unix time [88].
    - nBits: A hash corresponding to all hashes [86].
    - Nonce (number only used once): It is an arbitrary—4-byte [4]—string to be combined with each block's hash [84].
    - Hash value of the previous block: A hash value that addresses the previous block [86].

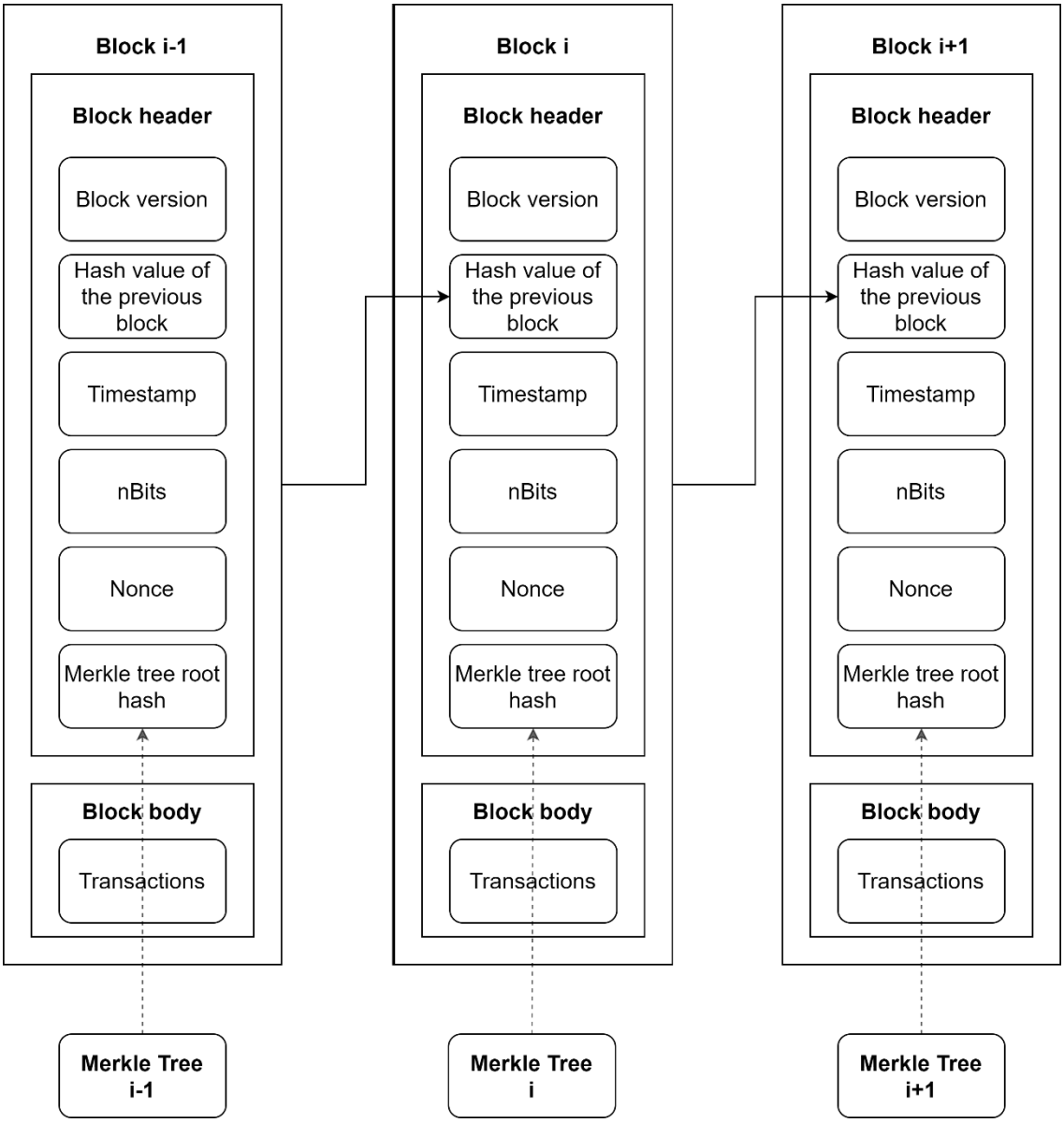

Figure 11: Blockchain Architecture

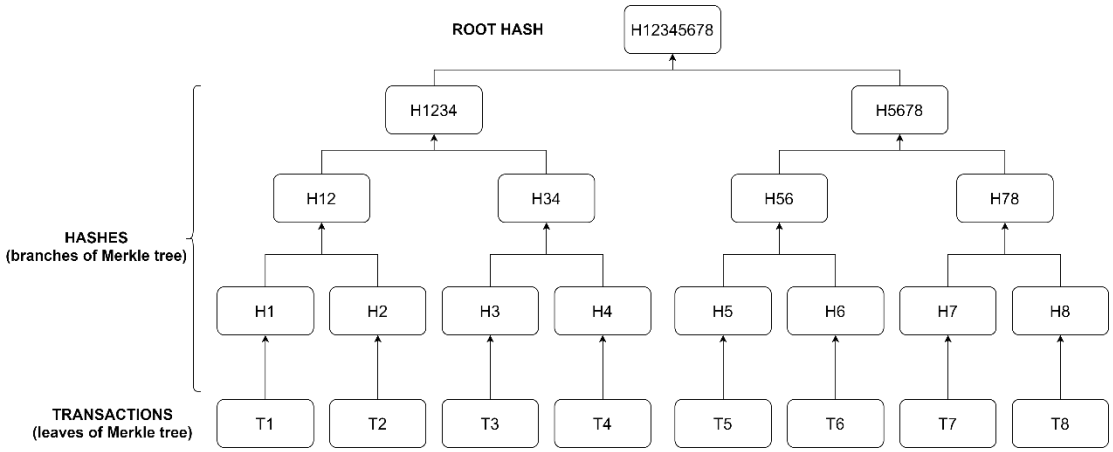

Figure 12: A simplified illustration of Merkle tree

Even though blocks are connected in a serial chain architecture, participants of the BC, or in other words, *nodes*, are physical or virtual machines that are globally distributed and connected in a peer-to-peer (P2P) network [89]. The nodes accept blocks if all the transactions stored in them are valid [85]. Figure 13 illustrates three different network types: centralised, decentralised, and distributed. Blockchain is an example of distributed networks, as mentioned previously.

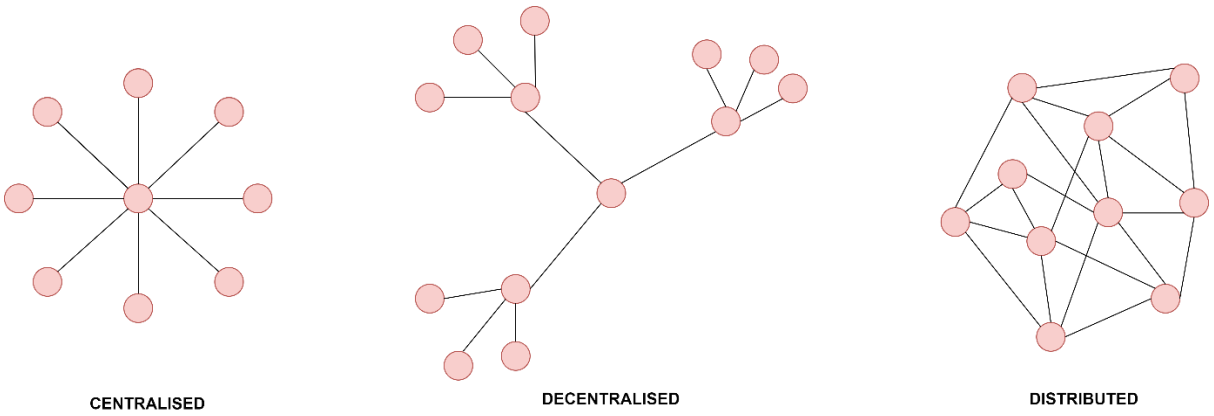

Figure 13: Centralised, Decentralised, and Distributed Networks

- **Digital Signature** makes use of private keys and public keys to authenticate transactions in BC environment [8]. Public keys are cryptographically created by using private keys for the verification of transactions [89], while private keys are used for signing the sent message by the sender [86]. Since public keys are accessible by everyone while private keys can only be accessed by the owner, generation of public keys from private keys is made extremely difficult to reverse with the utilisation of mathematical algorithms such as *elliptic curve digital signature algorithm (ECDSA)* [90]. A simple example of a transaction with the use of digital signature is as follows: (1) The sender generates a public key—with an algorithm such as ECDSA—by using its private key. (2) The sender signs—with a signing algorithm—the data to be sent by using its private key. (3) The receiver receives the signed data together with the public key. (4) The receiver verifies the received signed data by using the public key from the sender. In this example, data is not encrypted, only signed by the sender. The signature is verified by the receiver, which allows the verification of the authentication and the integrity of the data as well. A graphical illustration of this example can be seen in Figure 14.

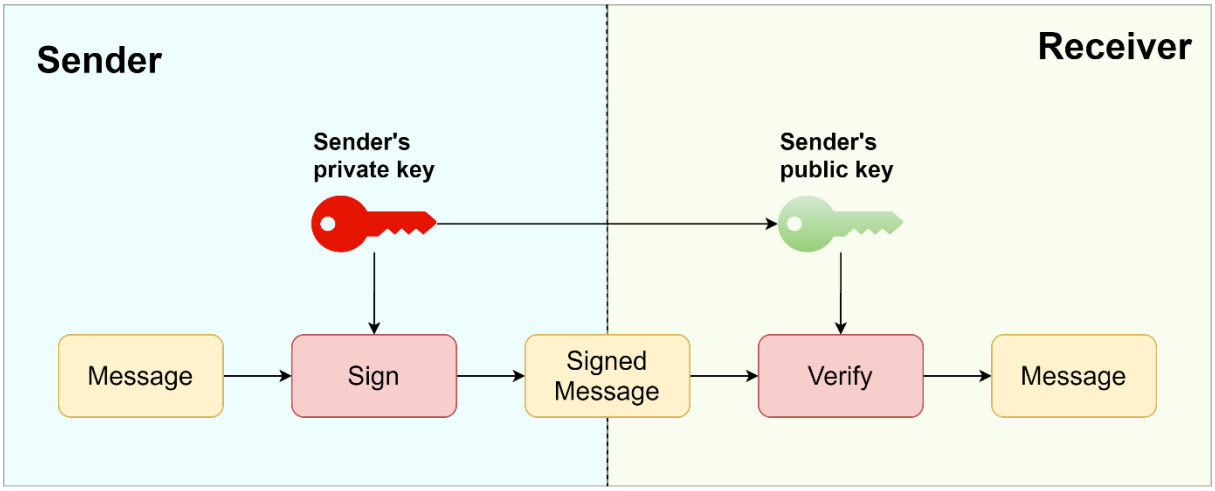

Figure 14: An example of the digital signature use with the private and public key

According to Buterin [91] (the co-founder of Ethereum), there are three types of BCs depending on the privacy: fully private BCs, public BCs, and consortium BCs. Fully private blockchains are the ones with only a group of authorised users that can validate the blocks and make transactions [89]. On the other hand, public blockchains like Bitcoin and Ethereum allow anyone to see the content of blocks, make transactions and participate in the validation of the blocks [81]. Consortium BCs are hybrid solutions for having a pre-selected, limited number of participants that has the authority to validate blocks [91]. Table 1 [86] makes a comparison between these three types of BC.

Table 1: Comparison of Blockchain Types Based on Privacy [86]

Property	**Public blockchain**	**Consortium blockchain**	**Private blockchain**
Consensus determination	All miners	Selected set of nodes	One organization
Read permission	Public	Could be public or restricted	Could be public or restricted
Immutability	Nearly impossible to tamper	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralized	No	Partial	Yes
Consensus process	Permissionless	Permissioned	Permissioned

BC is a distributed, transactional ledger [89] that has several essential differences from conventional centralised databases. According to Turk and Klinc [85], the following features make BCT unique and different compared to traditional database systems:

- Being able to have many copies of the chain in many devices,

- Not allowing for changes in the data in blocks once they are validated and joined to the BC,
- Ensuring that all copies of the chain across all devices are identical,
- Being able to access the entire data change and metadata history,
- Not requiring a central, trusted authority.

2.3.2 Consensus Mechanism to Improve Trust in Collaborative Environment

The consensus mechanism is one of the key features of BC that makes it different from financial institutions by removing the need for a trusted third party [92]. All nodes in a BC agree on a consensus protocol for validating transactions and adding new blocks to the chain [81]. The need for a robust consensus protocol in BC systems is evolved from The Byzantine Generals Problem [86], which was first mentioned in 1982 [93]. It is based on the hypothetical situation that the Byzantine army is planning to attack a city. Several generals are waiting to attack with their soldiers, and the only way of communication between generals is via messengers. They have to agree on a strategy to be successful; however, some of the generals may be traitors who want to jeopardise the plan. The problem in this situation is to find a mechanism to make loyal generals reach a consensus despite the disloyal ones [93]. In BC systems, the need for a consensus protocol arises from a similar problem: some of the nodes in the BC might be malevolent; however, the honest nodes must reach on an agreement. Following are some of the widely used consensus algorithms to overcome the Byzantine Generals Problem in BCs:

- **Proof of Work (PoW):** PoW is the consensus protocol utilised by Bitcoin and Ethereum. It is based on the idea that the nodes that want to create new blocks to be added to the BC needs to solve complex mathematical problems—easy to verify despite the difficulty of solving—, which is also known as *mining* [86]. In this mechanism, the first node to solve the problem wins the competition to create the next block [94], which makes it highly dependent on the computing power of nodes. When a node solves the problem, the solution is broadcasted to the BC network for the validation by other nodes [86]. After the validation, the new block is added to the BC, and the same process starts for the next block. It is criticised for spending too much energy and thus resources [95]. Ethereum is planning to release an upgrade, Ethereum 2.0, to start employing Proof of Stake (PoS) consensus protocol to prevent the extensive use of energy [96].
- **Proof of Stake (PoS):** This algorithm is as a lower energy consumption alternative to PoW [86]. In this mechanism, the leader for adding the next block is chosen by a process that randomly selects the winner in proportion with the owned stake [97]. It is assumed that people holding more stakes are less likely to attack the system since it would affect their earnings as well [86]—particularly for cryptocurrency BCs.
- **Practical Byzantine Fault Tolerance (PBFT):** It is a consensus protocol that can tolerate up to 1/3 malicious nodes in a BC network [86]. A node is selected as the primary node in each round for determining the new block in the BC [86]. A node needs to be voted by more than 2/3

of all nodes to join the next round [86]; therefore, this protocol requires all nodes to know all of their peers in the network [98]. For this reason, its scalability is much lower compared to PoW protocols that can handle thousands of nodes [98].

