A GENERIC BLOCKCHAIN PROCESS REFERENCE MODEL FOR SOFTWARE DEVELOPMENT IN SAFETY CRITICAL DOMAINS

A THESIS SUBMITTED TO

THE GRADUATE SCHOOL OF INFORMATICS OF

MIDDLE EAST TECHNICAL UNIVERSITY

BY

MERVE VİLDAN BAYSAL

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN

INFORMATION SYSTEMS DEPARTMENT

JANUARY 2024

A GENERIC BLOCKCHAIN PROCESS REFERENCE MODEL FOR
SOFTWARE DEVELOPMENT IN SAFETY CRITICAL DOMAINS

Submitted by MERVE VİLDAN BAYSAL in partial fulfillment of the requirements for the degree of **Doctor of Philosophy in Information Systems Department, Middle East Technical University** by,

Prof. Dr. Banu Günel Kılıç
Dean, **Graduate School of Informatics** ____________________

Prof. Dr. Altan Koçyiğit
Head of Department, **Information Systems** ____________________

Asst. Prof. Dr. Özden Özcan Top
Supervisor, **Information Systems, METU** ____________________

Assoc. Prof. Dr. Aysu Betin Can
Co-Supervisor, **Information Systems, METU** ____________________

Examining Committee Members:

Prof. Dr. Altan Koçyiğit
IS, Middle East Technical University ____________________

Asst. Prof. Dr. Özden Özcan Top
IS, Middle East Technical University ____________________

Prof. Dr. Banu Günel Kılıç ____________________
IS, Middle East Technical University

Assoc. Prof. Dr. Ayça Kolukısa
Computer Engineering Dept., Hacettepe University ____________________

Assoc. Prof. Dr. Nurcan Alkış Bayhan
Technology and Information Management, Baskent University ____________________

Date: 26.01.2024

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name : Merve Vildan Baysal

Signature :

ABSTRACT

A GENERIC BLOCKCHAIN PROCESS REFERENCE MODEL FOR SOFTWARE DEVELOPMENT IN SAFETY CRITICAL DOMAINS

Baysal, Merve Vildan
Department of Information Systems
Supervisor: Asst. Prof. Dr. Özden Özcan-Top
Co-Supervisor: Assoc. Prof. Dr. Aysu Betin Can

January 2024, 173 Pages

In recent years, blockchain technology has garnered significant interest and shown promises in various safety critical domains such as health, automotive, and energy. In safety critical domains, any failure or malfunction of a system or technology could potentially result in significant harm, injury, or damage to the environment. Therefore, ensuring the safety, reliability, and correctness of operations within these domains is crucial and often subject to strict regulations, standards, and rigorous testing procedures. Although these domains are highly regulated, there are currently no studies presenting the essential blockchain processes, practices, and development guidelines for ensuring compliance with related regulations. To resolve this deficiency, this study introduces a comprehensive Blockchain dApp Process Reference Model (BDRM) tailored for health, energy, automotive domains. BDRM was developed through a systematic review of both formal and informal literature, leveraging expert insights to define precise processes and practices. Design science research was applied during the development of the model. The model integrates the requirements of the ISO/IEC 12207 alongside health-focused standards (i.e. IEC 62304, IEC 82304, ISO 14971) automotive-specific standards (i.e. ASPICE, ISO 26262), and energy domain-related standards (i.e IEC 61508) to ensure regulatory compliance. Comprising 15 processes and 68 practices, its applicability was confirmed through multiple case studies. The proposed BDRM would provide benefit to developers, researchers, and decision-makers by providing a valuable resource for the development of blockchain-based applications in safety critical domains.

Keywords: Blockchain, dApp, Safety Critical Domain, Process Reference Model, Standards

ÖZ

GÜVENLİK KRİTİK ALANLARDA YAZILIM GELİŞTİRME İÇİN GENEL BLOKZİNCİR SÜREÇ REFERANS MODELİ

Baysal, Merve Vildan
Doktora, Bilişim Sistemleri Bölümü
Tez Yöneticisi: Dr. Öğr. Üyesi Özden Özcan Top
Tez Yöneticisi: Doç. Dr. Aysu Betin Can

Ocak 2024, 173 sayfa

Son yıllarda, blokzincir teknolojisi sağlık, otomotiv, enerji gibi çeşitli güvenlik kritik alanlarda büyük ilgi görmekte ve potansiyel vadetmektedir. Güvenlik kritik alanlarda, herhangi bir sistem veya teknolojinin arızası önemli zararlara, yaralanmalara veya çevreye hasara yol açabilir. Bu nedenle, bu alanlardaki işlemlerin güvenliği, güvenilirliği ve doğruluğunu sağlamak son derece önemlidir ve genellikle sıkı düzenlemelere, standartlara ve titiz test prosedürlerine tabidir. Ancak ilgili düzenlemelere uyumluluk için gerekli olan temel blokzincir süreçlerini, uygulamalarını ve geliştirme yönergelerini içeren kapsamlı çalışmalar mevcut değildir. Bu eksikliği gidermek amacıyla, bu çalışma sağlık, enerji, otomotiv alanları için özelleştirilmiş bilgiler içeren genel bir Blokzincir Uygulama Süreç Referans Modeli (BDRM) önermektedir. BDRM, literatürün sistematik bir incelemesi yapılarak, süreçleri ve uygulamaları belirlemek için uzman görüşleri dikkate alınarak geliştirildi. Modelin geliştirilmesi sırasında tasarım bilimi araştırması uygulandı. Mevzuat uyumluluğuna yönelik olarak ISO/IEC 12207 standardının gerekliliklerini sağlık odaklı standartlar (IEC 62304, IEC 82304, ISO 14971), otomotive özel standartlar (ASPICE, ISO 26262) ve enerji alanı ile ilgili standartlar (IEC 61508) ile bütünleştirmektedir. 15 süreç ve 68 uygulamayı içeren modelin uygulanabilirliği birden fazla vaka çalışması ile doğrulanmıştır. Önerilen BDRM, blokzincir tabanlı uygulamalarının geliştirilmesi için bir kaynak olması yönüyle geliştiricilere, araştırmacılara ve karar vericilere fayda sağlayabilir.

Anahtar Sözcükler: Blokzincir, dApp, Güvenlik Kritik Alan, Süreç Referans Modeli, Standartlar

To My Family

ACKNOWLEDGMENTS

I would like to express my heartfelt gratitude to my advisors, Assistant Professor Dr. Özden Özcan-Top, and Associate Professor Dr. Aysu Betin Can for their unwavering guidance, encouragement, and support throughout my thesis study.

In addition, I want to extend my appreciation to my wonderful family: Tacettin, Oya Selma, Ahsen, and Safa Muhsin Şimşek, as well as my amazing grandfather, Muhsin Şimşek, for their continuous concern and support during this challenging journey.

I am completing this challenging process, which I initially undertook on my own, with my beloved husband and 3-year-old son. I would like to offer special thanks to my husband, Osman Nuri Baysal, for his unwavering help and support throughout my doctoral program. His encouragement has been my pillar of strength.

Most importantly, I want to express my deepest gratitude to my dear son, Volkan Emir Baysal. Having you by my side has brought immeasurable joy to this journey, and I am incredibly fortunate to have you in my life.

Thank you all for being a vital part of this significant achievement in my academic and personal life.

With warm regards,

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

API	Application Program Interface
BDRM	Blockchain dApp Process Reference Model
dApp	Decentralized Application
DSRM	Design Science Research Methodology
EHRs	Electronic Health Records
FDA	U.S. Food and Drug Administration
FL	Formal Literature
GL	Gray Literature
IEEE	Institute of Electrical and Electronics Engineers
IT	Information Technology
ISO	International Organization for Standardization
IEC	The International Electrotechnical Commission
MDD	Medical Device Directives
MDR	Medical Device Regulation
SQuaRE	Software product Quality Requirements and Evaluation
SaMD	Software as a Medical Device
MDS	Medical Device Software

CHAPTER 1

INTRODUCTION

Blockchain technology, known for its decentralized and immutable nature, serves as a distributed ledger system, recording transactions across a network of computers. Its primary attributes include transparency, security, and the elimination of intermediaries in data transfer processes.

In safety critical domains—such as health, automotive, and energy—where system failure can lead to significant harm, injury, or damage, blockchain holds immense potential. Its ability to provide secure, transparent, and tamper-proof records enhances data integrity and reliability within safety critical domains. Recognizing blockchain's potential in safety critical domains, this thesis endeavors to harness its capabilities by introducing a generalized Blockchain dApp Process Reference Model (BDRM).

This thesis introduces a generic BDRM encompassing blockchain dApp development processes. It also provides insights into tailoring this framework specifically for safety-critical domains such as health, energy, and automotive by incorporating domain-specific information for ensuring compliance with related regulations in these domains.

This chapter outlines the background details and includes the discussion of the identified problem. The study's objective is clarified prior to addressing its significance. Subsequently, the research strategy employed in developing the BDRM is stated.

1.1.Background of the Problem

The blockchain technology is characterized by its decentralized and distributed nature, enabling multiple entities to securely and transparently record and monitor transactions. The utilization of tamper-evident and tamper-resistant technology ensures the establishment of a dependable system for managing data. A blockchain system is comprised of a distributed network of computational devices, commonly referred to as nodes, which undertake the task of verifying and documenting transactions onto a publicly accessible ledger. Cryptographic functions are employed to ensure the security of each transaction, which is subsequently appended to a block (Yaga et al., 2018). These blocks interconnect with the preceding blocks and form a sequential series of blocks.

Decentralized applications, commonly referred to as dApps, are software applications that are developed to operate on blockchain or other distributed ledger systems (Cai et al., 2018). The distributed and open-source nature of these applications characterizes them. According to a report, there has been significant development of blockchain dApps in diverse fields, and their advancement has been occurring steadily (State of the DApps, 2022). Application areas of blockchain technology can be observed in diverse domains such as digital voting (Khan et al., 2018), supply chain management (Kumar et al., 2020), electronic copyrights (Omar et al., 2021), banking and financial services (Schär, 2021), and health applications (Hölbl et al., 2018). It is estimated that the total size of the blockchain market will reach $67.4 billion by 2026, which was $4.9 billion as of 2021 (MarketsandMarket, 2022).

The Energy and Commerce Committee passed a draft bill called the "Deploying American Blockchains Act of 2023" on December 4, 2023. The bill directs the Secretary of Commerce to develop best practices, policies, a Blockchain Deployment Program, and examine the benefits of blockchain technology for federal agencies, aiming to advance blockchain technology in the U.S. The fact that the world's first bills on this subject are being created shows that blockchain technology is promising (ECC, 2023).

Within the various safety critical domains under consideration, the health domain exhibits significant potential for the application of blockchain technology. This potential stems from its ability to enhance data transparency in clinical trials, facilitate the monitoring of data for disease surveillance purposes, enable the collection and sharing of data generated by biosensors for remote patient monitoring, as well as facilitate the tracking and verification of pharmaceutical authenticity (Baysal et al., 2023). One example of a blockchain dApp used in the health domain, is the utilization of blockchain technology for the management of electronic health records (EHRs). These systems facilitate the storage and retrieval of patient-related data pertaining to medications, diagnoses, and treatments within the healthcare provider's domain (Shi et al., 2020). Healthcare providers can effectively safeguard the confidentiality and reliability of shared medical information by simultaneously addressing the inherent risks associated with inaccuracies in health record data (Fan et al., 2018; Tripathi et al., 2020).

Blockchain technology holds significant potential not only in the health domain but also in the automotive and energy industries. In the automotive industry, blockchain technology finds its application in supply chain management, vehicle maintenance and repair, vehicle security, and sales. For instance, a blockchain-based supply chain solution enables transparent tracking of vehicle resources, production stages, and transportation processes, minimizing errors and delays in production and logistics. Moreover, utilizing blockchain can make vehicle maintenance and repair processes more transparent and secure. Concerning vehicle security, blockchain technology can assist in swift and accurate identification of vehicle histories, facilitating quick recalls when necessary. In vehicle sales, blockchain technology aids in recording vehicle histories, contributing to the detection of counterfeit vehicles (Lawson, 2018).

In the energy sector, blockchain technology is applicable in areas such as energy trading, distribution, management, and efficiency. For instance, a blockchain-based energy-trading platform directly connects energy producers and consumers, eliminating intermediaries and optimizing energy transactions. Additionally, blockchain technology enhances the transparency and security of energy resource tracking and management in energy distribution and management processes. Addressing energy efficiency, blockchain technology tracks energy consumption and provides recommendations for energy-saving measures (Nour et al., 2022).

The potential of blockchain technology is substantial; however, it is crucial to recognize and confront the diverse obstacles and hazards that arise in both technological and domain-specific settings. The development of blockchain dApps necessitates the establishment of decentralized systems that enable multiple parties to access and authenticate data. This process presents various challenges, including the testing of decentralized systems (Koul, 2018) and the attainment of interoperability between diverse blockchain platforms (Chattu et al., 2019; Fan et al., 2018). Moreover, within the context of safety-critical systems, the matter of ascertaining responsible entities emerges as a noteworthy apprehension (Schneier, 2021).

The presence of vulnerabilities in smart contracts, characterized by deficiencies or imperfections in their code, has the potential to result in security breaches or the exploitation of blockchain systems (Destefanis et al., 2018; Vacca et al., 2021). In order to address these vulnerabilities, it is crucial to adhere to the recommended guidelines for the development and verification of smart contracts. Furthermore, the augmentation of transaction volumes may give rise to scalability and performance concerns, thereby affecting the efficiency and responsiveness of the system. To tackle these challenges, it is important to optimize the system architecture, carefully choose suitable consensus mechanisms, and effectively implement solutions such as sharding. In addition, it is imperative for blockchain applications in the safety critical domain to comply with stringent regulations in order to safeguard the confidentiality, protection, and authenticity of highly sensitive information (Sylim et al., 2018; Takyar, 2021).

Hence, the implementation of a process reference model that is in accordance with the pertinent standards would offer significant guidance in attaining regulatory compliance, upholding legal and ethical responsibilities, and effectively addressing the aforementioned challenges and risks throughout the development process. Although several prior studies (Antal et al., 2021; Chakraborty et al., 2018b; Marchesi et al., 2020; Nousias et al., 2022) have examined life cycle models for blockchain dApps, a standardized process reference model tailored specifically to blockchain dApps has yet to be established. A process reference model is a conceptual framework that facilitates the advancement, administration, and sustenance of applications within a specific domain. The maturation of processes frequently coincides with the advent of technology, thus necessitating a comprehensive assessment of current development practices and their cohesive presentation. The integration of specialized domain requirements into reference models enhances the ability to adhere to regulatory inspections, particularly in industries with strict regulations.

1.2.Statement of the Problem

The adoption of blockchain technology in safety-critical domains, notably health, automotive, and energy, introduces immense potential owing to its attributes of transparency, security, and decentralization. Blockchains, as tamper-evident and tamper-resistant digital ledgers with distributed, shared, and cryptographic functionalities, offer resilience to alterations and establish a trustworthy environment for stored data. We aim to understand the potential of blockchain technology and identify the development processes of blockchain-based decentralized applications in safety-critical domains in this thesis study.

Despite the safety critical domains being heavily regulated, there is a notable absence of comprehensive studies outlining essential blockchain processes, practices, and development guidelines necessary to ensure alignment with the domain regulations. This gap necessitates the development of a generalized BDRM addressing the needs of safety critical domains, aligning with related standards, and facilitating effective blockchain application development within the health, energy and automotive domains.

1.3.Purpose of the Study

The objective of this study is to introduce a generic BDRM that encompasses the fundamental blockchain processes and practices required for the development of blockchain dApps and specific information about health, energy, and automotive domains. The objective of the model is to establish a shared foundation for the development of blockchain dApps. This is achieved by outlining the fundamental procedures and methodologies while taking into account the guidelines in ISO/IEC 12207 Systems and software engineering - Software life cycle processes (2017), IEC 82304 Health software – Part 1: General requirements for product safety (2016) and IEC 62304 Medical device software – Software life cycle processes (2006), Automotive SPICE (VDA QMC Working Group, 2023). Additionally, the model considers the guidelines specified in ISO 14971:2019 Medical devices – Application of risk management to medical devices (2019), ISO 26262: 2018 Road vehicles - Functional safety (2018), IEC 61508-3:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements (IEC, 2010).

In addition, we explain the utilization of the design science approach in addressing the following research questions during the development of the model:

- RQ1. What are the fundamental processes and practices involved in the development of blockchain dApps?

- RQ2. What are the differences in the development process and practices between blockchain dApp development and traditional software development?

- RQ3. How could the development process and practices of blockchain dApp be specialized to ensure adherence to regulatory requirements in the safety critical domains (i.e. health, automotive, energy)?

1.4.Significance of the Study

We believe this study has the potential to make a substantial contribution to the existing literature and to practitioners in the following areas:

- Dual Purpose: The BDRM serves a dual model by not only guiding development activities but also ensuring compliance with regulatory software development standards. Adapting to these standards often requires a substantial investment of effort and time. The BDRM offers guidance in complying with these standards and serves as a starting point to understand the complex requirements in these domains.

- Addressing Challenges: The BDRM addresses the potential benefits of blockchain technology to the inherent challenges of the safety-critical domains.

- Guidance for Developing Models: The BDRM provides guidance for researchers interested in developing models using the design science research approach.

Based on the available information, we could assert that the BDRM represents a pioneering model that encompasses the requisite processes and practices essential for the development of blockchain-based decentralized applications (dApps) within the safety critical domains. The model is independent of any particular life cycle development model.

1.5.Research Strategy

The research strategy followed through this thesis study is given step by step in Figure 1. The research strategy employed in constructing the BDRM involves a multifaceted approach, integrating theoretical foundations, expert insights, and compliance with established standards. During the development of the BDRM, we followed Runeson *et al.*’s (2020) Design Science Research (DSR) methodology, which comprises five stages: problem conceptualization, solution design, abstraction, instantiation, and empirical validation.

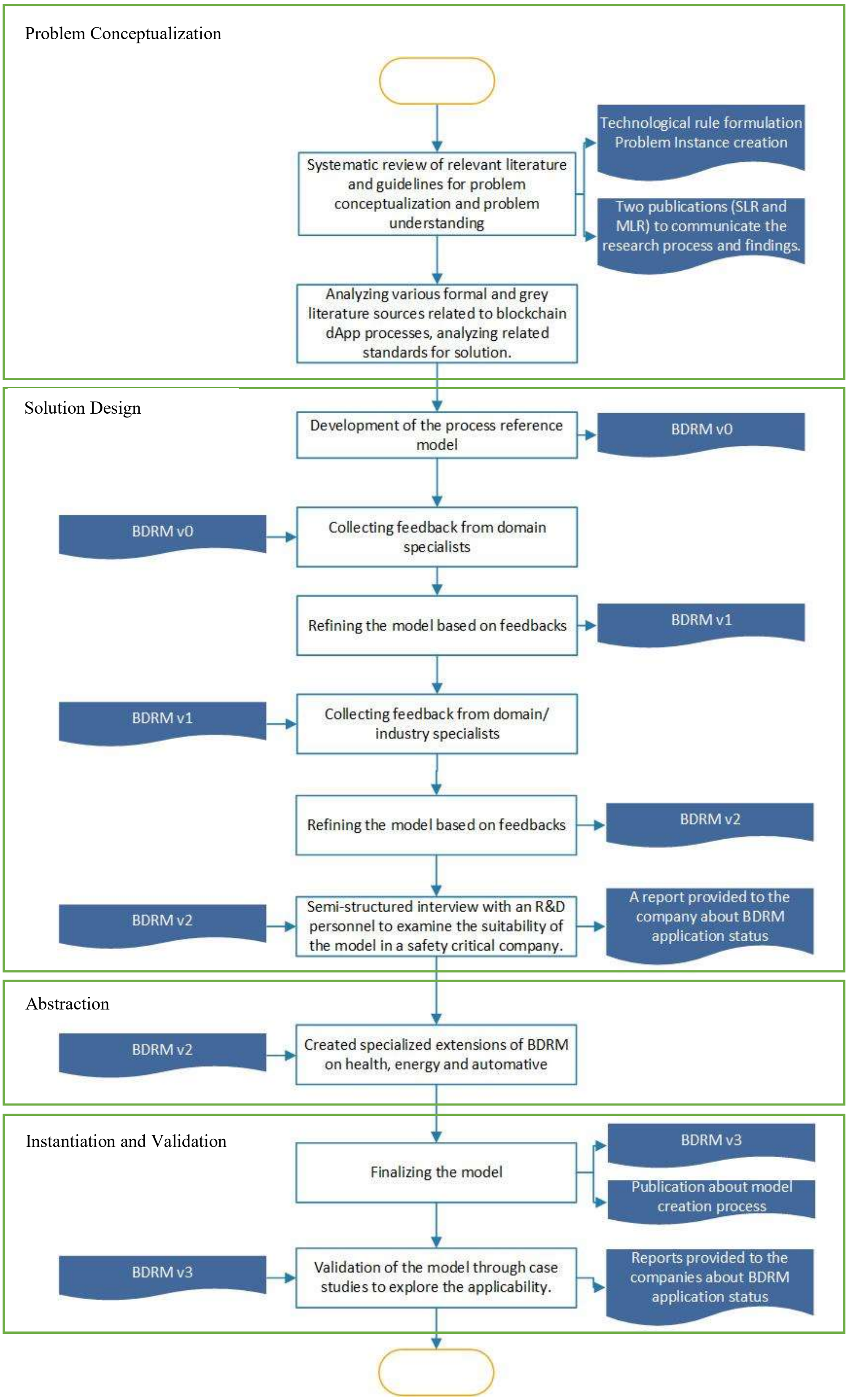

Problem Conceptualization
Systematic review of relevant literature and guidelines for problem conceptualization and problem understanding
Technological rule formulation Problem Instance creation
Two publications (SLR and MLR) to communicate the research process and findings.
Analyzing various formal and grey literature sources related to blockchain dApp processes, analyzing related standards for solution.
Solution Design
Development of the process reference model
BDRM v0
BDRM v0
Collecting feedback from domain specialists
Refining the model based on feedbacks
BDRM v1
BDRM v1
Collecting feedback from domain/ industry specialists
Refining the model based on feedbacks
BDRM v2
BDRM v2
Semi-structured interview with an R&D personnel to examine the suitability of the model in a safety critical company.
A report provided to the company about BDRM application status
Abstraction
BDRM v2
Created specialized extensions of BDRM on health, energy and automative
Instantiation and Validation
Finalizing the model
BDRM v3
Publication about model creation process
BDRM v3
Validation of the model through case studies to explore the applicability.
Reports provided to the companies about BDRM application status

Figure 1: Steps of the Research Strategy

Our objective is to identify the development processes of blockchain-based decentralized applications in safety-critical domains; therefore, we formulated the technological rule in the following manner: To identify the fundamental blockchain processes and practices required for the development of blockchain dApps in safety critical domains, develop a process reference model.

We used the health domain to explore the problem, which is one of the safety-critical domains and subjected to strict regulations, and conducted a systematic literature review (SLR) (Baysal et al., 2021), and multivocal literature review (MLR) (Baysal et al., 2023) for problem understanding. Due to their similar safety-critical characteristics, alongside the health domain, we included the energy and automotive domains in both the solution and validation processes. We analyzed various formal and grey literature sources related to blockchain dApp processes, analyzed related standards (ISO/IEC 12207, IEC 82304, IEC 62304, ISO 14971, ASPICE, ISO 26262, and IEC 61508), collected feedback from domain/industry specialists through two iterations to refine the model, and conducted an interview with an industry expert for solution design. The applicability of BDRM was confirmed through five case studies in the health, automotive, and energy domains, as well as in a general context. We shared the results of the case studies as improvement suggestions with the organizations.

This study aims to deepen the understanding of blockchain technology within safety-critical domains, potentially offering a new perspective and contributing to the existing body of knowledge in this domain. The model emphasizes the process dimension, and the objective of the model does not entail capability assessment. However, it would be possible to use the BDRM in conjunction with the ISO/IEC TS 33061:2021 Information technology - Process assessment - Process assessment model for software life cycle processes standard (2021) to address the capability dimension, as we followed the meta-model structure of the process dimension given in this standard.

1.6.Organization of the Thesis

The subsequent sections of the thesis are organized in the following manner:

- Chapter 2 provides an overview of the safety critical domain software, the structure of blockchain technology, and the results of a literature review in order to identify various processes and practices that are involved in developing blockchain-based applications.

- Chapter 3 includes the details of the systematic and multivocal literature review studies carried out to identify the problem. Health domain is chosen as the pilot domain for safety-critical domains.

- Chapter 4 explains the research methodology that was employed in the development of the BDRM. It also outlines the framework of the BDRM, including the various processes and practices encompassed within this model.

- Chapter 5 includes case study design and conduct for validation of the BDRM. It also provides an overview of the discussions and validity threads.

- Chapter 6 presents the concluding remarks and outlines potential topics for future research.

CHAPTER 2

LITERATURE REVIEW

The purpose of this chapter is to provide information about structure of blockchain technology, safety critical domain software, and review results of literature to identify the various processes and practices involved in the development of blockchain dApps.

Section 2.1 provides information about brief history of blockchain technology and structure of this technology. Section 2.2 explains safety critical domain software. Section 2.3 presents related work on studies that have contributed to the understanding of blockchain dApp development processes.

2.1. Background on Blockchain Technology

The inception of blockchain technology can be attributed to Satoshi Nakamoto, who provided a comprehensive explanation of the Bitcoin cryptocurrency's design and underlying principles (Nakamoto, 2008). The first deployment of the initial blockchain network, functioning as an electronic payment system (Bitcoin, n.d.), occurred in 2009. Subsequently, a multitude of cryptocurrencies, including Ethereum, have emerged (Ethereum, n.d.). Over the course of its development, blockchain technology has undergone substantial advancements, leading to the expansion of its utility beyond the realm of cryptocurrencies. Nevertheless, despite these advancements, the fundamental technologies have predominantly remained unchanged (Yaga et al., 2018). The National Institute of Standards and Technology (NIST) defines blockchain as a distributed digital ledger that is tamper-resistant and tamper-evident, typically without a central authority (Yaga et al., 2018).

Below, we describe the main elements of the blockchain system, as the terminology commonly used in the BDRM and the rest of this thesis. Figure 2 provides a visual representation of the various components that constitute a blockchain system.