- **Delegated Proof of Stake (DPoS):** In this kind of mechanism, nodes to generate blocks (representatives) are elected by the stakeholders [86]. Since there are much fewer nodes for generating and validating blocks and thus confirming transactions, this process becomes much faster [86]. Each elected representative has an assigned time to generate the new block [99]. If the representative does not create a block in the allocated time, its turn is skipped, and the next representative can generate a block [99].
- **Proof of Elapsed Time (PoET):** The technology company, Intel proposed this mechanism, and it makes use of Intel's set of security instruction codes, SGX (Software Guard Extensions) [100]. This consensus protocol works as follows:

  Each node is assigned with a random waiting time before creating a block. SGX ensures the randomness of this assigned time. The first node that expires its waiting time is entitled to create the new block. Each node needs to submit a proof for the waiting time—provided by the SGX hardware—together with the block. There are also statistical checks to confirm the authenticity of the waiting time [100].

2.3.3 Related Concepts

2.3.3.1 Smart Contracts

One of the most exciting uses of BCT beyond cryptocurrencies is *smart contracts* [85]. They are "automated and self-enforcing digital contracts relying on tamper-proof consensus on contingent outcomes" [101, p. 11]. They work only when the specific conditions of the contracts are met, which removes the necessity of having a central authority [81]. Smart contracts can improve the enforceability and contractibility of BCs by its algorithmically automated approach [101].

Another term to be mentioned in the context of smart contracts and BC is "oracle". Oracles are the contracts that work as third party sources for information from outside the BC [94]. Oracles are required since BCs usually do not permit smart contracts to query information from external sources; therefore, they work as an interface between smart contracts and outside data sources [81].

2.3.3.2 Hyperledger Fabric

Hyperledger Fabric is a platform with a modular design, developed within the Hyperledger Project, to enable users developing distributed ledger solutions with a high level of confidentiality and scalability as well as robust resilience [102]. Therefore, solutions can be developed in Hyperledger Fabric for all industries [102]. It is an example of private (permissioned) BCs according to its level of

privacy [103], and it supports plugging components from various businesses and the utilisation of various consensus mechanisms to adapt to the complexity and needs of each case [102].

In Hyperledger Fabric, participants (nodes) are maintained by Membership Service Provider (MSP), that provides node credentials for authorisation [103]; and it is one of the features of Hyperledger Fabric that makes it different from a public BC. Two other characteristics of Hyperledger Fabric are particularly significant for its use in BIM environment: offering to store data in various formats and having the option to create a separate ledger for a specific group of participants [4]. It allows managing the user access to data exchange environment since all stakeholders shall be assigned with customised access according to their roles in the project.

3 CYBERSECURITY RISK ASSESSMENT IN THE DESIGN PHASE

There are seven international and seventy-nine national risk assessment/management documents—methods, standards, guidelines, frameworks, and tools—published by various organisations all around the world by November 2018, listed in the guidelines prepared by the European Union Agency for Cybersecurity (ENISA) [8]. While some of these standards, guidelines, or frameworks are developed targeting all industries without having sector-specific aspects, some are targeting specific industries such as finance, energy, or oil & gas. However, in ENISA guidelines, there is no cyber assessment framework, particularly addressing the risks faced during construction projects.

With the utilisation of BIM tools and processes, the need for a bespoke cybersecurity risk assessment framework increases. Since the digital collaboration and information exchange peaks at the design phase—especially for design-build and IPD projects—[26], it is of utmost importance to have a security-minded approach. Hence, this chapter focuses on selecting a generic cyber assessment framework so that it can be adapted— in Section 3.3 of this chapter—to the context of the design phase in BIM-enabled construction projects.

3.1 Selection of The Suitable Framework for Adaptation

In order to select the most suitable option for the purposes of this chapter, some available documents about cybersecurity and information security risk assessment published by international and national organisations are reviewed. Reviewed documents and their brief definitions are introduced in the following sub-sections.

3.1.1 National Institute of Standards and Technology (NIST) - Framework for Improving Critical Infrastructure Cybersecurity v1.1

It is a comprehensive and advanced framework for reducing cybersecurity risks for critical infrastructure. It is developed based on other references such as frameworks, guidelines, or specifications. There are three main components of the framework: Framework Core, Framework Implementation Tiers, and Framework Profile.

In the Framework Core, there are four sections: Functions—identify, protect, detect, respond, and recover—, Categories, Subcategories, and Informative References. Under the Informative References section, documents from other organisations explaining how to achieve cybersecurity targets are listed. The Framework Implementation Tiers component provides an overview of how organisations see cybersecurity risks. On the other hand, the Framework Profile component helps organisations to develop cybersecurity risk strategies aligned with their resources and company goals.

In conclusion, this framework by NIST does not provide a checklist with questions for performing a cyber assessment. Instead, it guides organisations to develop their cybersecurity strategies and provides references to find detailed information about each security aspect.

3.1.2 ISO/IEC 27005: Information technology — Security techniques — Information security risk management

It is an international set of standards that provides guidelines related to information security risk management. It is developed to be employed by companies from all industries. It describes the process of information security risk management by defining all the steps and the activities at each stage. Risk assessment is covered in three components: risk identification, risk analysis, and risk evaluation. Risk treatment follows the risk assessment process, and it consists of four options: risk modification, risk retention, risk avoidance, and risk sharing.

In summary, this standard from ISO and IEC describes how to develop information security risk management processes and defines boundaries; however, it does not provide an assessment framework with a list of questions to be answered by organisations.

3.1.3 The Institute of Internal Auditors (IIA) - Global Technology Audit Guide (GTAG), Assessing Cybersecurity Risk: Roles of the Three Lines of Defense

It is a guide that addresses cybersecurity risks and threats for all types of organisations and provides an approach to perform cybersecurity risk assessments. It points out the significance of ensuring the robust operation of each three lines of defence separately. The first line of defence covers the management of risks, data, processes, and controls; the second line of defence ensures the effectiveness of the first line of defence; the third line of defence assesses the effectiveness of the first and second lines of defence.

In this guide, a framework for cybersecurity risk assessment is presented. The framework comprises six components: Cybersecurity Governance, Inventory of Information Assets, Standard Security Configurations, Information Access Management, Prompt Response and Remediation, and Ongoing Monitoring. Suggestions are made under each component of the framework rather than providing a checklist for performing a risk assessment.

3.1.4 NCSC - Cyber Assessment Framework v3.0

It is a comprehensive framework developed to be used by the organisations themselves or by third-party assessment entities for assessing cybersecurity functions of organisations. The assessment structure is formed around four main objectives: managing security risks, protecting against cyber-attack, detecting cybersecurity events, and minimising the impact of cybersecurity incidents.

In total, there are fourteen principles under four main objectives, and these principles are broken down into thirty-nine contributing outcomes for detailing the assessment. For each contributing outcome, a set of good practice indicators are listed in tables to assess if the contributing outcome is achieved, partially achieved, or not achieved by the organisation. Good practice indicators are presented as clear statements in a checklist format, which makes it easier and more convenient to use. Table 2 provides a list of all fourteen principles that take place in the assessment framework.

Table 2: List of principles in the cyber assessment framework from NCSC

Objectives	**#**	**Principles**
Managing security risk	**1**	Governance
	2	Risk Management
	3	Asset Management
	4	Supply Chain
Protecting against cyber-attack	**5**	Service Protection Policies and Processes
	6	Identity and Access Control
	7	Data Security
	8	System Security
	9	Resilient Networks and Systems
	10	Staff Awareness and Training
Detecting cybersecurity events	**11**	Security Monitoring
	12	Proactive Security Event Discovery
Minimising the impact of cybersecurity incidents	**13**	Response and Recovery Planning
	14	Lessons Learned

3.1.5 Conclusion of the Review

As a result of the review, the Cyber Assessment Framework v3.0 published by NCSC in September 2019 is selected as the most suitable option to proceed. The reasons for selecting the framework of NCSC are as follows:

- All concerns are presented in a well organised and easy-to-use checklist format which is lacking in the other three reviewed documents.
- It comprehensively addresses cybersecurity issues under thirty-nine items while the framework from IIA only gives brief suggestions for each of its six components.

- It does not require utilising other standards/methods, unlike the framework from NIST and the standard from ISO/IEC.
- It provides a ready-to-use assessment framework instead of describing how to perform the assessment, unlike NIST and ISO/IEC documents reviewed in the previous sections.

3.2 Method for Framework Adaptation

Cyber assessment adaptation is executed in Section 3.3 under four main categories similar to the original framework by NCSC: cybersecurity risk management, cybersecurity defence mechanisms, monitoring cybersecurity activities, and minimising the consequences of cyber incidents. A total of fourteen items addressing security issues are covered under these four main categories. For each item, three components take place:

- **Original:** It summarises the non-industry specific concerns mentioned by NCSC in the original framework to assess the cybersecurity level of organisations. Each concern for each item in the original document is not presented verbatim as the target is to have a concise summary of each subject rather than copying all details. Summarised security issues are presented as questions to be answered by organisations for cybersecurity assessment.
- **Adaptation:** Under this component, cybersecurity-related issues addressed in the original framework are adapted into the design phase in BIM-enabled construction projects. Stakeholders and organisation chart, technology tools, network systems, and database systems utilised during construction projects are taken into consideration for the adaptation. The aim is to keep the original concern while making it more specific for the needs of design workflows. Adapted security issues are introduced as questions to be answered by security personnel of construction projects for cybersecurity assessment.

  Discussion: This component targets to find possible solutions to the adapted issues. Related cybersecurity best practices relevant to the design phase and BIM processes are provided to support the key points of each item. Since the practical aspects may vary from project to project according to the requirements of each case, the goal is to discuss possible solutions, rather than giving definite answers. Discussion section includes many suggestions from PAS 1192-5 [3] as it is a comprehensive document addressing security threats in digital built environments.

3.3 Cyber Assessment Framework Adaptation for BIM-enabled Design Phase

3.3.1 Cybersecurity Risk Management

3.3.1.1 Governance

- **Original:**
  - Is there a board-level executive owning the security management of networks and information systems, bringing security issues to the attention of other board members and leading related discussions, and tracking organisational practices pertinent to cybersecurity?
  - Are roles and responsibilities for maintaining the secure environment within the organisation defined and assigned to the related staff with adequate knowledge?
  - Are there decision-makers responsible for risk management that make timely decisions in accordance with the risk appetite of the organisation?
- **Adaptation:**
  - Is there an executive in the project management team who follows the security issues in the project, leads the security discussions in coordination meetings, and points out security-related concerns of IT infrastructure and CDE of the project?
  - Are project members with sufficient security-related knowledge assigned with roles for maintaining the security level of the project before the initiation or using any external services?
  - Are there decision-maker project members who are delegated by the project management and aware of the risk management strategy of the project to make decisions when necessary?
- **Discussion:** According to the recommendations of PAS 1192-5 [3], a Built Asset Security Manager (BASM) shall be appointed by the asset owner or the employer if the asset is identified as sensitive. BASM position can be a full-time job if the project is large-scale and complex; otherwise, it can be handled by a project member equipped with security-related knowledge and experience as a part-time responsibility [3]. BASM shall be responsible for developing: the built asset security strategy (BASS), the built asset security management plan (BASMP), the security breach/incident management plan (SB/IMP), and the built asset security information requirements (BASIR) defined in PAS 1192-5 [3]. This role is not precisely equivalent to any roles mentioned in the questions of "Adaptation". However, BASMP may assign security-related roles to the project members with sufficient knowledge to distribute the responsibilities for maintaining a secure environment as well as delegating risk management decision-makers. Even though BASMP is accountable for all security decisions, someone from the senior project management shall still track the overall security level of the project and raise awareness to the recent security concerns.