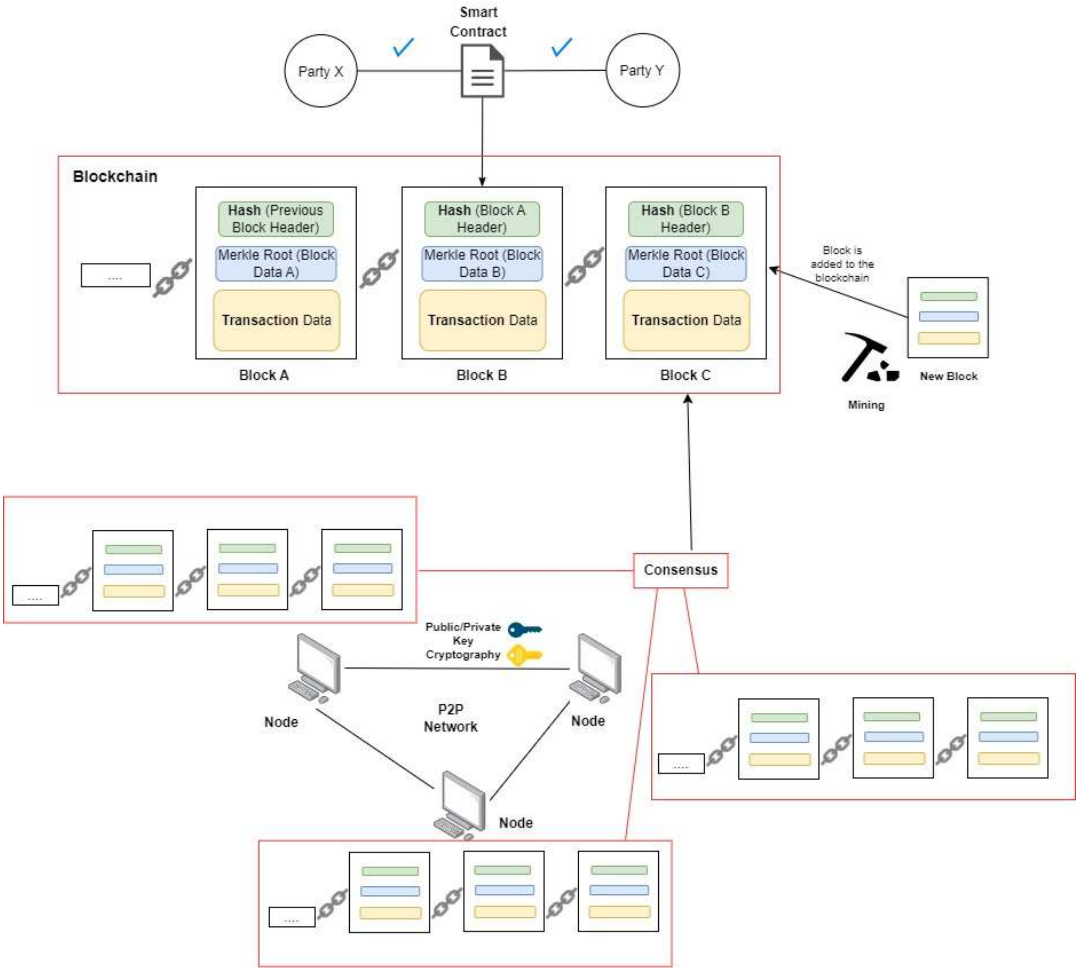


Figure 2: Blockchain Components

The blockchain technology encompasses various components, including *blocks, transactions, nodes, consensus models,* and *smart contracts.* They use *public/private key cryptography, mining,* and *hashing* functions.

Blocks are data structures that exist within a blockchain, serving as containers for permanently recording valid transactions. *Cryptographic hashing* is a computational procedure employed to transform data of varying sizes into a standardized string of fixed length. Every individual block within a blockchain possesses a distinct hash value. Blocks are composed of the hash value of the preceding block, thereby establishing a sequential and interconnected structure. The act of manipulating the data contained within a block would result in an alteration of its hash value, thereby disrupting the connection with the subsequent blocks. Hence, the utilization of hashing is imperative in order to guarantee the integrity of data within blockchain networks. A *transaction* refers to the documentation of an occurrence, such as the exchange of assets between multiple entities or the generation of new assets. Every transaction consists of a sender address, a destination address, the quantity of assets being transferred, and additional metadata such as transaction fees. *Nodes* refer to the computational entities, such as computers or servers that actively engage in the storage and verification of transactions within a blockchain network. In addition, these entities collaborate in order to uphold the integrity, confidentiality, and precision of a blockchain system through the process of validating new transactions and blocks via active engagement in consensus protocols. The *consensus mechanism* refers to the procedural framework employed within a blockchain system to attain consensus or agreement among its participants. The nodes within the network establish a collective comprehension of the network's present condition. *Mining* refers to the computational process involved in solving intricate puzzles within a Proof of Work (PoW) consensus mechanism, which serves the purpose of appending new blocks to the blockchain. A *smart contract* refers to a programmable code and associated data that are implemented through the utilization of cryptographically signed transactions on a blockchain network. Smart contracts are autonomously executed at the nodes once a specific set of predetermined conditions have been satisfied. *Public-private key cryptography*, also known as *asymmetric cryptography*, is a cryptographic method employed to ensure the security of communication and the authentication of involved entities. The process of encrypting messages involves the utilization of public keys, while the decryption process relies on the utilization of private keys. Private keys play a crucial role in blockchain networks as they are utilized for the purpose of signing transactions and validating ownership of assets.

Blockchain networks can be classified into three categories (Yaga et al., 2018): permissionless, permissioned, or a combination of both. *Permissionless blockchain networks* refer to decentralized ledger platforms that allow any participant to publish blocks without requiring prior authorization or approval. In the context of network architecture, *a permissioned network* is characterized by its restriction of block publication to a specific subset of users. The blockchain categories and their corresponding types are illustrated in Figure 3.

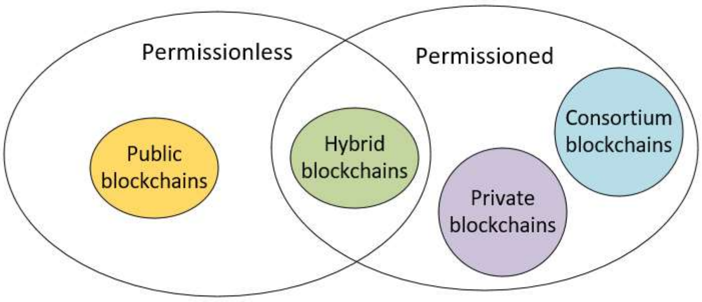


Figure 3: Blockchain Categories and Types adapted from (Jha, 2023)

The most common types of blockchains are given below:

- *Public blockchains* provide a means for individuals to engage in the network, contribute transactions, and assume the role of a validator. The blockchains in question are commonly characterized by their decentralized nature, which indicates the absence of a central governing authority overseeing the network.

- *Private blockchains* are characterized by their limited accessibility, as they are exclusively available to a designated set of participants, such as a single enterprise or a consortium of multiple businesses. Participation in the private network is restricted to the nodes that have been specifically chosen.

- *Consortium blockchains* can be classified as a combination of public and private blockchains. In this type, a collective of organizations that jointly exercise control and governance over the network establishes a network. Consortium blockchains are frequently employed in scenarios where multiple entities necessitate collaboration and the exchange of data.

- *Hybrid blockchains* integrate the characteristics of both public and private blockchains, thereby enabling the advantages associated with public blockchains, such as decentralization and transparency, while simultaneously upholding the privacy and control offered by private blockchains.

Due to the multi-stakeholder structure of the health domain, blockchain applications in this domain frequently require interoperability. The NIST defines blockchain interoperability as "*a composition of distinguishable blockchain systems, each representing a unique distributed data ledger, where atomic transaction execution may span multiple heterogeneous blockchain systems and where data recorded in one blockchain is reachable, verifiable, and referable by another possibly foreign transaction in a semantically compatible manner*". As implied by this definition, information assets will be exchanged and utilized across multiple ledgers, and this exchange must be verifiable. Although the NIST defines interoperability as communication between heterogeneous blockchain systems, Belchior et al.'s (2022) definition also includes communication between homogeneous blockchain systems. In both cases, transactions require a trusted third party to ensure the correctness of underlying protocols (Belchior et al., 2022). During a multi-ledger transaction, a source blockchain issues a transaction against a target blockchain and an exchange occurs between the source node and the target node. When participants select a source node from the source blockchain and a target node from the target blockchain, decentralization is achieved (Belchior et al., 2022).

2.2. Safety Critical Domain Software Overview

A safety-critical domain is an area where malfunctioning of systems or software can have severe consequences, including:

- Loss of life or serious injury: This is the most critical consequence, with examples like medical devices, aircraft flight control systems, automotive systems, and nuclear power plants.

- Significant environmental damage: This could involve chemical spills, oil spills, or other environmental disasters caused by system failures.

It is critical to guarantee the safety, reliability, and correctness of operations in these domains; consequently, they are often subject to strict regulations, standards, and rigorous testing procedures.

In the following headings, we provide information about three safety critical domains: health, automotive, and energy.

2.2.1 Health Domain Software Overview

Health domain software covers a wide range of applications used in healthcare and well-being. These programs are crucial for various aspects of medical care, patient management, and personal health.

As previously stated, the process of aligning the health domain specifications with the BDRM involved the utilization of established standards such as IEC 82304 Health software – General requirements for product safety (2016) and IEC 62304 Medical device software – Software life cycle processes (2006), and ISO 14971:2019 Medical devices – Application of risk management to medical devices (2019). This section provides an overview of the various categories of health domain software and offers a description of the content found within the aforementioned standards.

Health domain applications are subject to audits by different regulatory agencies, which vary depending on the specific region where the product is marketed. Health domain software in the United States is subject to regulation by the U.S. Food and Drug Administration (FDA) (FDA, n.d.). In order to guarantee the security and efficiency of applications intended for patient use, the FDA requires software developers to comply with pertinent health domain standards throughout the entirety of the development process. The regulation of health domain software in the European Union is governed by the Medical Device Regulation (MDR), which superseded the preceding Medical Device Directives (MDD) (2017). Ensuring adherence to pertinent health domain standards is of utmost importance in acquiring the CE mark, denoting conformity with European regulations and enabling the software’s commercialization and utilization within the European Union.

The regulatory standards related to software in the health domain exhibit variability depending on the specific category of software and its intended purpose. The software within the health domain can be categorized into two distinct groups: Health Software and Medical Software. The categories of health domain software in terms of regulatory compliance requirements are depicted in Figure 4, which has been adapted from Heidenreich’s (2014) study. Health software must adhere to the IEC 82304 standard, while medical software is governed by the IEC 62304 standard. ISO 14971 has the potential to be implemented in the health domain, encompassing Health Software as well as Medical Software.

The IEC 62304 standard offers guidance pertaining to the processes involved in the software development lifecycle for software utilized in medical devices. The present standard delineates the requisite activities, documentation, and controls essential for the progression, authentication, and substantiation of software employed in medical devices. The IEC 82304 standard is applicable to software utilized within the healthcare domain. The objective of this standard is to establish a comprehensive structure for guaranteeing the safety of health software applications and assisting organizations in the development and upkeep of software that is of superior quality and ensures safety within the health domain. The IEC 82304 standard provides guidance on software life cycle processes. It advises users to refer to the IEC 62304 standard and adhere to its prescribed steps. The ISO 14971 offers comprehensive guidance on the management of risks associated with health domain software, encompassing both the development and post-market stages.

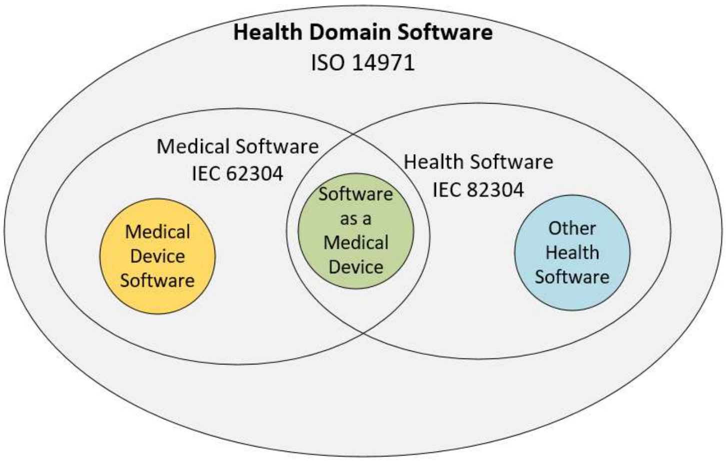


Figure 4: Health Domain Software Categories and Standards—adapted from (Heidenreich, 2014)

The Health Domain Software categories depicted in Figure 4 are explained as follows:

- *Software as a medical device (SaMD)* pertains to software applications designed for medical use, obviating the necessity for supplementary hardware. These applications are considered medical devices on their own. Software applications that fall under the category of Software as a Medical Device (SaMD) encompass various functionalities, including clinical decision support, diagnostic analysis of medical data for diagnostic insights or predictions, physiological parameter monitoring and tracking (e.g., heart rate, blood pressure, glucose levels), as well as treatment planning and guidance.

- *Medical device software (MDS)* pertains to software that is incorporated into a medical device, commonly operating on the device itself or on a specialized embedded system. Several instances of Medical Device Software (MDS) can be observed, including software integrated within implantable medical devices like defibrillators, pacemakers, neurostimulators, or drug delivery systems. Additionally, software embedded in infusion pumps and systems designed to continuously monitor glucose levels in patients with diabetes also serve as examples of MDS.

- *Health software* encompasses a diverse array of applications pertaining to the domains of healthcare and overall well-being. This category encompasses software applications such as fitness tracking, wellness management, telemedicine, and electronic health records (EHR) management.

2.2.2 Automotive Domain Software Overview

Automotive domain software refers to the software applications and systems that are used within automobiles or in the automotive industry. In order to include the automotive domain specifications in the BDRM, established standards including Automotive SPICE and ISO 26262 were utilized. This section presents an outline of the various categories of automotive domain software and offers an explanation of the description of the content within the aforementioned standards.

Software in the automotive domain could be decomposed into the categories of vehicle operational software, vehicle information security software, and vehicle experience software. The automotive domain software categories and example applications (Trustradius, 2023) are explained as follows:

- *Vehicle operational software* category covers a wide range of applications including manufacturing, logistics, supply chain operations, connected car software, performance and efficiency-focused systems. Additionally, it comprises vehicle driving software such as Vehicle Operating Systems (VOS) controlling core vehicle functions like engine management, transmission control, braking, and steering; Advanced Driver-Assistance Systems (ADAS), such as automatic emergency braking, lane departure warning, adaptive cruise control, and parking assistance; Autonomous Driving Systems (ADS) enabling a vehicle to operate without driver input.
- *Vehicle information security software* category encompasses software designed to ensure the digital security of vehicles, safeguard data privacy, and take preventive measures against potential cyber threats.
- *Vehicle experience software* category includes software systems focused on improving driver and passenger experiences. These systems include a variety of functions, such as radio, music player, navigation system, smartphone connectivity, software that controls features such as sound system, ambient lighting, and seat settings. Additionally, software for car dealership/rental, automotive marketing is also in this category.

In the automotive domain, there is no industry-specific standard for blockchain software development processes. ISO 26262, which is a functional safety standard for road vehicles, covering software development, safety lifecycle, and risk management standards, helps to ensure the safety and functionality of the systems. This standard could be utilized in applications within the vehicle operational software category.