3.3.1.2 Risk Management

- **Original:**
  - Are security risks to IT systems identified with an approach focused on the possible adverse effects of the attacks?
  - Are risk assessments performed considering current security threats to IT systems, and are the outputs of the assessments considered as security requirements to be met? Are crucial outputs from the assessment communicated to decision-makers?
  - Are risk assessments updated with the changes in the IT infrastructure or cyber threat landscape, and the effectiveness of the assessments reviewed regularly?
  - Do you have confidence about the effectiveness of your security measures, and do you feel comfortable to be verified by a third party?
- **Adaptation:**
  - Are possible security risks that may interrupt stable design processes or compromise sensitive design information identified by considering the possible consequences?
  - Are possible security threats specifically related to the requirements of the current project, software and hardware utilised for BIM processes, and design workflows considered for risk assessments? Are risk management decision-makers assigned by the BASMP aware of critical outcomes of the assessments?
  - Are risk assessment criteria updated when there is a change in the utilised software or hardware such as CDE, design tools, database systems, and network systems, or when there are known changes in construction-related threats?
  - Are you confident about the employed measurements for maintaining robust security of project IT systems? Are you confident of your security level to be verified by a third party assessor?
- **Discussion:** PAS 1192-5 [3] recommends developing three main strategies and plans to manage security risks of built assets in BIM environment: the built asset security strategy (BASS), the built asset security management plan (BASMP), and the security breach/incident management plan (SB/IMP). The built asset risk management strategy is suggested as well, as a part of the BASS to specify the method of conducting risk assessments for identifying potential vulnerabilities and threats [3]. Risk assessments shall be updated dynamically by following the latest threats, particularly against CDEs, design authoring tools, and databases that store critical project information. The project type can define the detail level of risk assessments since the effect of a data breach is proportional to the sensitivity of the project and the significance of the information stored in the CDE.

3.3.1.3 Asset Management

- **Original:**
  - Are all assets affecting the secure environment inventoried, prioritised according to their impact on the vital functions, and managed in a security-minded fashion?
- **Adaptation:**
  - Are all assets with vital importance on security such as project computers, data servers (if applicable), and supporting equipment such as uninterruptable power supply (UPS) or cooling devices inventoried by their effects on the critical functions of the project? Is the inventory managed and updated in a security-minded fashion?
- **Discussion:** Tangible assets such as data storage hardware and intangible assets such as design details, bill of quantities, and commercial information can be considered as security-critical assets during the design phase of projects. Inventories of tangible assets shall be managed with respect to their security impact on the project. If the project is utilising an in-house server for the CDE, keeping the hardware infrastructure of the server secure can be critical.

3.3.1.4 Supply Chain

- **Original:**
  - Do have a profound understanding of security-critical aspects of your suppliers, such as their partners, employers, and competitors; and do you consider these aspects for your risk assessments?
  - Are all data sharing systems and networks as well as vital information shared with suppliers adequately protected?
  - Are there clauses in the contracts with suppliers indicating security requirements to be fulfilled?
  - Do you and your suppliers have incident management procedures to follow when necessary?
- **Adaptation:**
  - Is there detailed security-critical information about your suppliers, such as design and engineering subcontractors, surveying subcontractors, and cost estimation consultants, regarding their other current projects or partnerships they are involved? Is this information about your suppliers included in your risk assessments?
  - Is there adequate protection from cybersecurity attacks against networks and sensitive data, such as confidential design details and quantity information, shared with suppliers during the design phase?
  - Are all suppliers aware of security requirements they need to fulfil to protect the sensitive information shared with them and to access the project network and CDE without violating security rules? Are these security requirements stated unambiguously in supplier contracts?

  - Do you and your suppliers have incident management procedures to follow in case of having a data breach or an interruption to CDE? Is having an incident management procedure included in supplier contracts as a requirement?
- **Discussion:** Intellectual property produced by the in-house design team, design subcontractors, and consultants during the design phase and stored in CDE can be the target of cyber attackers depending on the type of the project [3]. PAS 1192-5 [3] recommends cautiously managing user access levels to CDE, databases, and other data exchange platforms when sharing information with suppliers. Having detailed information about the other projects of suppliers and their business relationships with companies can provide valuable tips to discover possible malicious intentions from suppliers. Security requirements expected to be met by suppliers shall be mentioned explicitly in supplier contracts to protect intellectual property and prevent intrusions. PAS 1192-5 [3] suggests developing a security breach/incident management plan (SB/IMP) to take prompt actions when needed, and a similar incident management plan can be requested from the supplier as a requirement in the contract if the work includes the sharing of sensitive project information.

3.3.2 Cybersecurity Defence Mechanisms

3.3.2.1 Service Protection Policies and Processes

- **Original:**
  - Are security-related aspects comprehensively embedded in your company policies and processes in practical and achievable manners considering the main functions of your organisation?
  - Are security-related policies and processes reviewed and updated periodically, and in case of facing new threats or experiencing a notable incident?
  - Are cybersecurity policies and processes integrated with other organisational policies and processes, followed rigorously, and evaluated in terms of their performance?
  - Are all employees well informed about the security-related policies and processes of the organisation?
- **Adaptation:**
  - Are security policies and procedures to follow throughout the lifecycle of the project identified in BIM Execution Plan (BEP) considering the sensitivity of the built asset, and the confidentiality of the data to be stored in CDE and shared with stakeholders?
  - Are security policies and procedures reviewed and updated regularly, and in case of changes in the threat landscape or experiencing a significant cyber incident?
  - Are security policies and procedures integrated with other project policies and procedures, carefully followed by the project stakeholders, and regularly evaluated to assess their effectiveness?

  - Are security policies and procedures communicated to all project members to create awareness about the security due diligence, the confidentiality level of different types of information, and the requirements of working in a shared data environment?
- **Discussion:** PAS 1192-5 [3] suggests developing a built asset security management plan (BASMP) that identifies policies, processes, and procedures to maintain security during the lifecycle of the project. As an example, a policy can be necessary for managing user access to CDE, and a process related to user access can identify the mechanism to accept or reject access requests by users [3]. On the other hand, a procedure related to user access application may indicate the required information from users such as their role, the access duration, and the privileges needed [3]. The effectiveness of these policies, processes, and procedures may decrease in time with new cyber threats; therefore, regular reviews shall take place for evaluating the performance of these rules. PAS 1192-5 [3] recommends a holistic approach for security that encompasses people, technology tools, and processes since the security measures cannot be effective without due diligence from the individuals.

3.3.2.2 Identity and Access Control

- **Original:**
  - Is access to data sharing systems and networks only available to authorised and personally authenticated users? Is the user access restricted to a limited group of users in the minimum level possible?
  - Is there an additional level of authentication—more secure than single-factor authentication (SFA)—for privileged access and remote user access to data sharing systems and networks? Are these privileged accounts monitored by a user access management system and reviewed regularly?
  - Do devices used for privileged access only serve for internal connections, and not for connecting external websites or e-mail servers?
  - Is there a device identity management system tracking all connected devices to the company network, granting access to only known devices, and allowing the access of third party devices only if the security assurance is provided?
  - Is there a robust user access management system providing the minimum necessary access rights to users, reviewing the permissions regularly, and logging authorised and unauthorised access to network systems?
- **Adaptation:**
  - Is the access to CDE and other data sharing system limited to authorised and authenticated project members with personally granted user access?
  - Is there a more robust authentication system for project members with administrative access rights such as department managers or IT personnel, and users who need to access from remote

locations due to the requirements of the project? Are these privileged accounts monitored and reviewed regularly?

  - Are the devices authorised to make administrative changes to the CDE, and permissioned to modify or delete all project data, only allowed to connect internal project network and not allowed to access external websites?
  - Is there a robust device management system controlling all connections to the CDE and project network to allow the access of only known devices, and granting access to supplier or consultant devices when sharing of CDE is required?
  - Is there a robust user access management system ensuring the minimum required level of permissions to project members, reviewing these permissions regularly, and keeping the record of all authorised and unauthorised access to CDE and project network?

- **Discussion:** Controlled access to CDE by project members, suppliers, and consultants during the design phase is required to ensure the confidentiality, integrity, and availability of sensitive project data. A user access management system and a device identity management system can be developed before the project initiation to be active during the design phase and other project phases. Accounts with privileged user access to CDE and the accounts connecting to CDE from mobile devices, such as mobile phones and tablets, shall be closely monitored to detect any suspicious event in time. While providing robust security for project PCs with required configurations and directly connected to the project network can be relatively manageable, mobile devices that can access to CDE via mobile applications can be more challenging to handle. Therefore, these devices shall be particularly considered as critical in BIM environment. PAS 1192-5 [3] points out the recent trend of "bring your own device (BYOD)" as a security concern for holding sensitive information and suggests necessary measurements to ensure the removal of critical information after the demobilisation of these devices. Another significant matter to manage can be third parties such as design subcontractors, cost consultants, and construction subcontractors that request access permission to CDE. Access shall be granted to these third parties after rigorous security checks, especially in case of working with a company for the first time.

3.3.2.3 Data Security

- **Original:**
  - Do you have a deep understanding and detailed identification of your important data, which may affect your main functions when unavailable, tampered, or lost?
  - Is there robust protection of important data that is transmitted over trusted and non-trusted carriers via data links?
  - Do you have robust security protection of important data stored in the internal storage of the company with only a necessary number of copies, and a secured backup to be used when required?

  - Do you have full control over all mobile devices that store important data, which allows you to erase this data remotely when necessary and configure these devices according to the requirements of your security system?
  - Do you permanently erase the important data from all the devices and equipment with storage before disposal?
- **Adaptation:**
  - Do you have detailed identification of your sensitive project information stored in CDE, such as confidential design details, bill of quantities, and commercial information, which would cause damages if tampered, or accessed by competitors or malevolent parties?
  - Is there robust data protection for transmissions of sensitive project data over trusted and non-trusted carriers?
  - Is there robust data protection for stored data in CDE, which would cause competitive disadvantage, loss or disclosure of intellectual property, financial losses, or reputation damage if accessed by malicious third-parties?
  - Do you have a system to control—or wipe all the sensitive information when necessary—all mobile devices—such as mobile phones, tablets, and project laptops—that can access to CDE?
  - In case of disposal of a project device or equipment with storage, do you erase all information permanently to prevent any possible disclosure of sensitive project information?
- **Discussion:** PAS 1192-5 [3] defines sensitive information as the information that may cause damage—such as loss of intellectual of property, financial loss, and reputation loss—to the organisation when lost, altered, or disclosed. During the design phase of construction projects, sensitive information can include the design details if the project is classified as sensitive, quantity details to be used in the bill of quantities, and any other information that may provide a competitive advantage to competitors if disclosed. Therefore, utilising a system to assess and record the sensitivity of all information stored in CDE from the beginning of the project can be advantageous while granting access to project members and third parties, and defining access limits.

3.3.2.4 System Security

- **Original:**
  - Is the company network designed to support efficient security by having simple data flows, being divided into secure zones, and by allowing easy recovery in case of attacks?
  - Are all the platforms, company network, and information systems configured to the latest versions and settings to ensure robust security?
  - Are all the platforms, company network and information systems maintained and managed only by privileged accounts from isolated devices dedicated to this task?
  - Do you closely follow the announced vulnerabilities for the used software and operating systems and mitigate them, and regularly perform tests to detect vulnerabilities?

- **Adaptation:**
  - Is the CDE utilised in the project designed in a way to support robust security by creating various security zones for different levels of information sensitivity, and allowing easy recovery after a possible attack?
  - Are configurations of CDE and other data sharing systems that hold sensitive information are updated regularly to the latest versions to maintain security?
  - Are there dedicated and isolated devices to make administrative changes to the project network and CDE? Are these changes only managed by privileged accounts assigned to a limited number of trusted project personnel with IT experience?
  - Are the latest announced vulnerabilities by software companies for utilised design authoring tools, operating systems, and CDE platforms carefully followed to be able to perform required mitigations and patch if necessary? Do you or a third-party security consultant make regular vulnerability tests to your systems to detect possible vulnerabilities?

- **Discussion:** Developing a system to assess and record the sensitivity of all project information from the beginning, as suggested in the Data Security section, can be useful for creating various security zones for different levels of sensitivity. This way of designing segregated zones for each level of sensitivity can improve the resilience of the critical project systems. Moreover, providing a high level of protection to all project information without having an assessment for the information sensitivity may increase the total security cost of the project significantly. Vulnerabilities of critical software used in the project—such as design authoring software, CDE platform, and technical analysis software—and operating systems shall be followed to take timely mitigation actions. IT personnel responsible for maintaining the technical security in the project shall be responsible for following these announced vulnerabilities—and patches if available. The latest security configurations for software and operating systems shall be carefully followed to minimise the probability of cyber incidents.

3.3.2.5 Resilient Networks and Systems

- **Original:**
  - Do you have confidence about the resilience of your information systems in case of incidents? Do you make regular security tests to evaluate the effectiveness of your system resilience?
  - Are all utilised networks and information systems designed to be resilient to cyber-attacks? Are systems supporting the primary function of your organisation treated separately from the rest of the network?
  - Is there an automatic system to create backups of all critical information for the continuity of operations? Are these backups held in secured, accessible storage?

- **Adaptation:**
  - Are your project network and CDE capable of returning to functional status in the minimum possible time after experiencing a cyber incident without delaying the ongoing design work? Do you have disaster recovery procedures to follow after a possible cyber incident? Do you have periodical tests for the resilience of your systems?
  - Are the systems utilised for the main design works—that directly affect the project schedule—treated separately from the supporting project work such as business administration functions in terms of security?
  - Is there an automated backup system for critical project data that may have an adverse schedule impact if modified by malicious individuals or lost? Is there robust protection provided for these backups?
- **Discussion:** H. Boyes [5] defines resilience as being ready for any kinds of threat to be able to continue the main business functions. In the design and cybersecurity context, resilience can be defined as being able to maintain the design work critical for the timeline of the project in case of possible cyber incidents. Developing a security breach/incident management plan (SB/IMP) as suggested by PAS 1192-5 [3] can be a solution for providing resilience in construction projects. SB/IMP includes having a process to follow in case of experiencing a breach or incident, having knowledge about the disaster recovery plan of CDE service provider—if applicable—, and having contractually binding liabilities with subcontractors and consultants in case of incidents caused by them [3]. Critical documents and information produced during the design phase can be treated with special attention in terms of disaster recovery to maintain the essential functions and not delaying the main design deliveries after a possible incident.