Automotive SPICE (Software Process Improvement and Capability Determination) provides a framework for improving and determining the capability of software processes in the automotive domain. This framework is used particularly to manage and assess software development processes. It can be considered a general standard for any automotive software, rather than specifically for usage within a particular category. Therefore, this standard could be applied to software in the automotive domain, including the identified three categories.

2.2.3 Energy Domain Software Overview

Energy domain software refers to a broad range of software applications specifically designed for the generation, transmission, distribution, trading, consumption, and management of energy resources. To include the energy domain specifications into the BDRM, potentially applicable standards were utilized, such as IEC 61508-3:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems - Software requirements. This section provides a comprehensive overview of the various categories of energy domain software, and potentially applicable standards in this domain.

Software in the energy domain could be decomposed into the categories of energy management and operation, energy information security software, and energy experience software. The energy domain software categories and example applications (TBV, 2022a, 2022b) are explained as follows:

- *Energy management and operation software* category covers software applications involved in the generation, transmission, and distribution of energy, grid management systems, systems integrating renewable energy sources into existing grids, smart meters. Additionally, it comprises energy management software used for energy trading, billing, certification, predictive maintenance in energy infrastructure, energy analytics, and reporting.
- *Energy information security software* category focuses on protecting energy infrastructure and data from cyberattacks and security threats. Examples are intrusion detection and prevention systems, secure communication protocols, access control systems.
- *Energy experience software* category includes software systems focused on improving consumer experiences. Examples of applications are home energy management systems, electric vehicle charging and management platforms, smart building/home programs, adjustment software for energy consumption to reduce bills, etc.

In many countries where blockchain applications have been implemented, there is currently no mature legal framework specifically for the energy domain (TBV, 2022a). IEC 61508 is an international standard for the functional safety of electronic safety-related systems. It provides a framework for ensuring the safety and reliability of these systems throughout their lifecycle. The utilization of this standard in applications within the energy management and operation software category could be considered.

The ISO/IEC 12207 Software Life Cycle Processes standard and the ISO/IEC 250xx Software product quality requirements and evaluation (SQuaRE) series are general standards; thus they could also be employed for energy domain software. The ISO/IEC 12207 provides guidance on the management, implementation, and monitoring of processes throughout the software lifecycle. Meanwhile, the ISO/IEC 250xx series provides guidance on software quality management.

2.3. Related Work on Blockchain Development Process Models

There is a growing interest among researchers in the blockchain dApp development field. A literature review has been conducted on the processes, practices, and process models to be applied during blockchain-based software development. The results are provided in this section. We present the studies that are relevant to our study, focusing on the subject of blockchain development processes and practices. Table 1 presents an overview of the studies that have made contributions to the understanding of blockchain dApp development procedures. Nevertheless, there is currently a lack of research that comprehensively outlines the various processes and practices involved in the development of blockchain dApps. Existing studies cover specific phases of the development process separately.

Table 1: Related Studies

Study Ref	**Contribution of the Study**	**Suggested Processes & Practices**
(Chakraborty et al., 2018b)	Presented the practices that may be applicable to blockchain development	*Suggested Practices:* Code review and unit test Voluntary assignment of tasks to developers. Community discussion for eliciting requirements
(Marchesi et al., 2020)	Presented a Scrum-based method for developing blockchain-based software.	*Suggested Practices:* Defining goals Identifying actors Defining user stories of the system and related UML use cases and class diagrams Defining actors Reviewing actors and user stories *Suggested Processes:* Designing, coding, and testing smart contracts Designing, coding, and testing user interface

		Testing the integrated system Deploying the complete system
(Antal et al., 2021)	Guidelines for the design and implementation of decentralized applications.	*Suggested Design Practices*: Identification of potential risks Understanding the existing system design and business model Determining potential tradeoffs Defining a Distributed Ledger Technology (DLT) compliant application design and business model translation *Suggested Implementation Practices*: Choosing a DLT implementation platform Listing tokens on public exchanges Offering token launch or initial coin Developing and deploying the dApp
(Nousias et al., 2022)	Introduced dApp development and deployment processes on the Ethereum blockchain to assist practitioners.	*Suggested Practices:* Developing dApp and deploying on test net Deploying smart contract code Approving smart contract creation transactions Verifying, and publishing smart contract code Deploying dApp on the main network

The studies listed in Table 1 are primarily concerned with recommending practices for blockchain dApp development, as opposed to providing a comprehensive reference model for the entire development process to guide the systematic development of blockchain dApp in safety critical domain.

In addition, while there are other studies address the blockchain-oriented development process by focusing on specific stages, they do not discuss or propose the processes or practices required to ensure the safety of applications. One of them is Porru *et al.* (2017) that suggest improvements in testing and debugging blockchain-oriented software, increasing collaboration for sustainable development, enhancing software quality, and blockchain developer and community synergy. Similarly, Vacca *et al.* (2021) propose applying traditional testing techniques to blockchain-oriented software, developing developer guidelines, identifying patterns and developing a taxonomy for detecting attacks, and constructing a framework for comparing various blockchain platforms. Another study, (Lahami et al., 2022) summarizes the most important studies in the context of black-box, white-box, and grey-box testing techniques used in blockchain-oriented software. The study’s findings suggested that the field of study is still in its early stages.

None of the current studies address the safety critical domain standards. BDRM was developed in accordance with health-focused standards (i.e. IEC 62304, IEC 82304, ISO 14971) automotive-specific standards (i.e. ASPICE, ISO 26262), and energy domain-related standards (i.e IEC 61508) to ensure regulatory compliance.

In addition to defining processes for blockchain dApp development, the BDRM also aims to contribute to addressing the challenges of safety critical domains. We conduct general research in the automotive and energy domains. Current specific challenges of these domains can be confronted using blockchain technologies.

Ensuring security, privacy, trust, and traceability in the automotive domain is important to mitigate fraud in the registration, maintenance, selling, and buying of vehicles (Alhajjaj et al., 2023). Data management is a crucial aspect of the automotive industry, as it involves sharing reference data across all stakeholders. A distributed record system is needed to control who can change and access data, making the process more reliable. This approach reduces errors, improves real-time access to critical data, and supports natural workflows around creation, modification, and deletion of data elements. A shared set of data can be efficient in managing reference data, reducing errors, improving real-time access to critical data, and supporting natural workflows. Blockchain technology can help maintain privacy and immutability by controlling who can see what across the business network. This creates a verifiable audit trail of everything owned/traded across the business network (Fraga-Lamas & Fernández-Caramés, 2019).

Operations management in automotive industry is another area where blockchain technology can improve efficiency. Supply chain risk management (SSCM) includes complete traceability of key assets, enabling faster and more confident information sharing across a trusted network. Smart contracts provide a lower cost of transactions with a trusted contract monitored without third-party intervention (Fraga-Lamas & Fernández-Caramés, 2019).

Incorporating blockchain into transaction processing systems can transform transactions from days to almost real-time, reduce overhead and cost intermediaries, and improve trust within the business network. Financial management in the automotive industry involves letters of credit, financing, leasing, and cross-border import and export systems. Smart contracts can ease verification steps, allowing for automatic negotiation of payment on car leases without a middleman (Fraga-Lamas & Fernández-Caramés, 2019).

An example of a challenge in energy domain is the complexity of energy supply chain management. The lack of transparency and traceability in energy transactions and resources often leads to inefficiencies, errors, and difficulties in tracking energy sources from generation to consumption. Blockchain's transparency, immutability, and traceability can revolutionize supply chain management in the energy sector. By recording every transaction and data point securely on a distributed ledger, blockchain technology can create an unalterable trail of energy production, distribution, and consumption. This transparency can enhance accountability, reduce disputes, and optimize energy resource allocation.

Moreover, the integration of renewable energy sources poses interoperability and integration challenges. The diverse nature of renewable energy systems and their interaction with conventional grids often leads to compatibility issues, making seamless integration challenging. Blockchain's ability to facilitate smart contracts and decentralized energy trading platforms can potentially address these integration challenges. Through smart contracts, energy producers and consumers can engage in secure and automated transactions, promoting a more flexible and efficient energy grid. Additionally, decentralized energy trading platforms powered by blockchain can enable peer-to-peer energy trading among households and businesses, fostering a more resilient and adaptive energy ecosystem.

Blockchain ensures transparency and immutability of data and activities, enhancing traceability and reliability in transactions and operations in safety critical domains. Blockchain's distributed nature makes hiding individual activities within the network almost impossible, ensuring transparency across all nodes. The elimination of third-party control is another significant advantage. Decentralization in blockchain eliminates third-party intervention, boosting reliability and stability in both energy and automotive transactions (Erturk et al., 2019).

Cost reduction is also a notable benefit. Blockchain technology can potentially reduce transaction costs and eliminate middlemen, thereby reducing expenses in financial processes like leasing in the automotive industry, and decreasing the likelihood of failed transactions in the energy domain (Erturk et al., 2019).

However, blockchain technology is not without shortcomings. The deficiencies are primarily present in the immaturity of current technology, the absence of industry standards and guidelines, and the deficiency of advanced technical skills in blockchain technology (Upadhyay, 2020).

Limited scalability and speed also remain major concerns. The current blockchain technology, for instance, exhibits limited transaction processing speed compared to traditional payment systems like Visa, which can handle significantly more transactions per second.

The necessity for off-chain support is another challenge. While blockchain improves digital record-keeping, ensuring accurate and reliable data input into the system requires a well-designed off-chain system, particularly in the automotive domain, for correct data input.

High establishment and maintenance costs are also identified in blockchain adoption. The decentralized nature and unique implementation may pose cost challenges compared to traditional systems.

Lastly, detailed testing is required. While proposed systems often perform well in simulations, real-world testing is crucial to unearth potential issues and ensure the reliability and scalability of blockchain technology.

Overall, blockchain technology ensures transparency and immutability in data and activities, enhancing traceability and reliability in transactions and operations in safety-critical domains. Its distributed nature eliminates third-party intervention, boosting reliability and stability in both energy and automotive domain transactions. Furthermore, blockchain technology could potentially decrease transaction costs and eliminate middlemen in financial processes, contributing to overall efficiency in the automotive and energy domains.

Compliance with domain related standards, risk mitigation, detailed testing tailored to safety critical domain specific challenges, and addressing maintenance issues are some of the important aspects in developing safe, secure, and reliable software.

The BDRM aims to contribute to an increase in awareness by containing information about how to avoid challenges faced in safety critical domains. Problem of the safety critical domain is explored in detail with the health domain. The detailed review studies were carried out to identify challenges and solution approaches in the health domain. We present the results in Chapter 3.

CHAPTER 3

MULTIVOCAL LITERATURE REVIEW ON BLOCKCHAIN TECHNOLOGY IN THE HEALTH DOMAIN

The purpose of this section is to detail the studies carried out to set the problem properly at the problem conceptualization stage, which is the first step of the design science methodology. Our objective in this study is to identify development processes of blockchain-based decentralized applications in safety-critical domains. Using health domain, which is one of the safety-critical domains to explore the problem was deliberate due to its strict regulatory environment.

Although software in the health domain is subject to strict regulations, there is currently no established standard or guideline regarding the use of blockchain technology in this domain. Concerning the necessary processes that must be performed for blockchain-based health software to be safe and secure, a gap is required to be filled. We initiated our research in this area by conducting a comprehensive review of the existing literature (Agbo et al., 2019; Hölbl et al., 2018; McGhin et al., 2019; Yaqoob et al., 2019) addressing the application of blockchain technology in the health domain. Our analysis revealed that the aforementioned studies provided only a brief review of the software development challenges confronted by practitioners when developing health applications based on blockchain technology. Furthermore, no thorough examination of the suggested solutions for these challenges was addressed. In addition, the experiences of the practitioners were not the primary focus of these prior investigations. We conducted a systematic literature review (SLR) based on the guidelines by Kitchenham and Charter (2009), focusing on practitioners' perspectives. The SLR addressed key research questions related to potential blockchain applications in the health domain, challenges and solution suggestions in blockchain health software development. Our analysis included 27 formally published studies from 2016 to 2020, emphasizing practitioner experiences (Baysal et al., 2021).

After the SLR study, practitioners and researchers published a number of blockchain-related applications and studies. This growth indicates the exponential expansion of the blockchain health applications domain. In the duration of a single year, the quantity of new papers that satisfied the quality criteria and were included into the paper pool has tripled. Thus, we decided to investigate the most recent developments and present a summary of the opinions considered by researchers and practitioners regarding the possible applications of blockchain technology in the health domain and the degree to which it can address challenges of the domain. We also aimed to explore new challenges that blockchain introduces to the domain and existing solution suggestions of these challenges. We conducted a multivocal literature review (MLR) of blockchain adoption in the health domain for these objectives. The MLR, comprises 23 Gray literature resources and 78 formal literature resources, which reflect the problems in the safety critical domain.

Section 3.1 includes multivocal literature review process, Section 3.2, 3.3, and 3.4 presents the summary of results of the MLR, Section 3.5 provides a discussion about comparison of SLR and MLR studies.

3.1.A Multivocal Literature Review Process of Blockchain Technology Applications in the Health Domain

The MLR approach offers a systematic methodology for examining gray literature as well as formal literature. Luxembourg states that "*gray literature is produced on all levels of government, academics, business and industry in print and electronic formats, but which is not controlled by commercial publishers, i.e., where publishing is not the primary activity of the producing body*" (Garousi et al., 2019). Thus, the MLR approach could incorporate both theoretical and practitioner (e.g., developers, designers, and quality engineers) perspectives into the study.

The MLR study enhances the existing body of knowledge by conducting a comprehensive review and evaluation of the most recent research on blockchain technology in the health domain. In the following subheadings, we present the details of review process (Baysal et al., 2023). In this study, we aim to answer the following research questions:

- RQ1: What are the potential health applications of blockchain technology and what are the main motivations for its adoption?
- RQ2: What challenges comprise the process of developing health software?
- RQ3: To what degree does blockchain technology aid in addressing of current software development challenges within the health domain?
- RQ4: Does the implementation of blockchain technology introduce new challenges to the development of software in the health domain?
- RQ5: What are existing solution suggestions that address the challenges associated with blockchain technology in the health domain?