3.3.2.6 Staff Awareness and Training

- **Original:**
  - Are the employees of your organisation informed about the security priorities of the company and motivated to report any cybersecurity issues they face?
  - Are all the employees in your organisation trained to have cybersecurity awareness regardless of their positions and roles?
- **Adaptation:**
  - Are all project employees aware of security priorities of the project and cybersecurity threats that they may face? Are they recognised for addressing cybersecurity issues of the software and information systems utilised in the project?
  - Is there a routine cybersecurity training for all the stakeholders in the project regardless of their roles and responsibilities?
- **Discussion:** PAS 1192-5 [3] suggests conducting security awareness training for the project personnel to create a security-minded culture within the project. In addition to the general security

awareness training, role-based security training is also recommended for key roles in the project such as information manager, procurement personnel, and supplier or contractor employees responsible for security [3]. A rewarding system for personnel, discovering and reporting cybersecurity issues may improve security awareness. Receiving recognition for helping to maintain a secure environment can be motivating for the project staff.

3.3.3 Monitoring Cybersecurity Activities

3.3.3.1 Security Monitoring

- **Original:**
  - Do you have a robust security monitoring system considering possible cyber threats and cyber-attack methods against your organisation network and information systems?
  - Do you protect logging data against security threats and only allow access in business required cases?
  - Are suspicious logs and activities generate alerts automatically based on indicators of compromise (IoC)?
  - Do you regularly receive updates of virus signatures and IoCs for your information systems?
  - Do you have a monitoring team in your organisation tracking logging data, and developing and following monitoring processes and procedures?
- **Adaptation:**
  - Do you have a robust security monitoring system tracking all logging by project personnel and supplier devices to identify suspicious activities in the information system?
  - Is logging data protected and only accessible by a limited group of project personnel that need it for business reasons?
  - Do suspicious logs and activities in your project network and CDE—either provided by an external host or in-house—trigger alerts?
  - Do you regularly check the updates for virus signatures and compromise indicators for the design software and CDE platform you are using?
  - Is there a team in your IT department responsible for monitoring logging data and suspicious activities?
- **Discussion:** In the design phase of construction projects, there may be many suppliers and project personnel using the project network and CDE. Therefore, it is of utmost importance to track logging data to detect potential threats and suspicious activities. Keeping all the software updated for virus signatures and IoCs is one of the measures to be taken for detecting unexpected logging activity. If an external company provides the CDE service, their measures for monitoring the logging data and automatic security alerts shall be checked with them. Responsibilities for following logging data to project information systems can be assigned to the IT personnel. In case of hosting the CDE in-

house, having a robust security monitoring system can alleviate the risks of potential cyber-attacks against the CDE.

3.3.3.2 Proactive Security Event Discovery

- **Original:**
  - Do you have a system to detect abnormalities in your company network and IT systems, which is supported by the current threats and past experiences?
  - Is there a regular check for system abnormalities to detect any malicious activity and intrusion attempts in advance?
- **Adaptation:**
  - Do you have a detection mechanism for abnormalities in the project network and CDE, which makes use of experienced incidents and threats from previous projects and current known threats?
  - Are there routine abnormality checks for the project network and CDE to detect potential malicious activities by hackers, competitors, or insiders?
- **Discussion:** Having mechanisms to detect abnormalities in information systems can prevent malicious activities as well as hostile reconnaissance. According to PAS 1192-5 [3], during hostile reconnaissance, malevolent parties can be looking for physical vulnerabilities, the security level of the information systems, and some hints that can be used for social engineering. Therefore, detecting suspicious activities in the reconnaissance stage may help in avoiding attacks. Detecting abnormalities in the CDE platform—if it is hosted by an external software company—can be performed with the support of the service provider.

3.3.4 Minimising the Consequences of Cyber Incidents

3.3.4.1 Response and Recovery Planning

- **Original:**
  - Do you have an incident response plan that is developed considering your critical functions, and covers potential attacks and their impacts?
  - Are there sufficient resources—skilled staff, response mechanisms, and external consultant if necessary—to use for response activities in case of attacks?
  - Do you run routine tests for response plans that are developed based on the experiences of your company and other companies?
- **Adaptation:**
  - Is there a functional incident response plan that covers potential attacks against the project network and CDE, and aiming to maintain critical design activities after incidents?

  - Are there enough resources to use for incident response activities, such as skilled staff, IT infrastructure for incident response, and cybersecurity incident response consultancy if required?
  - Are there routine tests for checking the effectiveness of response plans, supported by the experiences from previous projects and experiences of other organisations if available?
- **Discussion:** Having a security breach/incident management plan (SB/IMP) as recommended by PAS 1192-5 [3] can be a solution to maintain the critical design activities after an incident. Incident response plans shall be developed based on the risks particular to the type of project, location of the project, and sensitivity of the information stored in the CDE. A robust plan to follow for the worst-case scenarios is necessary for the resilience of the information systems of the project, and not having adverse schedule impacts. Having the resources necessary for running the incident response plan with full functionality is another significant matter for quick recovery. Training the IT staff about developing and running response plans, and employing state-of-the-art cybersecurity technologies capable of promptly returning the system to its initial state can be beneficial for performing incident response activities effectively.

3.3.4.2 Lessons Learned

- **Original:**
  - Do you perform extensive root cause analysis after cyber incidents as a lessons learned practice?
  - Are there procedures to follow for recording lessons learned in detail after each incident, and implementing these lessons to improve the security?
- **Adaptation:**
  - Do the lessons learned processes and procedures in your project include conducting root cause analysis after cyber incidents?
  - Are all the lessons learned items after cyber incidents recorded in detail to improve the security of project information systems, including the CDE?
- **Discussion:** Analysing the causes of each incident after the occurrence is a good practice for preventing the recurrence of similar incidents and taking quick actions in case of future circumstances. Keeping a record of lessons learned and regularly updating it shall be a part of the project's routines; the results of the root cause of analysis after cyber incidents can be a vital part of the lessons learned.

4 MANAGING SECURITY ISSUES IN THE DESIGN PHASE WITH BLOCKCHAIN TECHNOLOGY

4.1 Security Issues to be Managed by Blockchain Technology

In Chapter 3, fourteen main security concerns in the context of design and BIM processes are addressed as questions to be answered by the cybersecurity personnel of construction projects. These questions cover security issues related to project networks, CDEs, physical assets, people, processes, procedures, and policies. In this chapter, it is aimed to show that some of these concerns can be managed with Blockchain Technology (BCT). In order to manage these issues, a schema showing the integration of BCT in BIM processes is proposed.

Identified cybersecurity issues in Chapter 3 that can be potentially managed with BCT are presented together with their explanations below. Note that it is not claimed to manage these main issues as a whole by BCT, but some particular aspects of the main concerns that are introduced in this section.

- **Supply Chain:** Sensitive project data such as critical design details, pricing information, and engineering calculations that will be shared with suppliers requires potent protection against breaches. Since BCT does not allow for changes in transactions and thus information stored in blocks once they are added to the chain [85], it provides a more tamper-proof environment for data sharing compared to centralised databases. Therefore, BCT helps in maintaining the integrity aspect of the information shared with third-parties. Another advantage of utilising BC systems for data sharing with suppliers is the improved resilience as it allows keeping many copies of the chain in many devices [85]. For this reason, if malicious individuals from suppliers manage to erase the data even though they have read-only access, other copies of the chain can still be used for the continuity of the critical design work.
- **Identity and Access Control:** Another advantage of not being able to make changes in transactions in verified blocks in BC systems is the improved authenticity. Once a document is modified and saved by an authorised stakeholder, the block that holds the transaction logs all the information, hashes all the relevant data, the block is approved by the authorised nodes, and the block becomes a permanent part of the BC. It means that the BC records the owners of the modifications and the originators of documents. In this way, tracking the identities of users who made modifications becomes more manageable and trustworthy. BCT can also provide robust security in terms of access control if a consortium (hybrid) or private BC system is preferred to be utilised. Consortium and private BCs allow restricting the group of people who has permission to read and write data and validate blocks added to the BC [86]. In the example of Hyperledger Fabric, nodes are managed by a system called “Membership Service Provider (MSP)”, which is responsible for assigning node credentials that are used in authorising and

authenticating users [103]. It shows that BCs can be designed in a way to enhance control over user identities and authorisations if they are supported with additional software systems.

- **Data Security:** It is possible to restrict access to data by utilising consortium or private BC systems, as mentioned before. Moreover, employing an additional mechanism similar to the Membership Service Provider (MSP) from Hyperledger Fabric can help in maintaining only authorised access to sensitive data. Another security measure for enhanced confidentiality can be the use of private and public keys for the encryption of data. Usually, cryptocurrency BCs make use of public and private keys for digitally signing the data instead of encrypting since they aim to provide transparent and public ledgers, and the confidentiality of the data in transactions is not a prior concern. However, it is also possible for the sender to encrypt the data with the receiver's public key [104]. In this case, the receiver needs to decrypt the encrypted data to see the original content. Figure 15 illustrates this cryptography mechanism with a simple representation. Employing a similar cryptography approach in the design of the BC system can prevent the unauthorised disclosure of sensitive information.

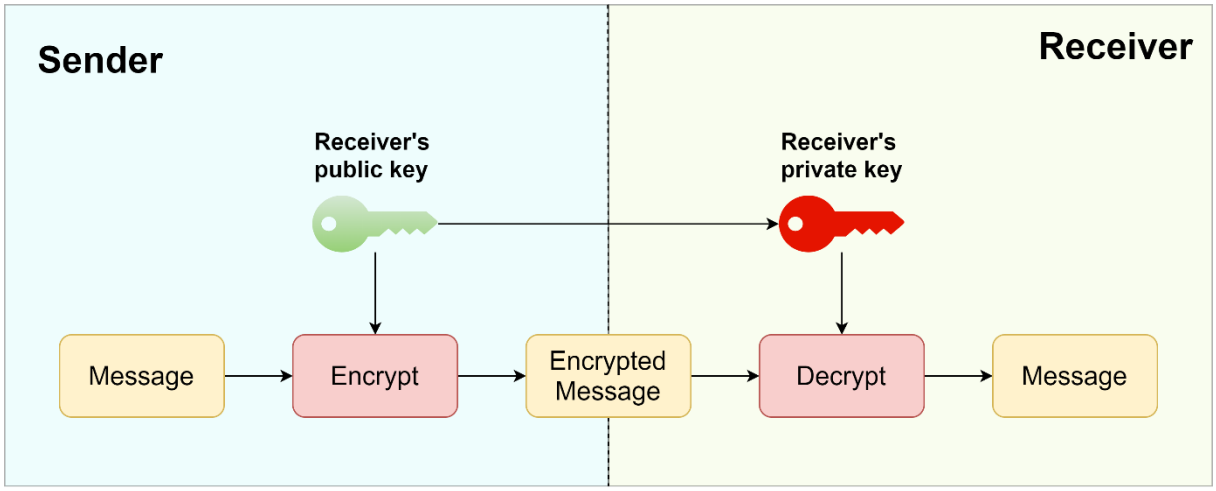

Figure 15: An example of public-key cryptography

- **Resilient Networks and Systems:** As mentioned before in this section, BCT provides robust resilience by allowing many devices (nodes) to store many copies of the whole blockchain [85]. Therefore, a possible deletion of all transactions and data stored in the BC would not create a significant issue in the system unless all copies of the BC are deleted from all user devices, which is a lower probability. The copies of transactions can be considered as backups distributed over the devices; therefore, an additional backup system would be unnecessary. These features validate the claim that BCT enhances the resilience of systems and networks.

4.2 Proposed Schema to Utilise Blockchain Technology and Decentralised Storage

4.2.1 Introduction

In this section, a data sharing architecture is proposed as a solution to abovementioned cybersecurity issues. This architecture makes use of several concepts related to decentralised networks mostly developed in the recent past. Two main concepts that are employed in the proposed schema are BCT and decentralised storage. Despite all the advantages of BCs mentioned previously, storing the BIM data inside the blocks of BC has some disadvantages:

- Most of the successful implementations of BCs, such as financial BCs, involve much smaller data compared to the size of BIM files. Therefore, dealing with huge files in BIM environments can make the whole process slower.
- While having a copy of the BC in each device is an advantage against single point of failure risks, storing each BIM file in the BC will cause the whole chain to grow enormously in size. Every device in the system would not be suitable to handle that amount of data in its storage.
- If the data stored in the block is signed by the private key—similar to the digital signature scheme used in Bitcoin and Ethereum—, it will be possible to verify the message with the public key. However, it will make all the data visible to all participants holding the BC, which is not desirable in BIM environments with a plethora of sensitive information.

For these reasons listed above, the proposed schema involves storing only the hashes—or fingerprints—of each file in the BC instead of the file itself. The hashes are strings unique to each file and do not give any hints related to the content; moreover, it is not possible to reverse the hashing algorithm to figure out the original data [105]. Therefore, even making the BC public does not jeopardise the privacy of the whole data sharing system with this kind of approach. Having the file version history stored in a BC with unique hashes allows verifying the authenticity and integrity of each file at any time in the future by comparing the hashes.

For the storage of the data, the decentralised storage approach is employed to avoid the security disadvantages of central storage systems. Employing a decentralised storage mechanism enables keeping the advantages of BCs such as immutability, identity tracking, and data security while avoiding the mentioned disadvantages for BIM networks. There are some decentralised storage projects under development such as IPFS, Sia, Storj, and Swarm. Some of the characteristics of the proposed schema in this research are inspired by these projects. The details of the decentralised storage system are explained in the following sections.

By combining the BCT and the decentralised storage mechanisms, the data is shared within the peers with improved security and without taking large disk space on each device. The protection for the files is provided by dividing them into smaller chunks of binary files, hashing them to create their unique fingerprints, and storing the chunks of files in objects together with their hashes. In order to re-assemble

the files from the smaller chunks of files, corresponding chunks for the original file shall be known. If the mapping of the original files with the smaller chunks is stored in a hash table, encrypted with public-private key pairs, and only made accessible to authorised participants, protection of the files can be maintained.

4.2.2 Data Structure

Initially, the data structure needs to be explained before going into the details of the hashing mechanism, BC system, and the decentralised storage. In the proposed schema, all shared files are divided into smaller *blocks* of binary files. Dividing the file into smaller blocks is advantageous for both the BC and the storage mechanisms.

Block Size: Block size shall be determined to find the optimum size by considering the average size of the BIM files used in similar construction projects. Optimisation of the size is necessary for optimising the bandwidth use among peers, for better performance in holding the data in the storage, and enabling more efficient deduplication—minimising the used storage by removing the identical copies of the data. For this proposal, the following block sizes are used:

- Files > 256 kb: 256 kb block size (Same as the default block size of IPFS project. Figure 16 illustrates the data blocks of 256 kb)
- Files <= 256 kb: Divide the file into 4 equal pieces (This is necessary for not having any file stored as only one block for the protection mechanism)

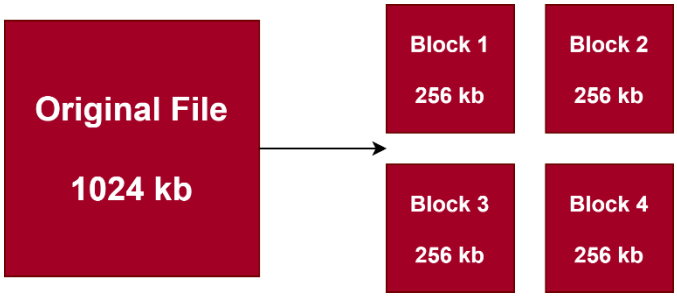

Figure 16: An example of the original file divided into data blocks

4.2.3 Hashing Mechanism, Objects and Merkle Tree

After splitting the original file into smaller blocks of data, each block is hashed to produce a fingerprint. In this proposal, the SHA-256 hashing function is used, which is one of the functions under the SHA-2 hashing algorithm family [105]. Figure 17 illustrates the hashing of each data block with SHA-256 (the hash values in Figure 17 are generated from random files just for illustration purposes).

Each hashed data block is stored in *objects,* which stores the data block, the hash of the block, and a set of metadata. Storing data blocks inside objects helps to link all required metadata to each data

block and creating links with other objects when necessary. Figure 18 shows an example of the object concept.

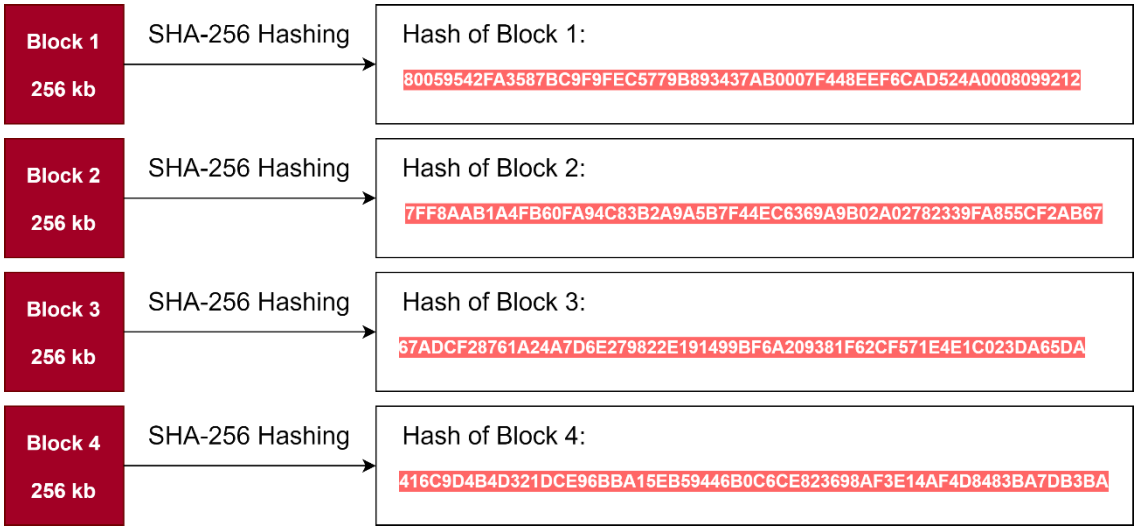

Figure 17: An example of hashing data blocks by the SHA-256 algorithm

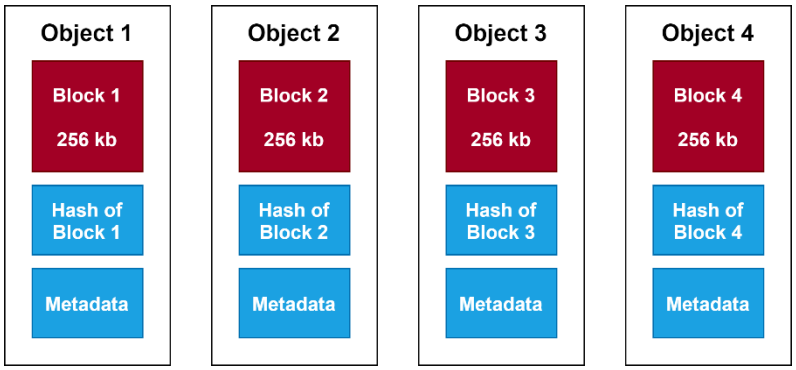

Figure 18: Illustration of objects with data blocks, hashes, and metadata

As explained in the literature review chapter, Merkle trees allow the verification of data structures securely. For this reason, the Merkle tree method is used for calculating the root hash of each file in the system. The objects with data blocks become the leaf nodes of the Merkle tree, and the hashes of parent nodes are calculated starting from these leaf nodes, as shown in Figure 19. Parent nodes do not contain any data in contrast to leaf nodes; they contain a hash value calculated by hashing the concatenation of the children nodes' hashes and a set of required metadata.

On top of the Merkle tree, the object that contains the root hash is placed. The root hash is the fingerprint of the original file since it is calculated starting from the smaller chunks of the file. In the future, the integrity of any file can be verified by calculating the root hash by using the same Merkle tree structure. Any change in the file, —even a minor change—will cause the root hash to change. Note that Figure 19 illustrates two children nodes under each parent node in the Merkle tree; however, the

number of children nodes under each parent node shall be adjustable depending on the file size to optimise the number of hashing.

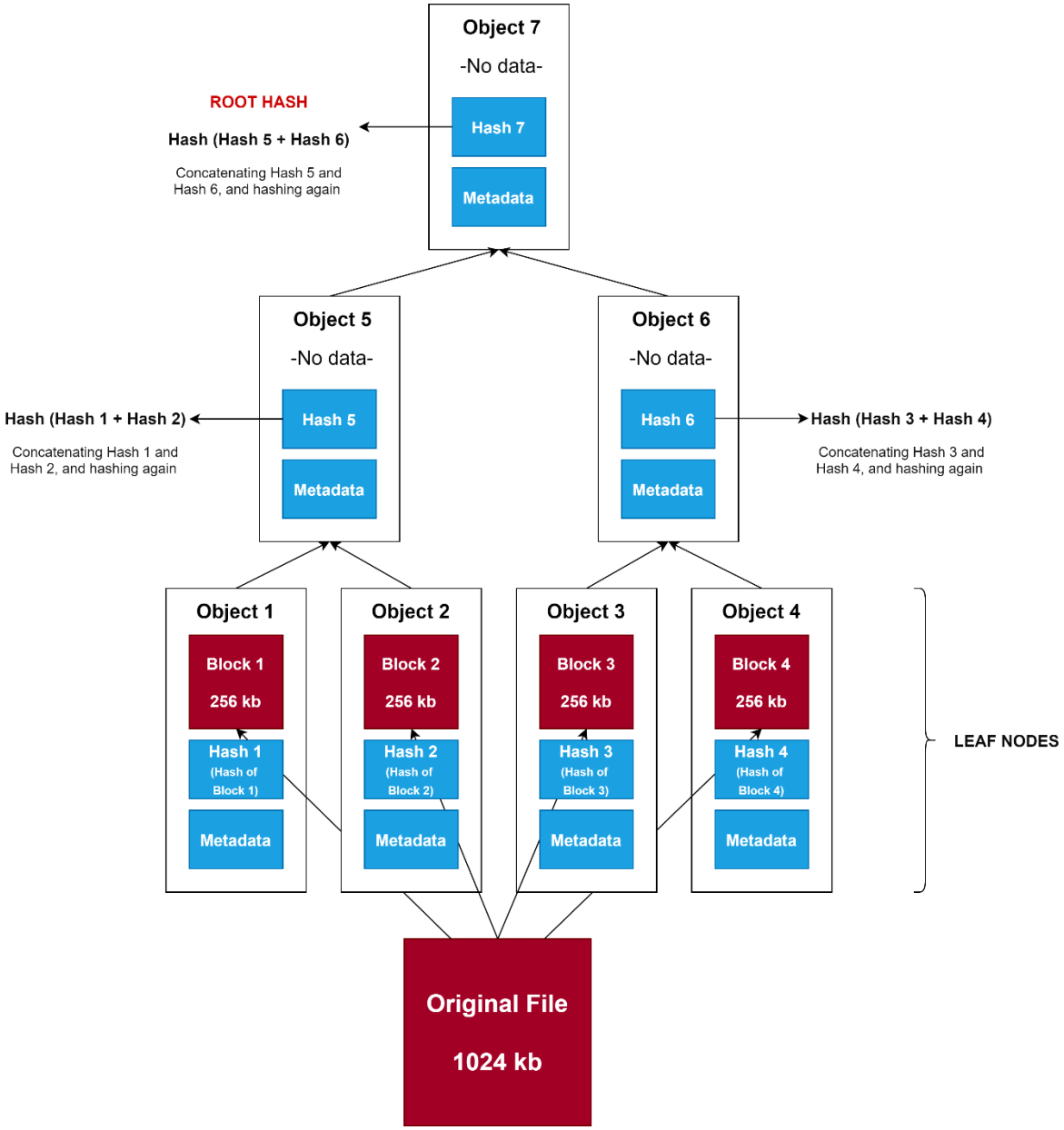

Figure 19: An example of a Merkle tree created from four data blocks

4.2.4 Decentralised Storage for Data

The decentralised storage approach is based on a P2P network where there is no central location to hold the data, and every node in the network pulls the data from the other nodes. This approach has advantages and disadvantages for the networks with relatively fewer nodes, which is usually the case for the BIM environments. Advantages are improved transfer speed by pulling different blocks of data from various peers, reduced risk of a single point of failure by distributing the copies of data across the network, and improved availability by not only relying on a central data server. Disadvantages are the

possibility of having unavailable blocks of data when the peers holding the data are offline and requiring some available storage in each device for holding the data and sharing with others when they request.

In order to avoid the mentioned disadvantages, a node that works as a *super-peer* is included in the proposed schema. This super-peer is a data server that pulls all data blocks as soon as they are available, works continuously with a required power supply, and serves only for storage purpose without being connected to external servers and websites. The super-peer does not turn the whole system into a centralised network since the other peers, as well as the super-peer, still communicate through a P2P protocol. Figure 20 illustrates a simplified version of the proposed storage network in the BIM context.

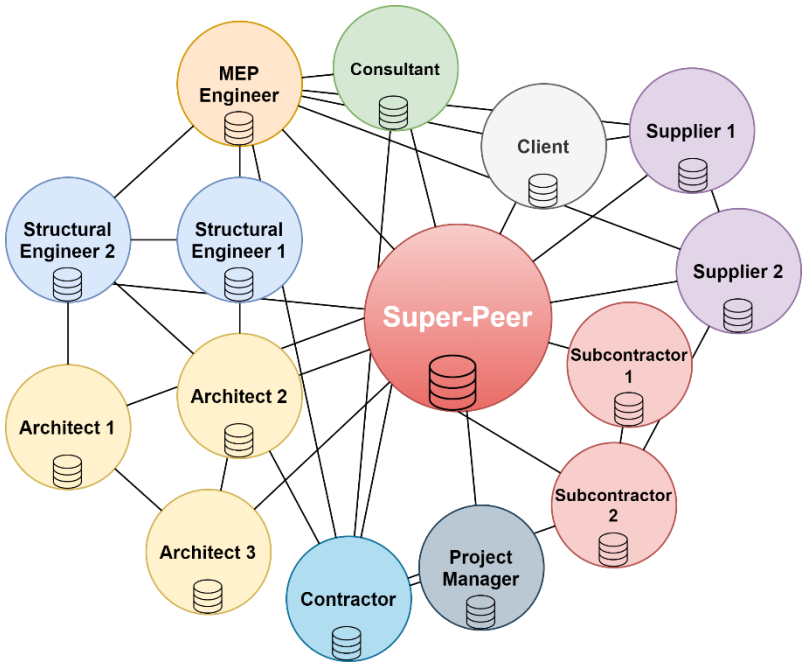

Figure 20: Proposed schema for storage with super-peer in BIM environment

As soon as a peer publishes a file to the network, the file becomes available via its fingerprint which is the root hash of its Merkle tree. However, the root hash alone does not provide access to the file since it is stored as smaller data blocks in the system. Therefore, a stakeholder who wants to access the published file needs to know the root hash of the file and the hashes of data blocks belong to that file. It means that this kind of approach only lets participants request data with a set of hash values. When the stakeholder accesses the relevant hash values, data blocks can be requested from the peers. The required data blocks are pulled from the most suitable peers in the network and reassembled once all the pieces are completed.