3.1.1. Research Methodology

A Multivocal Literature Review (MLR) methodology which is a form of a Systematic Literature Review (SLR) which includes the grey (non-published) literature such as videos, blog posts, and white papers, in addition to the formal (published) literature such as journal and conference papers. MLRs are useful to researchers and practitioners, as they summarize both practice and the state-of-the art in a particular area. There is a limited number of studies which present guidelines on how to conduct MLR studies in software engineering. We follow the MLR guideline developed by Garousi, Felderer and Mantyla (2019). Figure 5 illustrates the overview of our MLR process. Since there is a large volume of practitioner sources indicating high practitioner interest in our topic, we aimed to increase its contribution by including gray literature in our study.

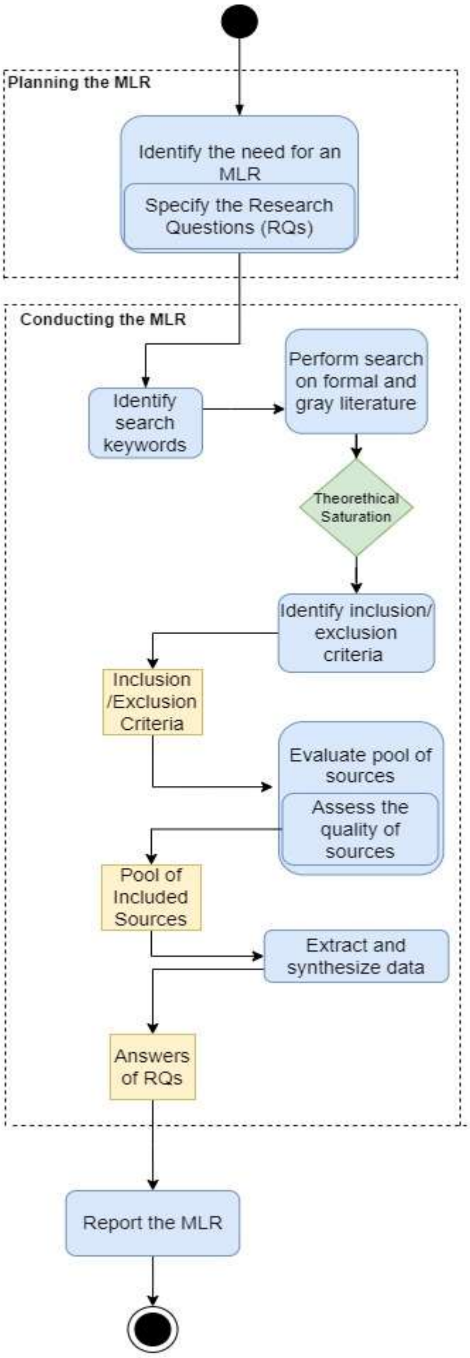

Planning the MLR
Identify the need for an MLR
Specify the Research Questions (RQs)
Conducting the MLR
Identify search keywords
Perform search on formal and gray literature
Theorethical Saturation
Identify inclusion/ exclusion criteria
Inclusion /Exclusion Criteria
Evaluate pool of sources
Assess the quality of sources
Pool of Included Sources
Extract and synthesize data
Answers of RQs
Report the MLR

Figure 5: Phases and Steps of the MLR Process

The MLR study (Baysal et al., 2023) included 78 formal literature sources (published journal papers, conference proceedings, and books) and 23 gray literature sources (magazines, white papers, news articles, presentations, Q/A sites such as StackOverflow, Wiki articles, and blogs).

3.1.2 White, Gray, and Black Literature definitions

Studies have varying definitions of the terms "white", "gray", and "black" literature. For example, books are classified as gray literature, as stated in reference (Adams et al., 2017). Conversely, they are regarded as components of the white literature, as stated in reference (Giustini, 2012). As a result of compiling these studies (Adams et al., 2017; Giustini, 2012), the spectrum classification presented in Table 2 was agreed upon. In order to categorize the sources according to their classification in the gray literature, we employed a pre-existing model derived from the guideline by Garousi *et al.* (2019). The instances belonging to the second-tier category, which includes preprints, e-prints, technical reports, lectures, and datasets, were revised.

Table 2: Spectrum of the 'white', 'gray' and 'black' literature

White (Formal) Literature	Published journal papers, Conference proceedings, Books

Gray Literature	**1st Tier** (High outlet control/High credibility):
	Magazines, Government reports, White papers
	2nd Tier (Moderate outlet control/Moderate credibility):
	Annual reports, News articles, Presentations, Audio-Video, Preprints, e-Prints, Technical reports, Lectures, Data sets, Q/A sites (such as StackOverflow), Wiki articles
	3rd Tier (Low outlet control/Low credibility):
	Blogs, emails, tweets

Black Literature	Ideas, Concepts, Thoughts

3.1.3 Evaluation Process and Selection of the Publications

Formal literature and gray literature was reviewed, as both contextual information and evidence from the industrial community (Garousi et al., 2019) are important.

Formal Literature: The search was conducted on the IEEE Xplore, ACM libraries, Google Scholar, PubMed databases, and the Research Rabbit tool, utilizing the search string provided below. The initial search was concluded on October 15, 2021.

(blockchain OR block chain) AND (healthcare OR health OR medical OR medicine OR ehealth OR e-health OR EHR OR EMR)

We used the following inclusion criteria in order to present a wider scope:

(i) the papers that discuss practitioner/researcher experiences;

(ii) the papers that offer blockchain solutions in the health domain;

(iii) the papers that discuss software development challenges faced in the health domain;

(iv) the papers that satisfy the quality criteria listed in Table 4; and

(v) the papers that are written in English and easily accessible.

In order to avoid duplicate findings, we omitted secondary research.

4076 results were returned from the original search. The titles and abstracts of the publications served as the basis for the first evaluation. The paper pool was reduced to 178 papers following the first evaluation. The papers were carefully examined in order to complete the second evaluation. Then, by performing snowballing on these publications and adding papers that were relevant to the topic, we increased the pool of papers. When no new concepts arose and the results approached theoretical saturation, the search was ended. Consequently, the evaluation procedure included an additional 78 formal pieces of literature.

Table 3 displays the number of publications available in online libraries as well as the outputs of every evaluation process.

Table 3: Results of Evaluation Process - FL

Online Library	**Initial Research**	**1st evaluation result**	**2nd evaluation result**
Google Scholar	2.400	47	124
IEEE Xplore	443	21	11
ACM Digital Library	754	11	4
Pubmed	279	6	6
ResearchRabbit	200	37	22
Snowballing		56	23
Total	4076	178	78

In evaluating the papers comprising the formal literature, we employed the subsequent criteria for assessment. Q1, Q2, and Q3 items in Table 4 are from the quality criteria developed by Höst and Runeson (2007), and we defined Q4.

Table 4: Quality Assessment Questions

ID	Quality Assessment Query	Quality Indicator (0–2)
Q1	Does the source have a clearly stated aim?	0- No 1- Partially 2- Yes
Q2	Does the item have a clearly stated date? (GL) Does the study contain conclusions, implications for practice and future research? (FL)	0- No 1- Partially 2- Yes
Q3	Does the study give a realistic and credible impression?	0- No 1- Partially 2- Yes
Q4	Are the challenges or solutions defined in detail?	0- No 1- Partially 2- Yes

Three researchers, including the thesis author, participated in the quality assessment process. We employed three-level indicators to answer the quality assessment questions for the 178 papers that made it through the initial evaluation:

(i) Level 0 in cases where the criterion was either completely ignored or handled extremely inadequately.

(ii) Level 1, in cases where the requirement was only partially met.

(iii) Level 2, in the event that the publication meets the requirement.

The review contained the research that received four stars or more on their rating.

To extract and review the data from the studies, the authors collaborated on a spreadsheet. We extract the information needed to respond to the research questions as well as bibliometric data, such as publication type, year, and citation number.

Gray Literature: Using the search string provided below, we conducted the search on the widely used web search engine Google, the specialized database Youtube, and the social question-and-answer website Stackoverflow.

(blockchain OR block chain) AND (healthcare OR health OR medical OR medicine OR ehealth OR e-health OR EHR OR EMR)

Between August 23, 2021, and October 1, 2021, 572 results were found overall from the searches. To provide a more comprehensive research scope, we employed the subsequent inclusion criteria:

(i) the sources that provide practitioner experiences;

(ii) the sources that present blockchain solutions in the health domain;

(iii) the sources that describe difficulties encountered during software development in the health domain;

(iv) the sources that meet the quality criteria specified in Table 4;

(v) the sources that are first- or second-tier outlet types;

(vi) the sources with more than 1000 views (valid only for videos);

(vii) written in English and easily accessible sources.

Based on the source titles, the first round of source elimination was carried out. In the second assessment, we examined the source’s full content using the previously stated inclusion criteria. 23 sources from the gray literature were therefore included in the review procedure. When the results achieved theoretical saturation, that is, no new concepts arose, we concluded the search procedure (Höst et al., 2007). Table 5 lists all of the sources that were found as well as the outcomes of each review.

Table 5: Results of Evaluation Process - GL

GL Database	Initial Research	1st evaluation result	2nd evaluation result
Google	160*	66	5
Youtube	382	65	14
Stackoverflow	30	6	1
Snowballing		5	3
Total	572	141	23

* The Google search engine returned about 92.2 million results for the query we entered. We thoroughly examined 160 sources, or the first 16 pages, because the 17th page begins to show irrelevant results.

Three authors, including the thesis author, participated in the quality assessment process. We responded to the quality assessment questions based on the three-level indicators provided above for 141 sources. We managed the data extraction procedure as a group using a spreadsheet, as was indicated in the formal literature section. Using the pyTranscriber program, we extracted the audio data from the videos and converted it to text on a local computer (Raryelcostasouza, 2020). We have included all the information required to address the research questions, together with the bibliometric data of the sources in the document. In the final MLR source pool, there are 78 formal literature (FL) and 23 gray literature (GL) sources.

We provide a bibliometric overview of the sources included in the MLR below.

Out of the 78 papers, 53 were published in journals and 25 were published in conference proceedings. Figure 6 shows the publication years of the papers included and the publication dates of gray literature sources. Although Satoshi Nakamoto introduced blockchain in 2008, no publications on its use in the health domain were found until 2016. The number of publications rose gradually in 2018, 2019, and 2020, as shown in the following graph. The numbers appear to be decreasing in 2021. As the year was not been over when the last search was conducted on October 1, 2021, we anticipate that interest in this field will continue to grow.

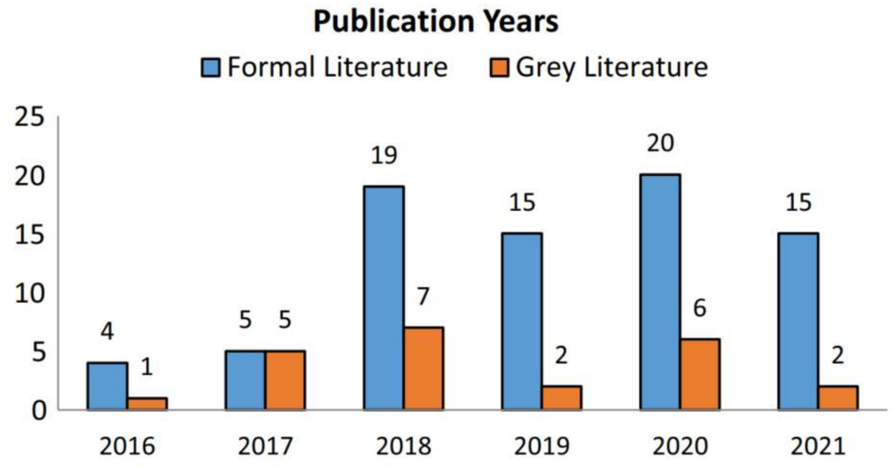


Figure 6: The Publication Years of the Sources Included

Figure 7 shows the publishing trend of blockchain technology in the health domain from 2016 to 2021. The number of studies on the topic shows an upward trend after 2017 and a downward trend after 2020. When we analyzed the publication types, we saw that early studies focused more on the concept, framework, and model development, and piloting implementation studies gained rapid momentum as of 2019.

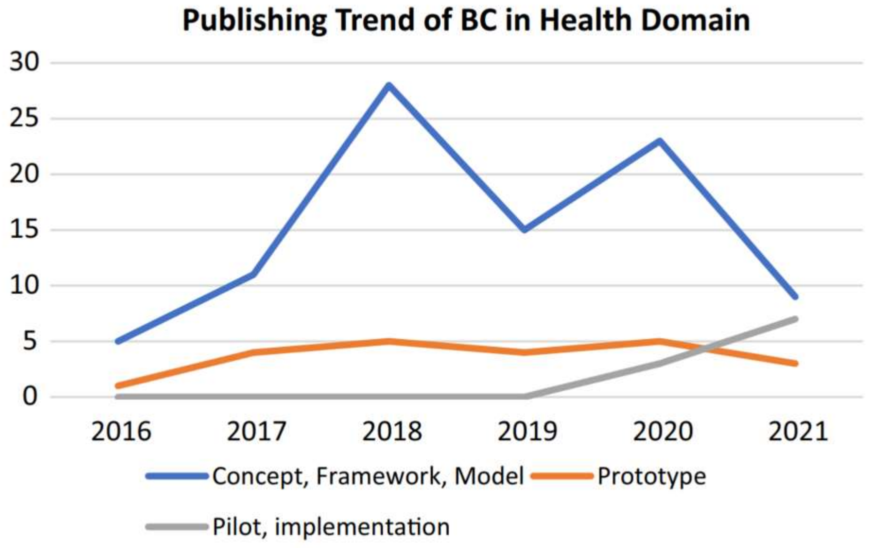


Figure 7: Evolution of Publications in Blockchain Technology in the Health Domain

Figure 8 shows the frequencies of the most published venues of formal literature studies. There are two venues with the highest number in terms of frequency: Journal of Medical Systems and IEEE Access. Journal of Medical Internet Research venue follows them with three studies. International Journal of Environmental Research and Public Health, International Conference on Open and Big Data, IEEE Globecom

Workshops (GC Wkshps), Blockchain in Healthcare Today, Sensors, and AMIA Annual Symposium Proceedings venues follow them with two FL studies.

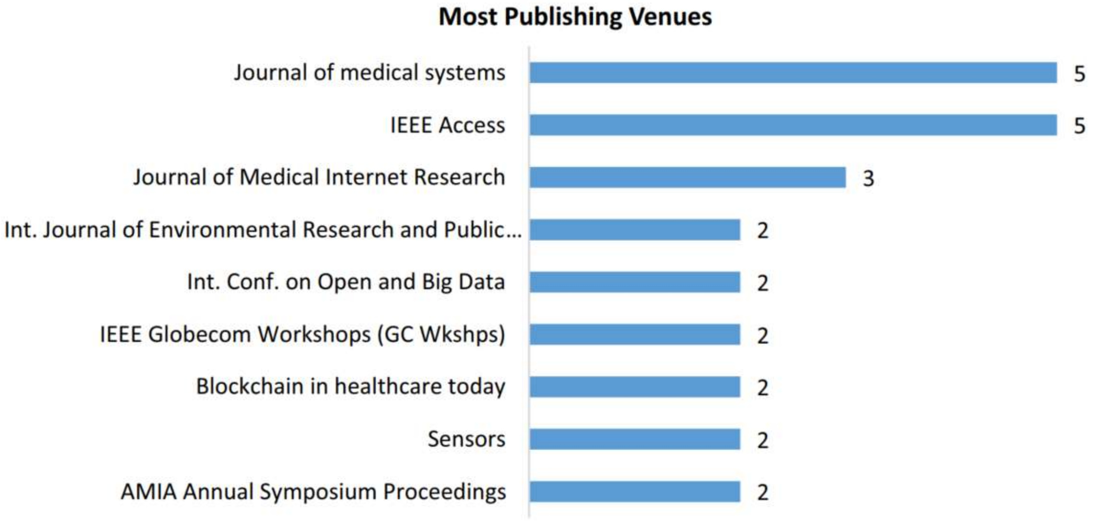
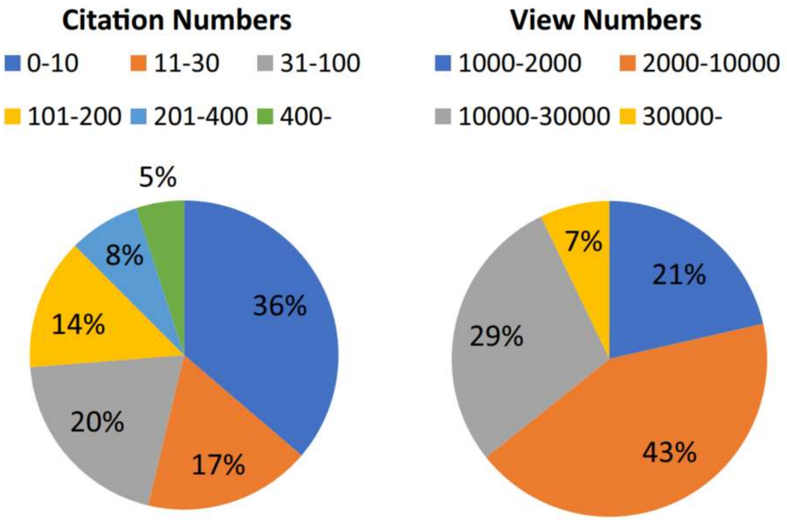


Figure 8: The Frequencies of most Published Formal Literature Venues

In Fig. 9 a, b, we present the distribution of formal (white) literature sources' citation numbers and YouTube video view numbers to show interest in the field.



(a) Citation Numbers of the FL Sources

(b) Video View Numbers of the GL Sources

Figure 9: Citation Numbers and Video View Numbers of the Sources

It was specified that 770 new papers were published in the domain within just one year. As mentioned, the number of new papers added to the MLR study has tripled in a single year. Thirty-six percentage of the publications have low citation numbers (less than ten citations per publication), mainly because these papers have been published in recent years (in 2020 and 2021). Considering that the latest publication date is 2016, the citation numbers of the remaining papers in the paper pool are high. Eighty percent of the YouTube videos included in the MLR source pool also have high viewing numbers above 2000.

We provide the answers to the research questions based on the analyzed formal and gray literature sources in Section 3.2, 3.3, and 3.4.

3.2. Blockchain Application Areas in the Health Domain (RQ1)

Blockchain applications have started to be widely utilized in the health domain. For instance, the Dentacoin application uses a blockchain network to associate dental clinics and patients for various services (Dentacoin Ecosystem, n.d.). MediBloc and SRCoin process and manage health data for healthcare professionals, patients, and researchers using blockchain technology (MediBloc, n.d.; SRcoin, n.d.). Medishare offers a blockchain-based marketplace for insurance management that is decentralized. Thus, anyone within the insurance circle can securely access insurance-related information (MediShare, n.d.). The AI Doctor platform is a decentralized virtual doctor application powered by artificial intelligence (Hohenheim, 2018). Users who provide their health data are rewarded with AIDOC tokens on this blockchain. Later on, AIDOC tokens could be used as health insurance credentials at preferential rates. Various organizations, such as pharmaceuticals, medical institutions, and AI companies, can use patient data stored on the platform for drug development and clinical research. MedicalChain (Medicalchain, 2020; Medicalchain, 2018) is a blockchain-based application that enables patients to control their medical data and is utilized in multiple UK hospitals. It provides a platform that enables users to grant conditional data access to parties including physicians, laboratories, hospitals, pharmacists, and health insurers. Patientory enables patients, clinicians, and health organizations to securely access and transfer private health information while gaining actionable insights to improve health outcomes (Patientory, n.d.). HealthVerity is a data marketplace that utilizes blockchain technology to share and analyze healthcare data in a secure manner. It enables pharmaceutical companies and researchers to access patient data from the real world while ensuring privacy and compliance (Healthverity, n.d.).

According to the 2022 OECD policy brief, national blockchain adoption is uncommon (OECD, 2022); however, there are government initiatives deploying blockchain technology in the health domain (Lindman et al., 2020). The Estonian government launched a project in 2016 to use blockchain technology to find new and innovative ways to secure the health records of its 1.3 million citizens. Estonia is the first nation to use blockchain on a national scale in the health sector (Einaste, n.d.). Malta is the second nation to implement blockchain technology on a national scale. Dwarna, a blockchain-based application, manages the "dynamic consent" of citizens regarding biospecimens for research studies (Mamo et al., 2020). The Australian government is working to develop a national blockchain framework for healthcare. The framework is intended to facilitate the adoption of blockchain technology by healthcare organizations and providers (Akmeemana, 2021).

Table 6 highlights the primary blockchain application areas in the health domain, the rationale for adopting this technology in these areas, and examples of blockchain oriented solutions presented in our resource pool. The use of blockchain technology for electronic health and medical record management is mentioned in most publications and GL sources (47 FL and 16 GL sources). The second most prevalent application area is Remote Patient Monitoring/Internet of Medical Things, with 12 formal literature sources (namely papers). Other application areas are medicine supply chain management (7 FL and 4 GL sources), clinical trials (7 FL), precision medicine (3 FL), blockchain in strengthening public health surveillance (1 FL and 1 GL sources), and health insurance (1 FL and 1 GL sources).

Table 6: Blockchain Technology in the Health Domain

Application Areas	**Motivation Behind Adopting Blockchain in the Relevant Area**	**Examples of Blockchain-Oriented Solutions**
Medicine Supply Chain Management	The difficulty of identifying unauthorized medicines, difficulty of specifying falsified medicines that misrepresent their content or source	Sylim *et al.* present a blockchain-based pharmacosurveillance system (2018). Tseng *et al.* (2018) and Takyar (2021) developed blockchain applications to manage the entire pharmaceutical supply chain life cycle. The originChain application created by Lu and Xu (Lu & Xu, 2017) aims to secure medicine data availability to service providers and automate regulatory compliance checks in the pharmaceutical supply chain. Uddin developed the Medledger application, which securely and efficiently executes drug supply chain transactions in a private permissioned distributed network of different pharmaceutical stakeholders (M. Uddin, 2021). Haq and Esuka (2018) and Musamih *et al.* (2021) developed blockchain applications for the pharmaceutical industry to track the drugs in manufacturing in a decentralized manner until they are delivered to patients. Omar *et al.* (2021) presented a blockchain solution using smart contracts to automate the Group Purchasing Organizations (GPOs) contract process. GPOs are large groups that healthcare providers

		usually reach out to improve procurement efficiency and collective pricing power in supply chain systems. Besides the researchers above, IBM has launched a blockchain network called Rapid Supplier Connect to enable government agencies and healthcare organizations to identify alternative suppliers and equipment vendors to overcome supply chain shortages experienced in the COVID-19 pandemic (Landi, 2020). Mauri (Mauri, 2017) and IBM (IBM, n.d.) also presented two blockchain solutions for fraud prevention in medicine supply chains.
Clinical Trials	The risk of clinical trial data manipulation, the need for providing data transparency in clinical trials for scientific reliability of the findings, the need for sharing and ensuring traceability of clinical trial data, the need for structuring clinical trial data which is usually kept in silo forms.	Nugent *et al.* (2016), Choudhury *et al.* (2019), and Wong *et al.* (2019) created smart contracts on a permissioned blockchain network to enable data transparency, eliminate data manipulation, and ensure scientific reliability in clinical trials. Shae *et al.* (2017) developed a four-layered system architecture for creating blockchain-based applications for clinical trials, precision medicine, and supporting medical decision-making. Zhuang *et al.* (2020) developed a blockchain framework with patient recruitment and patient engagement features. The framework also includes persistent monitoring modules to detect anomalies in patients' records in real-time and minimize the risk of record manipulation. Omar *et al.* (2020) developed a blockchain-based framework for clinical trials data management using Ethereum smart contracts, which employs the InterPlanetary Filesystem (IPFS) as the file storage system to automate processes and information exchange among clinical trials stakeholders. Jung *et al.* (2020) developed a blockchain-based healthcare solution named Decentralized Clinical Study Consent Management (D-CSCM). It contains features to create and manage consent documents, store them decentralized, and log all views and changes of the database entries on a chain.
Precision Medicine	The need for ensuring privacy and security of data in diagnosing, treating and preventing diseases by	Juneja and Marefat (2018) introduced a system that uses deep learning to classify arrhythmias and smart contracts to keep access under control. Lee and Yang (2018) created a nail analysis system that combines microscopy

	considering the variabilities in genes, environment and lifestyle of individuals.	sensors and blockchain to predict reliably the diagnosis of fingernail diseases. Gong and Zhao (2020) proposed a blockchain-based healthcare system that generates scientific knowledge such as the characteristics of gastric cancer or the cause of diabetes from personal health data by applying big data analysis techniques, knowledge discovery, and knowledge refining.
Remote Patient Monitoring / Internet of Medical Things	The need for a secure system in collecting and sharing data in a real time manner via IoT technology (e.g. body scanners, wearable devices, and heart monitors).	Griggs *et al.* (2018) used customized threshold values stored in smart contracts to analyze patient data gathered via IoT healthcare devices. Saravanan *et al.* (2018) created a smart contract-based IoT system for diabetes patients. Jita and Pieterse (2018) proposed an architectural design for a homecare system development that incorporates smart devices for monitoring patient vitals and blockchain for data storage. Liang *et al.* (2018), Pawar *et al.* (2021), and Taralunga *et al.* (2021) developed a blockchain-based user-centric health data sharing solution. Dey *et al.* (2018), Pham *et al.* (2019), Bhawiyuga *et al.* (2019), and Kumar *et al.* (2020) developed four different blockchain-based IoT solutions that employ biosensors to measure patients' medical conditions and save the data in a blockchain. Uddin *et al.* (2018) provided an architecture for developing a continuous patient monitoring system. Data streaming from body area sensors needs to be securely stored. An agent manages end-to-end data streams, and the blockchain stores data in a distributed manner. Hathaliya *et al.* (2019) proposed a decentralized AI and blockchain network for monitoring patients in real-time, and remotely. Blockchain and Machine Learning technologies were integrated for the early prediction of diseases in this network.
Electronic Health/Medical Record Management	The need for systems to be secure against attacks due to the sensitivity of patient data in electronic health records (EHR) and the need for	(Ivan, 2016; Khalil, 2019; Oliveira et al., 2019; Pandey & Litoriya, 2020b; Usman & Qamar, 2020; Vora et al., 2019; Wang & Song, 2018) provide EHR solutions for effective and secure storage of patients' medical data using blockchain. Due to their decentralized structure

	patient data to be up to date and available when needed.	and cryptographic functions, blockchains prevent hackers from breaching or corrupting data and keep data up-to-date. (Abdeen et al., 2019; Antwi et al., 2021; Azaria et al., 2016; Castaldo, Luigi and Cinque, 2018; Cernian et al., 2020; Chen et al., 2019; Chenthara, Ahmed, Wang, & Whittaker, 2020; Chenthara, Ahmed, Wang, Whittaker, et al., 2020; Cichosz et al., 2019; Cyran, 2018; Dubovitskaya et al., 2017; Ekblaw et al., 2016; Esposito et al., 2018; Fan et al., 2018; Gharat et al., 2021; Guti et al., n.d.; Hashim et al., 2021; Kaur et al., 2018; H. J. Kim et al., 2021; T. M. Kim et al., 2021; Kshetri, 2018; R. Kumar et al., 2020; H. A. Lee et al., 2020; Leeming et al., 2019; Muniat et al., 2021; Pandey & Litoriya, 2020a; Patel, 2019; Rathee & Sharma, 2020; Singh Chouhan et al., 2021; Sultana et al., 2020; Sun et al., 2021; Tith et al., 2020; Tripathi et al., 2020; Q. Xia et al., 2017; Q. I. Xia et al., 2017; Xiao et al., 2021b; Zhuang, Chen, et al., 2020; Zhuang, Sheets, Chen, et al., 2020; Zolfaghari et al., 2019) from formal litetature and (AMSYS, n.d.; Blockchain, n.d.; BlocksEDU, n.d.; Coinsider, n.d.; Crypto, n.d.; e-estonia, n.d.; Einaste, n.d.; Foundation, n.d.; Healthureum, n.d.; Interbit, n.d.; Lindman et al., 2020; Mccarthy, n.d.; Medicalchain, n.d., 2018; Stackoverflow, 2017; Telusko, n.d.; Webmedy, n.d.) from gray literature propose blockchain-based EHR sharing solutions. In these solutions, the accountability and transparency of transactions are maintained during the data-sharing process, and user-centric health data-sharing solutions are obtained using blockchain technology.
Blockchain in empowering public health surveillance	The need for disease monitoring systems, especially for infectious diseases, to aggregate data coming from a large network of agents. The need for the validation of data received, and making available to health officials to help manage their response to public health demands.	Coelho (2018) and Sharma (2019) proposed optimized, blockchain-based monitoring and reporting systems for disease surveillance that enable data transparency and enhance the accessibility of validated data. These blockchain-based solutions protect the society from future health risks.