Hash Tables: Hash tables are the tables that store the mapping of filenames, the corresponding root hashes, and the corresponding hashes of data blocks. They are crucial for peers to request data from other peers and shall be protected with enhanced security. There should be separate hash tables for separate groups of stakeholders to enable customised access for each group of peers. For instance,

structural design files can be stored in a hash table to be accessed by all engineering group, architects, contractor, project manager, and client; and, when a supplier needs access to a set of structural design files, a customised sub hash table can be provided. Figure 21 illustrates a section of a sample hash table that contains the file name—even though each file is addressed by its hash, file names are still necessary to understand the content—, root hash, data block hashes, and hashing algorithm. Columns of the table can be extended by adding the hashing timestamp, sizes of data blocks, and the person publishing the file.

File Name	Root Hash	Data Block Hashes	Hashing Algorithm
BIMA+2_Group9_Albania_PLM_15-11-2019.rvt	1606FF533E53831AFB011468E855C27348127972939E44D00917525B035B7290	877E60F9658854C6F4CAC1E7468A30ED85F57B0A6A05162721BEAB92FBA5E267	SHA-256
BIMA+2_Group9_Albania_PLM_15-11-2019.rvt	1606FF533E53831AFB011468E855C27348127972939E44D00917525B035B7290	A5B9B1E55D9108A43EF27B7ABA63148F0368AC63B8388A0BAE656AA4A8725695	SHA-256
BIMA+2_Group9_Albania_PLM_15-11-2019.rvt	1606FF533E53831AFB011468E855C27348127972939E44D00917525B035B7290	999F649F41051E4ABE94D550CA68CB5FF1E31DC8CC090E0A993D72D643E25C09	SHA-256
BIMA+2_Group9_Albania_PLM_15-11-2019.rvt	1606FF533E53831AFB011468E855C27348127972939E44D00917525B035B7290	48336F8D1767C0D470062C6DAB48AFDDBE4F737CD3CB99D840703124A9465BA9	SHA-256
BIMA+2_Group9_Albania_ARCH_14-11-2019.rvt	D64AB51CBB81D2EFFD5536A8E85E7F8F27769AD629AFC0D0A7510F1D071DB8B6	9C891AD8B3DC1BB8AEBD6FC86BE57142AA6AD9AF7A2883BC2089BB252B51B10C	SHA-256
BIMA+2_Group9_Albania_ARCH_14-11-2019.rvt	D64AB51CBB81D2EFFD5536A8E85E7F8F27769AD629AFC0D0A7510F1D071DB8B6	B87966BE3481D9BEAB516339EE922DBBF95301F241D0C368DB4F7C5EC9673A18	SHA-256

Figure 21: A section of a sample hash table

Since hash tables have the power of giving access to all files, the protection of them is of vital importance. Therefore, it is proposed to employ public-key cryptography for the protection of each hash table. The proposed protection mechanism is as follows:

- A public/private key pair is generated by secured hardware (SGX by Intel can be used to generate the key pair in a secure enclave).
- The hash table is encrypted with the public key.
- The private key to decrypt the hash table is provided only to authorised people.
- The authorised people decrypt the hash table with the private key and access the hash mapping for requesting the files.
- Public/private key pairs for each hash table are regenerated every n minute where n to be determined by considering the project requirements.

Figure 22 shows the abovementioned encryption mechanism visually.

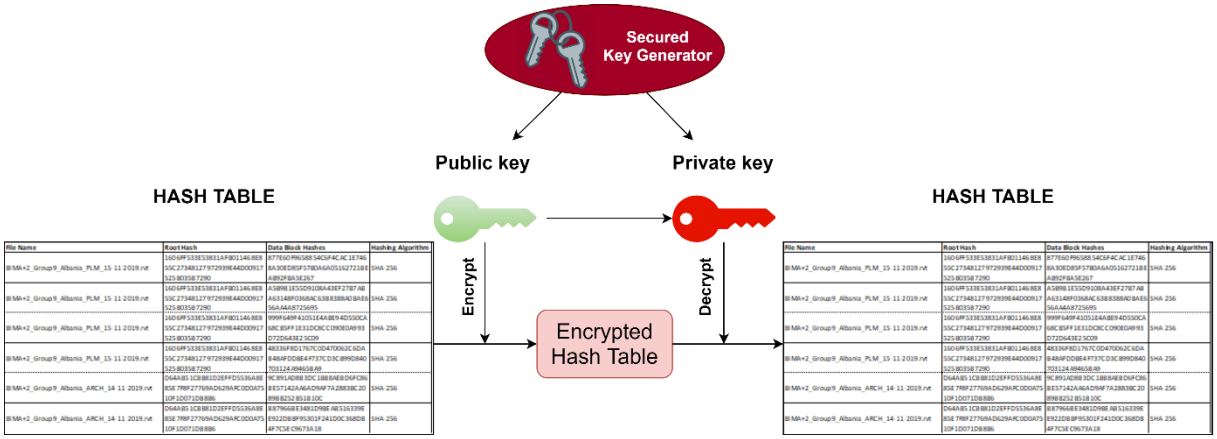

Figure 22: Hash table encryption mechanism

4.2.5 Blockchain for Immutability of Transactions

In this proposed data sharing architecture, the role of BCT is to store the root hashes of each published file together with a timestamp and other relevant metadata for security and verification purposes. It provides an immutable record of all new files and modifications of existing files. In contrast to the financial BC systems, there is no transaction stored in the blocks of the BC. The root hash to be stored in every new block in the BC is calculated by creating the Merkle tree based on the data blocks of the original file. A simple example of this mechanism is shown in Figure 23 for a 1024 kb file. Following features for the BC system are proposed:

- Each block in the BC shall relate to only one file in the system since timestamps and root hashes are unique to each published file in the network.
- Since it is not possible to make changes in the approved blocks, every modification to the existing files shall be published as separate files, and the new block containing the new file's root hash shall be added to the chain. This feature enables a robust version tracking of each file and enhances the intellectual property ownership.
- In terms of privacy, consortium (hybrid) BC is suitable for the needs of the BIM environment, as suggested by Turk and Klinc [85].
- As one of the main characteristics of BCs, every stakeholder shall hold a copy of the chain, which improves the immutability.
- Block validation shall be handled by a set of nodes which can be the delegated members of each team in the project. Including every team in the validation process helps to increase the awareness about changes in design made by different disciplines.
- Delegated Proof of Stake (DPoS) consensus mechanism can be employed for the validation of blocks since all nodes do not have to be involved in the block validation process. Moreover, since there will be a new block added to the chain after publishing each file, consensus

mechanism shall be working fast; and DPoS is a quick option for confirmations of the blocks [86].

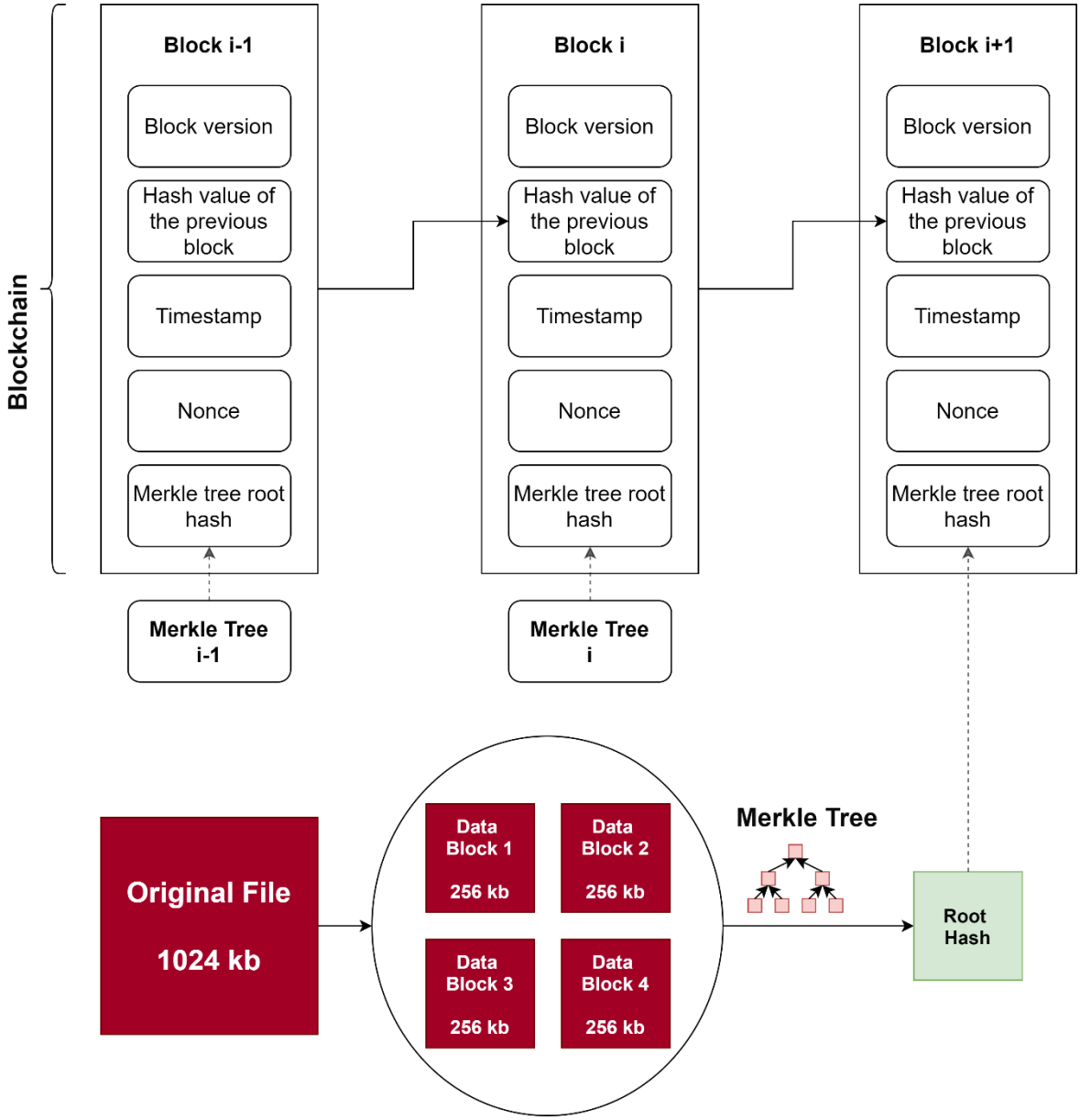

Figure 23: Diagram of adding a new block to the BC after publishing a new file

4.2.6 SWOT Analysis

A SWOT analysis is performed for the proposed data sharing architecture. It can be seen below in Table 3.

Table 3: SWOT analysis of the proposed data sharing architecture

STRENGTHS:	**WEAKNESSES:**
- Immutability is provided by storing the hashes of each file in the BC. Any changes in the files can be easily detected by hashing the file by using the same protocol and comparing the hashes. - Storing only hashes of the files instead of the file itself and the irreversible nature of hashing make it impossible to reach the content of the file when accessed to the BC. - Storing the data in smaller chunks in a decentralised way prevents a single point of failure for the availability and improves the data download speed. - Not storing the data directly in the blocks of BC allows keeping the size of the BC to a minimum. - Involving every team in the block validation mechanism creates awareness about the design changes made by different disciplines in the project.	- Having a fewer number of nodes in BIM networks brings the need of having super-peer storage to store all data in a central location. Therefore, the proposed schema does not totally remove the central storage. - Even though every node in the network does not have to store all the data in its device, having data distributed across the network as much as possible increases the efficiency of the system. However, it causes using the disk space of each device and thus requires a larger storage capacity. - The block validation process gives stakeholders an additional responsibility compared to the current CDE systems.
OPPORTUNITIES:	**THREATS:**
- During or after the completion of the project, any false claim regarding the late delivery of the design or missing project submittals can be disproved by the records in the BC. - During the later stages of the project, version history can easily be accessed when necessary. - Employing the proposed schema may provide a competitive advantage against the competitors in the future tendering processes. - Since all data is distributed across the network, and each file is stored by more than one device, the need for backup systems may reduce.	- Since the information stored in hash tables allows peers to pull data from other peers, a successful intrusion to the hash tables may disclose sensitive information. It can be considered as a single point of failure for the confidentiality of the information. - Having only one file related to each block in the BC may require adding many blocks every day since a new file needs to be published to the network even when a minor change is made. Therefore, many block validations may be needed to be performed, as well. - Even though all files are distributed over the network, super-peer storage guarantees the availability of data at all times. Therefore, a possible cyber attack against the super-peer may pose a significant risk to the availability of the files.

4.2.7 Possible Implementation

The proposed data sharing architecture is defined without going into all technical details in the previous sections, and the SWOT analysis is executed to illustrate what may cause success or failure in the implementation. The proposed architecture shall be considered as an infrastructure rather than a workflow to be followed by the stakeholders. Therefore, users shall not be concerned about all the steps of the process while utilising this architecture such data being divided into data blocks, getting hashed, or stored in a hash table. These parts of the architecture shall be working in the back-end layer. However, block validation for the blockchain or the user interface for the data sharing system can be considered as the front-end layer.

The proposed architecture can be feasible if all the following statements are true:

- The project is classified as sensitive, or there is sensitive project information stored and exchanged between stakeholders.
- The project has in-house data servers that can work continuously and necessary support equipment such as coolers and power supply.
- The project requires sharing data with untrusted third parties such as suppliers and consultants.
- There are enough employees in the project to maintain the block validation process without delaying the primary work activities.
- There are skilled IT personnel for maintaining the proposed data sharing infrastructure.

The proposed architecture can be set up by the IT personnel if there are knowledgeable employees in back-end development, object-based data models, hashing algorithms, BCT, and public-key cryptography. However, in most of the cases, subcontracting the setup and maintenance works of this infrastructure may be more feasible instead of employing IT personnel skilled enough to handle such work.

The infrastructure shall be set up before the project initiation, and the related cybersecurity processes and responsibilities shall be stated in the BEP. The infrastructure shall be tested before its use by the stakeholders to ensure that it works as expected. The security of the system shall be tested by penetration testing tools to exploit vulnerabilities, and these tests shall be maintained during the project lifecycle.

If all of the abovementioned criteria to implement the proposed architecture is not met, and the risk appetite of the project is not aligned with this level of cybersecurity, utilising one of the available and commonly used CDE systems may be a better option.

5 CONCLUSION

This chapter focuses on what were the problems stated in the introduction chapter, how the thesis objectives were met, what outcomes are derived as a result of this research, and what are the suggested future work. The relation between the literature review and the main study is presented.

In collaborative environments of BIM-enabled construction projects, the use of centralised data sharing systems improves the efficiency, helps saving time, and enhances the communication between stakeholders. However, sharing data with third parties such as subcontractors, suppliers, and consultants via centralised data networks such as CDEs significantly increases the risk of external and internal attacks. These attacks may result in financial losses, interruptions of the workflows, and reputation losses.

The digital collaboration between stakeholders, changes in design files, and thus information exchange peak at the design phase of construction projects. It gives rise to concerns related to change tracking in design files, ownership of intellectual property, and the confidentiality of sensitive project information. These concerns during the design phase shall be addressed by a cybersecurity assessment framework to identify the vulnerabilities and assess the security level of the project. Even though there are various generic cybersecurity standards, methods, and frameworks developed by international and national organisations, a sector-specific framework for the construction industry that mainly focuses on the design phase is lacking.

First of all, an extensive literature review has been conducted to identify cyber threats, cyber attackers, and attack motivations from BIM and design perspectives. CDE and IPD approaches have been reviewed from a cybersecurity point of view. Fundamentals of BCT were explained to establish a solid foundation for the study performed in Chapter 4. After the literature review, in Chapter 3, four cybersecurity frameworks and standards published by NIST, ISO/IEC, IIA, and NCSC were reviewed to select the most suitable option for adapting into the BIM environment in the design phase. As a result of the review, the cyber assessment framework from NCSC was selected since it provides clear statements in a checklist format, addresses concerns in sufficient detail, and does not require access to additional documents. A total of fourteen cybersecurity principles that are taken from the original framework were briefly summarised, adapted to the requirements of BIM and design, and discussed to provide suggestions.

In Chapter 4, four of the principles from Chapter 3 that can be managed with the implementation of BCT were identified. These principles are supply chain, identity and access control, data security, and resilient networks and systems. In order to manage the issues related to these principles, a data sharing architecture was proposed that makes use of BCT and decentralised storage approach. Even though BCT has notable benefits for providing a tamper-proof mechanism, storing BIM data in the

blocks of BC has several disadvantages. These disadvantages were listed to justify the need for an alternative storage system.

The proposed architecture utilises a hashing mechanism by the use of Merkle trees to derive the root hash. It is significant to note that the root hash has a vital role in the proposed system since it represents the fingerprint of the published file; moreover, it is stored in the BC to be used for verification purposes in the future. Another distinctive feature of the proposed data sharing system is storing files in smaller chunks of data in a P2P decentralised storage system. Such storage mechanism enables data to be stored by each peer in the network and sharing with other peers. However, such network emerges the need for a super-peer that holds all published data in its storage and stays available at all times, which was explained in detail. In the last sections of Chapter 4, SWOT analysis was performed for the developed architecture, and the criteria for a feasible implementation of the proposed system was presented. Table 4 shows to what extent has the developed architecture solved four targeted cybersecurity concerns mentioned at the beginning of Chapter 4, and what are the remaining issues.

The studies performed in this thesis contributes to the construction field in two significant ways. Firstly, by the cyber assessment framework adaptation performed in Chapter 3 since none of the previously developed frameworks specifically target the design phase of BIM-enabled projects. Therefore, this study underlines the cybersecurity vulnerabilities by considering the tools, processes, and participants of collaborative BIM environments. Secondly, by proposing a data sharing architecture with the use of two technologies; BCT and decentralised storage. Even though several prominent articles have already proposed the use of BCT in BIM such as the bcBIM model by Zheng et al. [106], combining the benefits of decentralised storage approach with the use of BCT provides a distinct way to manage cybersecurity issues.

Future work for the cyber assessment framework should concentrate on improving the details of each fourteen cybersecurity principle mentioned in Chapter 3. In the original framework from NCSC, fourteen main principles are broken down into thirty-nine individual assessments. Therefore, the same level of detail could be provided to make the study more specific. Moreover, the adapted framework should be used in several construction projects to assess its effectiveness and identify weaknesses. For the proposed data sharing architecture, no prototype has been created to validate its functionality, which is the main lacking aspect of the study. Future work should focus on developing a functional model by following the proposed methods and approaches. In this way, the overlooked points while developing the architecture can be identified, and suggestions for improvements can be made.

Table 4: Solved and remaining issues with the proposed data sharing architecture in Chapter 4

Principles from Chapter 3	**Solved issues**	**Remaining issues**
Supply chain	- Storing root hashes of each file in BC provides tamper-proof verification for the authentication and integrity of data. Therefore, an unauthorised change made by the supplier on the file would not create an issue. - Storing data in smaller chunks and sharing the customised hash table with the supplier helps to control the access to sensitive information.	- Since the proposed architecture does not involve storing the data in BC, each file in the network is not kept in each device. Even though the super-peer holds all the information, an attack against the super-peer by a supplier may still cause unavailability of information.
Identity and access control	- Storing the root hashes of each published file together with the metadata such as the owner of the published file in BC allows tracking the identities of participants who made changes or created the original file. - Hash tables control the access to files in the network. They can be customised to grant different access to different users.	- There is no user authentication system provided in the proposed architecture. No mechanism for assigning node credentials is mentioned.
Data security	- Data is stored in smaller data blocks, and the mapping of data block hashes with root hashes is kept in hash tables. These hash tables are secured by public-key cryptography, which provides additional security level.	- Hash tables, which allow access to stored information, are not secured by a tamper-proof mechanism in the proposed architecture. The access to hash tables are limited by encryption; however, they are not protected against unauthorised modifications.
Resilient networks and systems	- Copies of each file's data blocks are ideally stored in more than one device in the network, including the super-peer that stores all files. Therefore, a possible deletion of all files from a device does not interrupt the availability since there will be other copies in other devices.	- Even though the availability of each file's data blocks in more than one device is assumed, each user still has the right to delete any data in its device. For this reason, if some data blocks are only available in the super-peer, a possible attack against the super-peer may cause unrecoverable damage.

6 REFERENCES

[1] H. Boyes, "Cybersecurity and Cyber-Resilient Supply Chains," *Technology Innovation Management Review*, vol. 5, no. 4, 2015, [Online]. Available: http://timreview.ca/article/888.

[2] D. B. Parker, "Toward a New Framework for Information Security," in *Computer Security Handbook*, Fourth., S. Bosworth and M. Kabay, Eds. John Wiley & Sons, 2002, pp. 5.1-5.19.

[3] BSI, "PAS 1192-5:2015 Specification for security-minded building information modelling, digital built environments and smart asset management," *British Standards Institution*, 2015, [Online]. Available: https://shop.bsigroup.com/ProductDetail/?pid=000000000030314119.

[4] O. N. Nawari and S. Ravindran, "Blockchain technology and BIM process: review and potential applications," *Journal of Information Technology in Construction (ITcon)*, vol. 24, pp. 209–238, 2019, [Online]. Available: http://www.itcon.org/2019/12.

[5] H. Boyes, *Resilience and Cyber Security of Technology in the Built Environment*. 2013.

[6] NBS (National Building Specification), "What is the Common Data Environment (CDE)?" https://www.thenbs.com/knowledge/what-is-the-common-data-environment-cde.

[7] BSI, "PAS 1192-2:2013 Specification for information management for the capital/delivery phase of construction projects using building information modelling," *British Standards Institution*, no. 1, pp. 1–68, 2013, [Online]. Available: https://shop.bsigroup.com/Sandpit/PAS-old-forms/PAS-1192-2/.

[8] ENISA (The European Union Agency for Cybersecurity), "Guidelines on assessing DSP and OES compliance to the NISD security requirements," 2018, doi: 10.2824/265743.

[9] C. R. Kothari, *Research methodology: Methods & Techniques*, Second Rev. New Delhi: New Age International (P) Ltd., 2004.

[10] R. Kumar, *Research methodology: A step-by-step guide for beginners*, Fifth. SAGE, 2019.

[11] G. Thomas, *How to do your research project: a guide for students*, Third. SAGE, 2017.

[12] M. Oraee, M. R. Hosseini, E. Papadonikolaki, R. Palliyaguru, and M. Arashpour, "Collaboration in BIM-based construction networks: A bibliometric-qualitative literature review," *International Journal of Project Management*, vol. 35, no. 7, pp. 1288–1301, Oct. 2017, doi: 10.1016/J.IJPROMAN.2017.07.001.

[13] P. E. D. Love, D. J. Edwards, S. Han, and Y. M. Goh, "Design error reduction: toward the effective utilization of building information modeling," *Research in Engineering Design*, vol. 22, no. 3, pp. 173–187, 2011, doi: 10.1007/s00163-011-0105-x.

[14] E. Alreshidi, M. Mourshed, and Y. Rezgui, "Requirements for cloud-based BIM governance solutions to facilitate team collaboration in construction projects," *Requirements Engineering*, vol. 23, no. 1, pp. 1–31, 2018, doi: 10.1007/s00766-016-0254-6.

[15] Principia, "Data Governance Results of the Rapid Survey," 2006. [Online]. Available: ftp://ftp.software.ibm.com/software/uk/info/wp/data_governance_rapid_survey.pdf.

[16] Microsoft, "What is cloud computing?" https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/.

[17] A. Mahamadu, L. Mahdjoubi, and C. Booth, "Challenges to BIM-Cloud Integration: Implication of Security Issues on Secure Collaboration," in *2013 IEEE 5th International Conference on Cloud Computing Technology and Science*, 2013, vol. 2, pp. 209–214, doi: 10.1109/CloudCom.2013.127.

[18] I. Mutis and A. Paramashivam, "Cybersecurity Management Framework for a Cloud-Based BIM Model BT - Advances in Informatics and Computing in Civil and Construction Engineering," 2019, pp. 325–333.

[19] C. Preidel, A. Borrmann, C.-H. Oberender, and M. Tretheway, *Seamless Integration of Common Data Environment Access into BIM Authoring Applications: the BIM Integration Framework*. 2016.

[20] S. Pearson and A. Benameur, *Privacy, Security and Trust Issues Arising from Cloud Computing*. 2011.

[21] C. Eastman, P. Teicholz, R. Sacks, and K. Liston, *BIM Handbook: A Guide to Building Information Modeling for Owners, Managers, Designers, Engineers and Contractors*. John Wiley & Sons, 2008.

[22] G. E. Smith, K. J. Watson, W. H. Baker, and J. A. Pokorski II, "A critical balance: collaboration and security in the IT-enabled supply chain," *International Journal of Production Research*, vol. 45, no. 11, pp. 2595–2613, Jun. 2007, doi: 10.1080/00207540601020544.

[23] B. Becerik-Gerber and D. Kent, "Implementation of Integrated Project Delivery and Building Information Modeling on a Small Commercial Project," 2010. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.705.3757.

[24] AIA (The American Institute of Architects), "Integrated Project Delivery: A Guide," 2007, [Online]. Available: http://www.aia.org/groups/aia/documents/pdf/aiab083423.pdf.

[25] H. Abdirad and P. Pishdad-Bozorgi, "Developing a Framework of Metrics to Assess Collaboration in Integrated Project Delivery," in *50th ASC Annual International Conference*, Mar. 2014.

[26] Z. Ma, D. Zhang, and J. Li, "A dedicated collaboration platform for Integrated Project Delivery," *Automation in Construction*, vol. 86, pp. 199–209, 2018, doi: 10.1016/j.autcon.2017.10.024.

[27] D. Ilozor and D. Kelly, "Building Information Modeling and Integrated Project Delivery in the Commercial Construction Industry: A Conceptual Study," *Journal of Engineering, Project, and Production Management*, vol. 2, Jan. 2012, doi: 10.32738/JEPPM.201201.0004.

[28] B. Becerik-Gerber and K. Kensek, "Building Information Modeling in Architecture, Engineering, and Construction: Emerging Research Directions and Trends," *Journal of Professional Issues in Engineering Education and Practice*, vol. 136, Jul. 2010, doi: 10.1061/ASCEEI.1943-5541.0000023.

[29] B. Succar, "Building Information Modelling framework: A research and delivery foundation for industry stakeholders," *Automation in Construction*, pp. 357–375, May 2009, doi: 10.1016/j.autcon.2008.10.003.

[30] RIBA (Royal Institute of British Architects), "RIBA Plan of Work," 2020. https://www.architecture.com/knowledge-and-resources/resources-landing-page/riba-plan-of-work.

[31] S. Azhar, "Building Information Modeling (BIM): Trends, Benefits, Risks, and Challenges for the AEC Industry," *Leadership and Management in Engineering*, vol. 11, pp. 241–252, Jul. 2011, doi: 10.1061/(ASCE)LM.1943-5630.0000127.