Health Insurance	The need for the health insurance management systems to securely and efficiently exchange information between multiple entities used in decision making.	Panda *et al.* (2021) presented a decentralized authentication system based on the insurance claim blockchain (ICBChain) system that ensures patients' privacy and the exchange of sensitive healthcare information between multiple entities in a secure way. Synaptic Health Alliance (2021) conducted a pilot project and provided a blockchain solution to gather up-to-date demographic information about physicians and other providers.

We present the summary of this information in Fig. 10, including the application areas and the number of resources in those areas.

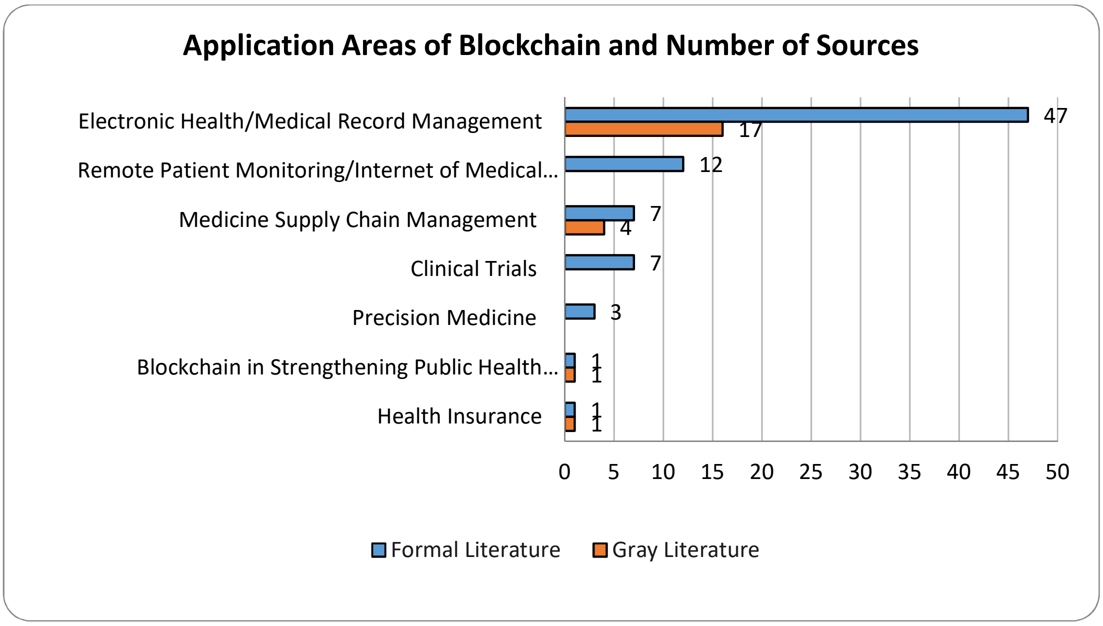


Figure 10: The Application Areas of Blockchain and the Number of Sources

3.3.Challenges of Developing Health Software and Contributions of Blockchain (RQ2 and RQ3)

We have grouped the challenges and associated solution suggestions of the MLR sources under four main headings: 1) Meeting regulatory requirements and public health surveillance, 2) Security and protection of privacy, 3) Ensuring interoperability, 4) Preventing waste of resources. The challenges and solutions is presented below exactly as it is from the MLR.

1) Meeting Regulatory Requirements and Public Health Surveillance

Challenge 1.1 Falsified drugs are one of the most serious threats to the pharmaceutical industry (IBM, n.d.; Mauri, 2017; Musamih et al., 2021; Takyar, 2021; Telusko, n.d.; Uddin, 2021; Webmedy, n.d.). The World Health Organization (WHO) highlights that one in ten medicines produced in developing countries is substandard or falsified and has serious adverse effects on human lives (WHO, 2017). To prevent the distribution of falsified medicines, regulatory agencies are required to monitor the product supply chain before and during distribution (Sylim et al., 2018; Takyar, 2021)

Solution 1.1. It is possible to detect data anomalies, unauthorized data insertions, and missing raw materials, identify authorized medication vendors/manufacturers, and store medical information by using blockchain technology and smart contract-based structures after data is inserted. Blockchain technology, which confirms and authenticates transactions, allows not only the system members but also drugs to be tracked throughout the medical supply chain (Haq & Muselemu, 2018; IBM, n.d.; Mauri, 2017; Sylim et al., 2018; Takyar, 2021; Telusko, n.d.; Webmedy, n.d.).

The primary structure used in blockchain for this problem is smart contracts. Smart contracts provide traceability by tracking information on the blockchain in the form of transparent, immutable, and timestamped blocks by recording medicines, their active ingredients, and distribution data (Telusko, n.d.; M. Uddin, 2021; Webmedy, n.d.). An account could be allocated to the FDA and notified by a smart contract when a transaction (i.e., the production, transportation, or receipt of medicine) occurs in a supply chain. The FDA account, as an oracle, could verify all transactions. When all other accounts attempt to upload a file, they automatically publish a session key encrypted with the FDA public key. Sylim *et al.* (2018) suggest that when unregistered products are entered into the medical supply chain, discrepancies in specific data points (e.g., dosage, ingredients) could be detected.

Additionally, a permissioned blockchain could be used to enable only trusted parties to join the network and to push data to the blockchain (Haq & Muselemu, 2018). These mechanisms aim to prevent data manipulation at the entry of data into the chain to some degree. However, blockchain cannot handle if data is manipulated at the source. For instance, if a permissioned network participant manipulates the content of drugs and records the manipulated data into the chain, the blockchain cannot notice the manipulation. However, this manipulation can be tracked down to the source once detected elsewhere.

Challenge 1.2. During the COVID-19 pandemic, healthcare industry leaders point out that reviewing suppliers can be time-consuming. Given the ongoing demand for materials, healthcare organizations need to make quick decisions to locate and verify new vendors (Landi, 2020).

Solution 1.2 These days, IBM leverages blockchain technology to help address medical supply chain shortages due to the COVID-19 pandemic. The company has launched a blockchain network called Rapid Supplier Connect to help government agencies and healthcare organizations identify alternative suppliers and equipment vendors more quickly. By creating their supply chains and adding non-traditional suppliers to their networks, they had a sufficient stock of equipment and materials. The blockchain network also helps identify existing suppliers and excess unused inventory, allowing hospitals to make them available to others and route suppliers where they are most needed (Landi, 2020).

Challenge 1.3. All clinical trials must make their methodology and findings available to regulatory agencies; however, more than half of the trials fail to do so (Nugent et al., 2016). Furthermore, a recent study (COMPARE, n.d.) found that clinical trials are highly vulnerable to data manipulation. Subject registration, and trial registration data, and clinical measures might be subject to manipulation (Nugent et al., 2016).

Solution 1.3. The clinical trial life cycle includes trial registration, recruitment of subjects, regulatory approval, data entry, compliance with the trial protocol, amendments to a clinical trial protocol, patient monitoring for giving or withdrawing their informed consent, and reporting of adverse events stages. Blockchain prevents backward data manipulation during the clinical trial life cycle if data is added to the blockchain at every stage when data is created instead of bulk data entry at the end of a trial (Nugent et al., 2016). Although blockchain does not guarantee correct data entry, a staged data entry process would reduce data manipulation risk. Smart contracts could be used to promote transparency in reporting clinical trial data by capturing data that might be intended to be manipulated (Choudhury et al., 2019; Jung & Pfister, 2020; Nugent et al., 2016; Omar et al., 2020; Tseng et al., 2018).

Additionally, smart contracts mandate a stage-by-stage data entry during the clinical trial process. This way, during a clinical trial, the intermediary stages can be traced, and the results can be disclosed to regulatory agencies without any missing data.

Challenge 1.4. Clinical researchers or clinicians may be fraudulent or careless and record misleading or incorrect data into case report forms (CRFs), including all data of patients participating in a clinical trial (Wong et al., 2019). A common healthcare fraud involves perpetrators who provide false or exaggerated diagnosis data for patients so that fraudulent insurance claims can be submitted for extra payment (Medicalchain, 2020). According to the FBI report: “The total cost of insurance fraud is estimated to be more than $40 billion per year.” in the USA (FBI, n.d.).

Solution 1.4. One method to solve this issue is to encourage clinical researchers and clinicians to provide raw data to the blockchain as early as possible. Incorrect data entry cannot be prevented by using blockchain; however, adding raw data early into the chain would eliminate data tampering to adapt to new situations. Later on, statistical analyses can be applied to verify the data (Wong et al., 2019) to detect discrepancies that signal data manipulation at the source.

Challenge 1.5. The Health Insurance Portability and Accountability Act (HIPAA) establishes standards for healthcare-related electronic transactions (HIPAA, n.d.). The HIPAA Privacy Rule requires protecting the privacy of health information. Therefore, patient information should be stored anonymously to prevent the identification of patients (Ivan, 2016; Juneja & Marefat, 2018).

Solution 1.5. Blockchain offers a partial solution with pseudo-anonymity where the user is anonymous, but their account identifiers are not (Griggs et al., 2018). The pseudo-anonym structure allows patients to hide their identities with alphanumeric addresses and yet to authenticate their identity when needed (Chen et al., 2019; Ivan, 2016; Jita & Pieterse, 2018; Liang et al., 2018; Muniat et al., 2021; Pandey & Litoriya, 2020a; Patel, 2019; Telusko, n.d.). Pseudo-anonymity is still considered personal data (Finck, 2018). Although privacy cannot be fully ensured with pseudo-anonymized data, it constitutes a partial solution for data privacy. Smart contracts enable regulation of the access control policy and achieve HIPAA compliance (Xiao et al., 2021a).

2) Ensuring Security and Privacy

Health data is a tempting target for criminals due to its potential economic value (Griggs et al., 2018; Haq & Muselemu, 2018; Lindman et al., 2020; Mauri, 2017; Medicalchain, 2020; Pandey & Litoriya, 2020a; Sultana et al., 2020). Therefore, health data storage and transmission processes must be performed in a reliable and secure way (Antwi et al., 2021; Azaria et al., 2016; Chen et al., 2019; Chenthara et al, 2020; Cyran, 2018; Dey et al., 2018; Ekblaw et al., 2016; Gharat et al., 2021; Ivan, 2016; Jita & Pieterse, 2018; Kumar et al., 2020; R. Kumar et al., 2020; H. A. Lee et al., 2020; Lindman et al., 2020; Muniat et al., 2021; Sun et al., 2021; Taralunga & Florea, 2021; Xia et al., 2017; Xia et al., 2017; Xiao et al., 2021a; Zhuang, et al., 2020). According to the Trustwave report: "a healthcare data record may be valued at up to $250 per record on the black market compared to $5.40 for the next highest value record (a payment card)" (Taylor, 2021). The number of patient records compromised in 2020 exceeded 40 million, according to the incidents reported to the USA government (IT News, 2021). Criminals may attack the healthcare system and threaten the confidentiality, integrity, and availability of patients' personal health information.

Challenge 2.1. Intruders may tamper with or delete patients' data, thereby benefiting insurance companies or hiding medical malpractices (e.g., delayed diagnosis and misdiagnosis) (Chenthara et al, 2020; Khalil, 2019). Intruders may also tamper with the cold-chain shipping data in medicine supply chains when the essential information is stored in centralized databases (Takyar, 2021).

Solution 2.1.a. In blockchain, all data and transactions are digitally signed which enables prevention of unauthorized access to network (Chen et al., 2019; Cichosz et al., 2019; Coelho, 2018; Dey et al., 2018; Ekblaw et al., 2016; Haq & Muselemu, 2018; Healthureum, n.d.; Ivan, 2016; Kumar et al., 2020; Lee et al., 2020; Saravanan et al., 2018; Vora et al., 2019; Wu & Wang, 2019). It employs asymmetric cryptography to authenticate users and safeguard data, thus enables confidentiality among the participants of a system (Chenthara et al., 2020; Gong & Zhao, 2020; Guti et al., n.d.; Hathaliya et al., 2019; Saravanan et al., 2018).

Solution 2.1.b. Each block in a chain keeps permanent logs of data transmissions (Azaria et al., 2016; Choudhury et al., 2019; Ivan, 2016; Jita & Pieterse, 2018; Juneja & Marefat, 2018; Xia et al., 2017), including data retrieval requests and updates from health service providers. As data are timestamped in a blockchain, data manipulations can be recognized (Coelho, 2018; Wang & Song, 2018). Blockchain technology ensures transaction security; however, it does not offer a specific advantage in preventing data theft. Using zero trust principles in a blockchain could enhance the overall security. While blockchain ensures transaction security, zero trust policies, including data encryption, would improve access management and user authentication (Sultana et al., 2020).