[32] Autodesk, "What Are the Benefits of BIM?" https://www.autodesk.com/solutions/bim/benefits-of-bim.

[33] CURT (Construction Users Roundtable), "Collaboration, Integrated Information and the Project Lifecycle in Building Design, Construction and Operation," no. August, p. 14, 2004, [Online]. Available: https://kcuc.org/wp-content/uploads/2013/11/Collaboration-Integrated-Information-and-the-Project-Lifecycle.pdf.

[34] K. Wong and Q. Fan, "Building information modelling (BIM) for sustainable building design," *Facilities*, vol. 31, no. 3/4, pp. 138–157, Jan. 2013, doi: 10.1108/02632771311299412.

[35] G. Lee, R. Sacks, and C. M. Eastman, "Specifying parametric building object behavior (BOB) for a building information modeling system," *Automation in Construction*, vol. 15, no. 6, pp. 758–776, 2006, doi: 10.1016/j.autcon.2005.09.009.

[36] LODPlanner, "The Ultimate BIM Software List for 2019," 2019. https://www.lodplanner.com/bim-software/.

[37] BuildingSMART, "Industry Foundation Classes (IFC) - An Introduction." https://technical.buildingsmart.org/standards/ifc.

[38] H. Boyes, "Building Information Modelling (BIM): Addressing the Cyber Security Issues," *The Institution of Engineering and Technology*, pp. 1–12, 2014, doi: 10.1049/etr.2014.9001.

[39] E. Pärn and D. Edwards, "Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence," *Engineering Construction & Architectural Management*, Feb. 2019, doi: 10.1108/ECAM-03-2018-0101.

[40] CMAA (The Construction Management Association of America), "An Owner's Guide to Project Delivery Methods," 2012.

[41] Autodesk, "Autodesk BIM Deployment Plan: A Practical Framework for Implementing BIM," pp. 1–42, 2010.

[42] L. Thames and D. Schaefer, "Industry 4.0: An Overview of Key Benefits, Technologies, and Challenges," in *Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing*, L. Thames and D. Schaefer, Eds. Cham: Springer International Publishing, 2017, pp. 1–33.

[43] CISA (Cybersecurity and Infrastructure Security Agency), "What is Cybersecurity?," 2019. https://www.us-cert.gov/ncas/tips/ST04-001.

[44] NCSC (National Cyber Security Centre), "What is cyber security?" https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security.

[45] S. Hooda, "Cybersecurity vs. Information Security: Is There a Difference?," *Cloud Academy*, 2019. https://cloudacademy.com/blog/cybersecurity-vs-information-security-is-there-a-difference/.

[46] ISO/IEC, "ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management," 2005, [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-1:v1:en.

[47] R. von Solms and J. van Niekerk, "From information security to cyber security," *Computers and Security*, vol. 38, pp. 97–102, 2013, doi: 10.1016/j.cose.2013.04.004.

[48] B. R. K. Mantha and B. Garcia de Soto, "Cyber security challenges and vulnerability assessment in the construction industry," in *Creative Construction Conference*, 2019, pp. 29–37, doi: 10.3311/ccc2019-005.

[49] A. A. Cárdenas, S. Amin, Z. S. Lin, Y. L. Huang, C. Y. Huang, and S. Sastry, "Attacks against process control systems: Risk assessment, detection, and response," in *Proceedings of the 6th International Symposium on Information, Computer and Communications Security, ASIACCS 2011*, 2011, pp. 355–366, doi: 10.1145/1966913.1966959.

[50] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-Physical Systems Security - A Survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, 2017, doi: 10.1109/JIOT.2017.2703172.

[51] J. Bakakeu, F. Schäfer, J. Bauer, M. Michl, and J. Franke, *Building Cyber-Physical Systems - A Smart Building Use Case*, no. June. 2017.

[52] ISO/IEC, "ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements," 2013, [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en.

[53] M. Bishop, *Introduction to Computer Security*. Addison-Wesley Professional, 2005.

[54] H. Boyes, "Security, Privacy, and the Built Environment," *IT Professional*, vol. 17, pp. 25–31, Jun. 2015, doi: 10.1109/MITP.2015.49.

[55] S. Thaseen, A. K. Cherukuri, and A. Ahmad, "Improving Security and Privacy in Cyber-Physical Systems," in *Cybersecurity and Privacy in Cyber-Physical Systems*, Y. Maleh, M. Shojafar, A. Darwish, and A. Haqiq, Eds. Taylor & Francis Group, 2019, pp. 3–43.

[56] D. Glavach, J. LaSalle-DeSantis, and S. Zimmerman, "Applying and Assessing Cybersecurity Controls for Direct Digital Manufacturing (DDM) Systems," in *Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing*, Springer Publishing Company, 2017, pp. 173–194.

[57] D. B. Parker, "Toward a New Framework for Information Security," in *Computer Security Handbook*, Sixth., S. Bosworth, M. E. Kabay, and E. Whyne, Eds. John Wiley & Sons, 2014, pp. 3.1-3.23.

[58] A. Davis, "Building Cyber-Resilience into Supply Chains," *Technology Innovation Management Review*, vol. 5, pp. 19–27, 2015.

[59] R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat, "Cyber-physical systems and their security issues," *Computers in Industry*, vol. 100, no. April, pp. 212–223, 2018, doi: 10.1016/j.compind.2018.04.017.

[60] J. M. Stewart, M. Chapple, and D. Gibson, *CISSP Certified Information Systems Security Professional Study Guide*, Seventh. John Wiley & Sons, 2015.

[61] R. Eastman, M. Versace, and A. Webber, "Big Data and Predictive Analytics: On the Cybersecurity Front Line," 2015.

[62] NCSC (National Cyber Security Centre), "Common cyber attacks: reducing the impact," 2016.

[63] M. E. Kabay, "History of Computer Crime," in *Computer Security Handbook*, Sixth., S. Bosworth, M. E. Kabay, and E. Whyne, Eds. John Wiley & Sons, 2014, pp. 2.1-2.41.

[64] S. Mahrach and A. Haqiq, "DDoS Defense in SDN-Based Cyber-Physical Cloud," in *Cybersecurity and Privacy in Cyber-Physical Systems*, Y. Maleh, M. Shojafar, A. Darwish, and A. Haqiq, Eds. 2019, pp. 133–157.

[65] Kaspersky, "What is Zero Day Exploit?" https://www.kaspersky.com/resource-center/definitions/zero-day-exploit.

[66] T. R. Peltier, *Information Security Risk Analysis*, Second. Taylor & Francis Group, 2005.

[67] H. Boyes, "Code of Practice for Cyber Security in the Built Environment," *The Institution of Engineering and Technology*, 2014.

[68] F. Platt, "Physical Threats to the Information Infrastructure," in *Computer Security Handbook*, Sixth., S. Bosworth, M. E. Kabay, and E. Whyne, Eds. John Wiley & Sons, 2014, pp. 22.1-22.28.

[69] C. Falk, "Gray Hat Hacking: Morally Black and White," *Center for Education and Research in Information Assurance and Security*, p. 9, 2004.

[70] M. Dunn Cavelty, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse," *International Studies Review*, vol. 15, no. 1, pp. 105–122, Apr. 2013, doi: 10.1111/misr.12023.

[71] D. B. Parker, "Fighting computer crime - a new framework for protecting information," 1998.

[72] M. Rogers, "The Development of a Meaningful Hacker Taxonomy: A Two Dimensional Approach," 2005. [Online]. Available: https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2005-43.pdf.

[73] Q. Campbell and D. M. Kennedy, "The Psychology of Computer Criminals," *Computer Security Handbook*. John Wiley & Sons, pp. 12.1-12.33, 2014, doi: doi:10.1002/9781118851678.ch12.

[74] S. S. Nidhyananthan, J. S. Kumar, and A. Kamaraj, "Cyber Profiteering in the Cloud of Smart Things," in *Cybersecurity and Privacy in Cyber-Physical Systems*, Y. Maleh, M. Shojafar, A. Darwish, and A. Haqiq, Eds. Taylor & Francis Group, 2019, pp. 393–425.

[75] M. Rogers, "The Psychology of Cyber-Terrorism," in *Terrorists, Victims and Society: Psychological Perspectives on Terrorism and its Consequences*, A. Silke, Ed. John Wiley & Sons, 2003, pp. 77–92.

[76] M. Dahan, "Hacking for the Homeland: Patriotic Hackers Versus Hacktivists," in *8th International Conference on Information Warfare and Security: ICIW 2013*, 2013, pp. 51–57.

[77] A. Segal, "The Rise of Asia's Cyber Militias," *The Atlantic*, 2012.

[78] T. McGuiness, "Defense In Depth," *SANS Institute Information Security Reading Room*, 2001, [Online]. Available: https://www.sans.org/reading-room/whitepapers/basics/defense-in-depth-525.

[79] V. Mani, "A View of Blockchain Technology From the Information Security Radar," *ISACA Journal*, vol. 4, pp. 1–8, 2017, [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-4/a-view-of-blockchain-technology-from-the-information-security-radar.

[80] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System | Satoshi Nakamoto Institute," 2008. [Online]. Available: www.cryptovest.co.uk.

[81] N. O. Nawari and S. Ravindran, "Blockchain and the built environment: Potentials and limitations," *Journal of Building Engineering*, vol. 25. Elsevier Ltd, Sep. 01, 2019, doi: 10.1016/j.jobe.2019.100832.

[82] A. Lastovetska, "Blockchain Architecture Basics: Components, Structure, Benefits & Creation," *MLSDev*, 2019. https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture.

[83] N. Reiff, "Blockchain Explained," 2020. https://www.investopedia.com/terms/b/blockchain.asp.

[84] A. Rosic, "What Is Hashing? [Step-by-Step Guide-Under Hood Of Blockchain]," *Blockgeeks*, 2017. https://blockgeeks.com/guides/what-is-hashing/.

[85] Ž. Turk and R. Klinc, "Potentials of Blockchain Technology for Construction Management," *Procedia Engineering*, vol. 196, pp. 638–645, 2017, doi: https://doi.org/10.1016/j.proeng.2017.08.052.

[86] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *2017 IEEE International Congress on Big Data (BigData Congress)*, 2017, pp. 557–564, doi: 10.1109/BigDataCongress.2017.85.

[87] J. Frankenfield, "Merkle Tree," *Investopedia*, 2020. https://www.investopedia.com/terms/m/merkle-tree.asp.

[88] N. Matthew and R. Stones, *Beginning Linux Programming*, 4th ed. GBR: Wiley, 2007.

[89] F. Glaser, "Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis," in *Proceedings of the 50th Hawaii International Conference on System Sciences (2017)*, 2017, doi: 10.24251/hicss.2017.186.

[90] D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," *International Journal of Information Security*, vol. 1, no. 1, pp. 36–63, 2001, doi: 10.1007/s102070100002.

[91] V. Buterin, "On Public and Private Blockchains," *Ethereum Blog*. 2015, doi: 10.1016/j.pop.2004.02.009.

[92] S. Brakeville and B. Perepa, "Blockchain basics: Introduction to distributed ledgers," *IBM*, 2019. https://developer.ibm.com/technologies/blockchain/tutorials/cl-blockchain-basics-intro-bluemix-trs/.

[93] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 4, no. 3, pp. 382–401, 1982, doi: 10.1145/357172.357176.

[94] M. Bartoletti and L. Pompianu, "An Empirical analysis of smart contracts: Platforms, applications, and design patterns," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017, vol. 10323 LNCS, pp. 494–509, doi: 10.1007/978-3-319-70278-0_31.

[95] I. Belle, "The architecture, engineering and construction industry and blockchain technology," in *DADA 2017 International Conference on Digital Architecture*, Sep. 2017.

[96] E. Muzzy, "What Is Ethereum 2.0?," *Consensys*, 2020. https://consensys.net/blog/blockchain-explained/what-is-ethereum-2/.

[97] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017, vol. 10401 LNCS, pp. 357–388, doi: 10.1007/978-3-319-63688-7_12.

[98] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2016, vol. 9591, pp. 112–125, doi: 10.1007/978-3-319-39028-4_9.

[99] D. Larimer, "Delegated proof-of-stake (dpos)," *Bitshare whitepaper*, 2014.

[100] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On security analysis of proof-of-elapsed-time (PoET)," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017, doi: 10.1007/978-3-319-69084-1_19.

[101] L. W. Cong and Z. He, "Blockchain Disruption and Smart Contracts," *The Review of Financial Studies*, vol. 32, no. 5, pp. 1754–1797, Apr. 2019, doi: 10.1093/rfs/hhz007.

[102] Hyperledger, "An Introduction to Hyperledger," 2018. [Online]. Available: https://www.hyperledger.org/wp-content/uploads/2018/08/HL_Whitepaper_IntroductiontoHyperledger.pdf.

[103] E. Androulaki *et al.*, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in *Proceedings of the 13th EuroSys Conference, EuroSys 2018*, Apr. 2018, vol. 2018-Janua, doi: 10.1145/3190508.3190538.

[104] A. Salomaa, *Public-Key Cryptography*, Second. Springer-Verlag Berlin Heidelberg, 1996.

[105] P. Nohe, "Re-Hashed: The Difference Between SHA-1, SHA-2 and SHA-256 Hash Algorithms," *Hashedout*, 2018. https://www.thesslstore.com/blog/difference-sha-1-sha-2-sha-256-hash-algorithms/.

[106] R. Zheng, J. Jiang, X. Hao, W. Ren, F. Xiong, and Y. Ren, "bcBIM: A Blockchain-Based Big Data Model for BIM Modification Audit and Provenance in Mobile Cloud," *Mathematical Problems in Engineering*, vol. 2019, p. 5349538, 2019, doi: 10.1155/2019/5349538.