Solution 2.1.c Nodes have full access to ledgers; however, users are only allowed to perform activities based on their role and can only access the files they own or have permission to view (Muniat et al., 2021; Musamih et al., 2021; Sultana et al., 2020). Smart contracts can be used to assign network users to different roles with associated functions and privileges (Azaria et al., 2016; Coinsider, n.d.; Omar et al., 2021) and generate immutable logs of transactions (Guti et al., n.d.; Kim et al., 2021; Lindman et al., 2020; Pham et al., 2019; Taralunga & Florea, 2021; Zhuang et al., 2020)

Solution 2.1.d. A wrapper layer integration mechanism can be used between cloud-based EHR management systems and public blockchain networks to develop tamper-proof health record management systems (Khalil, 2019).

Solution 2.1.e. Because of the sensitivity of health data, permissioned blockchains (e.g., Hyperledger Fabric) could be used to enhance privacy (Chenthara, Ahmed, Wang, & Whittaker, 2020; Choudhury et al., 2019; Einaste, n.d.; IBM, n.d.; Kim et al., 2021; Medicalchain, 2020; Stackoverflow, 2017; Taralunga & Florea, 2021; Telusko, n.d.; Usman & Qamar, 2020). In a permissioned network, participants are included in a system in a controlled manner. Thus, confidentiality in a network is met (Kim et al., 2021).

Challenge 2.2. When health records are stored in centralized databases, it becomes a necessity to rely on single authorities that may not effectively protect the data against internal and external attacks (Chenthara et al., 2020; Interbit, n.d.; Medicalchain, 2020; Telusko, n.d.). For example, in disease surveillance, authorities and independent agents must record sensitive information in centralized information systems. But, centralized data control systems are subject to single point of failure problem and do not provide data transparency (Coelho, 2018).

Solution 2.2. Blockchain's decentralized nature enables elimination of single-point-of-failures. If a node fails or is compromised in a chain, the failure does not cause the entire system to stop. Therefore, it has a more robust structure and resilient to cyber-attacks (Chen et al., 2019; Choudhury et al., 2019; Coelho, 2018; Dey et al., 2018; Gharat et al., 2021; Gong & Zhao, 2020; Ivan, 2016; Jung & Pfister, 2020; Kim et al., 2021; Musamih et al., 2021; Pandey & Litoriya, 2020a; Patel, 2019; Sultana et al., 2020; Tripathi et al., 2020; Uddin et al., 2018; Webmedy, n.d.). Patients' health data are stored on the servers of various healthcare providers in blockchain-based applications; thus, a single failure does not affect all locations to stop working simultaneously (Webmedy, n.d.; Zhuang et al., 2020). It can be said that BC-based systems are robust against data loss or data corruption (Coelho, 2018; Telusko, n.d.) and eliminate the need to rely on central authorities (Interbit, n.d.; Sultana et al., 2020; Wang & Song, 2018; Webmedy, n.d.).

Challenge 2.3. Healthcare system users (e.g., patients) should have control over on their own data due to its sensitivity (Choudhury et al., 2019; Foundation, n.d.; Haq & Muselemu, 2018; Mccarthy, n.d.; Telusko, n.d.). Data ownership management is a major challenge for healthcare systems currently (Tripathi et al., 2020). Cernian et al. mention that there is no platform to monitor patient traceability throughout the entire healthcare chain (Cernian et al., 2020). The risk of intermediaries or intruders accessing the patients' reports without their consent remains valid. Such information may be exploited by insurance vendors and other third parties (Rathee & Sharma, 2020). Patients should be the ones to decide with whom their health data will be shared, neither third parties nor institutions.

Solution 2.3. Blockchain technology allows patients to take ownership of their health data and share data without violating patient rights. Patients could retain control over every transaction in a blockchain-based system by accessing their health data using an asymmetric encryption algorithm. Only the trusted parties authorized by patients may access the data within the given access period (e-estonia, n.d.; Einaste, n.d.; Guti et al., n.d.; Leeming et al., 2019; Medicalchain, 2020; Pham et al., 2019). When a patient wants to grant access to a doctor to view their health data, a token is generated based on the public key of the patient, which will allow the doctor to access the medical data (Cernian et al., 2020). This secure sharing between doctors and patients eliminates the intermediary parties (Sun et al., 2021). Patients could also track how many times their records have been accessed (Webmedy, n.d.; Zhuang et al., 2020) and whether a change was made on their records, and the owner of the change (Guti et al., n.d.). Thus, blockchain-based health applications enable the storage and sharing of health data in a patient-centric manner.

Challenge 2.4. Patients' health data may not always be recorded electronically in healthcare systems. This issue affects the quality of health care. There is a need to establish a patient-reporting mechanism to improve the quality of care (Coinsider, n.d.; Xiao et al., 2021b).

Solution 2.4. Blockchain gives patients the right to report their health records on ledgers (Xiao et al., 2021b). This functionality creates opportunities to use health records for medical research with permission (Zhuang et al., 2020).

Challenge 2.5. IoT devices used for remote patient monitoring are especially vulnerable to cyber-attacks and data theft (Bhawiyuga et al., 2019; Pham et al., 2019; Tripathi et al., 2020). Hackers can take complete control of wearable IoT devices and misuse them. For instance, Johnson & Johnson had previously warned patients about the vulnerability of one of the insulin pumps that the hackers could exploit to overdose the patients (Tripathi et al., 2020). In blockchain and IoT integrated systems, IoT devices may be subject cyber-attacks.

Solution 2.5. Blockchain cannot be a solution to prevent the attacks or temper resistant to these attacks. However, audit trails in blockchain allow tracking who made the changes and when the changes were made (Kshetri, 2018). Cryptographic hash functions create immutable audit trails and guarantee that the most recent version of the record is always used (e-estonia, n.d.). When a patient's report residing in the blockchain network needs to be updated, a new report is generated with the reference of the original report and uploaded to the blockchain. This reference enables the updated reports to be identified (Coelho, 2018).

3) Ensuring Interoperability

Challenge 3.1. Regulations on data transfer among healthcare providers are not well defined. In addition, interoperability of systems is another issue when effective and coordinated data sharing is concerned (Abdeen et al., 2019; Blockchain, n.d.; Cichosz et al., 2019; Ekblaw et al., 2016; Fan et al., 2018; Uddin, 2021; Webmedy, n.d.; Zolfaghari et al., 2019) Therefore, there is a need to develop a secure and efficient data-sharing mechanism for highly sensitive health information among the stakeholders of healthcare systems (Panda et al., 2021).

Solution 3.1.a. When a nation-wide blockchain application covering all the health stakeholders is deployed, no need to transfer data among health providers. As blockchain enables the patients to control their health data, patients could give access rights to health providers directly. As a result, it is possible to avoid undefined procedures and interoperability issues in sharing data among healthcare providers (Kshetri, 2018).

Solution 3.1.b. When a single ledger is developed to include all stakeholders in a healthcare system, there is no need to manually transfer added or modified patient data from one system to another (Interbit, n.d.; Medicalchain, 2020). Agreements among patients, government, providers, and insurance companies can be stored via smart contracts. Thus, interoperability would not be a concern. Additionally, data format requirements can be defined on blockchain to record all information correctly. In this way, the problem of preventing data sharing due to inadequate information can be reduced or eliminated (Blockchain, n.d.).

Challenge 3.2. Patient mobility requires cross-border exchange of patient data, which causes difficulties in complying with different countries' privacy and data protection standards (Castaldo et al, 2018).

Solution 3.2. Different data privacy, security, and sharing policies need to be addressed in designing blockchains and smart contracts considering the patient mobility fact (Castaldo et al., 2018; Esposito et al., 2018). In addition, we suggest developing a structure that allows each country participating in the network to implement specific policies for the protection and control of health-related data.

Challenge 3.3. Patel states that infrastructures used for cross-site medical imaging data transfers require relying on third-party intermediaries (Patel, 2019). However, ensuring the trust among the relevant stakeholders is highly difficult.

Solution 3.3. A blockchain application dedicated to corresponding stakeholders could be a solution for cross-domain image sharing. Blockchain framework eliminates the third-party access to protect health information (Patel, 2019).

4) Preventing Waste of Health Resources

Challenge 4.1. In clinical research, manual processing may be required to capture, manage and report data (Choudhury et al., 2019; Omar et al., 2020), as the patient data is collected as bio-samples, questionnaires, and lab results. The clinical research forms and questionnaires are usually paper-based. Such a manual intervention for data management and maintenance increases the cost of clinical studies. Backup and the data recovery time for such systems are also high (Chen et al., 2019; Choudhury et al., 2019; Omar et al., 2020). In addition, clinical trial data have to be stored confidentially and securely for audits and potential future studies (Tripathi et al., 2020).

Solution 4.1. Blockchain-based data management frameworks may reduce the administrative burden and the time and effort to ensure data integrity and confidentiality in clinical trials (Choudhury et al., 2019). In blockchain health systems, medical data is recorded continuously. Additionally, since previous clinical studies' trial data are encrypted and stored in the blockchain in a distributed manner, they remain unchanged and would be available for future studies (Tripathi et al., 2020).

Challenge 4.2 Patients often experience burden in remembering their medication history or carrying physical copies of their medication records (Zolfaghari et al., 2019). Patient reports, tests, and medical treatments generated by various doctors are managed independently (BlocksEDU, n.d.; Kumar et al., 2020; Mccarthy, n.d.; Medicalchain, 2018; Rathee & Sharma, 2020). Many health institutions, doctors, laboratories have their own database and manages their own information (Adarsh Kumar et al., 2020), without the intervention of patients. This situation affects the prevention and treatment of diseases for the population due to misinformation about a patient, potential information loss, or data leakage, which may imply an immediate risk to individuals and increase public health costs (Guti et al., n.d.). For instance, doctors might prescribe a medicine to patients that they are allergic to, as they cannot access the patients' medical history (AMSYS, n.d.). On the other hand, patients may be unaware of their medical reports, as they are not provided with complete documentation (Rathee & Sharma, 2020; Vora et al., 2019).

Solutions 4.2. Electronic health records that are securely published on blockchain-based health applications with patients' consents would address the problem given in Challenge 4.2. Using a decentralized ledger system, health professionals could update and query medication histories of patients after getting patients' approval (Zolfaghari et al., 2019). Thus, doctors and other health care providers can reach patients' health data (BlocksEDU, n.d.; e-estonia, n.d.), and perform transactions such as adding scans and lab results (Medicalchain, 2020).

Challenge 4.3. The patients' consent is essential for using their medical records for various purposes. However, most people give consent using paper forms, and they do not have control over it. Healthcare organizations are also having difficulties in dealing with the patients' consent. Patients give consent and may want to withdraw it later. There is a need to allow healthcare organizations to manage patients' consent (Tith et al., 2020).

Solution 4.3. Individuals'/Patients' consent could be stored in blockchain and shared by the participating parties in an immutable way (Tith et al., 2020). This is a way to provide individuals to have control over their data. Rather than one-time-only consent models, this dynamic structure allows individuals to override their consent terms in time as a new block (Mamo et al., 2020).

Challenge 4.4. A patient's medical history or patient's informed consent must be available at the required time (Jung & Pfister, 2020; Zhuang et al., 2020). In current systems, maintaining a medical history to meet this criterion is costly (Kumar et al., 2020), time-consuming and labor-intensive.

Solution 4.4. The health records stored on the blockchain network are permanent and are replicated across multiple nodes (Coelho, 2018). This ensures that all patient data is available at the required moment and required place (Sharma, 2019).

Challenge 4.5. Regulations require insurance companies to maintain directories that contain up-to-date demographic information about doctors and other healthcare providers. Maintaining its index for each insurer is time-consuming and expensive. Claim and payment processing may be delayed if the information in these directories is inaccurate. Roughly $2.1 billion is spent annually to track and maintain provider data across the healthcare system in the USA. A review completed by the Centers for Medicare and Medicaid Services (CMS) found that 52% of listed provider directory locations had at least one inaccuracy (Synaptic Health Alliance, 2021).

Solution 4.5. Administrative costs and data quality can be improved by sharing healthcare provider data and sharing changes of different parties on a blockchain. This feature enables identifying data inaccuracies within healthcare provider data (Synaptic Health Alliance, 2021)."

3.4.Blockchain Related Challenges in the Health Domain and Solution Suggestions (RQ4 ve RQ5)

Adopting the blockchain technology in the health domain introduces new challenges. We recommend considering the challenges and recommendations related to blockchain outlined in the MLR when developing a blockchain application in the health domain, which is one of the safety critical domains. The challenges and solutions is presented below exactly as it is from the MLR.

Challenge 1. Data cannot be altered or deleted after storing it in a blockchain [130]. However, according to health data protection laws, data is required to be deleted when a patient requests it (Esposito et al., 2018; Musamih et al., 2021; Tith et al., 2020) or to be changed (e.g., if a manufacturer enters incorrect information about a medicine) (Musamih et al., 2021).

Solution 1. Storing health data in an external storage and its hash in the blockchain could overcome this problem (Azaria et al., 2016; Esposito et al., 2018; Juneja & Marefat, 2018; Jung & Pfister, 2020; Kim et al., 2021; Lindman et al., 2020; Stackoverflow, 2017). By not having the data itself on the blockchain, we could delete the data when requested by its owner. Hash values whose data has been deleted would remain in the blockchain.

Challenge 2. Heterogeneous data (e.g., X-rays, images and ECG signal data) are heavily used in the health domain (Kaur et al., 2018) and size of health data can be pretty large (Dubovitskaya et al., 2017; Uddin, 2021). Along with the increase in data size, we need to deal with storage issues (Guti et al., n.d.; Lu & Xu, 2017) and mining costs (Gharat et al., 2021).

Solution 2. Storing the original large-scale data in an external storage and keeping its hash in a blockchain would resolve dealing with large-sized data (Ekblaw et al., 2016; Esposito et al., 2018; Foundation, n.d.; Juneja & Marefat, 2018; Kim et al., 2021; Leeming et al., 2019) without compromising the tamper-resistant nature of blockchain. The hashes of large data embedded in a digitally signed transaction is added to blockchain by consensus. When the hash for the data in the external storage matches the hash in the blockchain, the origin and timestamp of the data can be verified. Furthermore, when the data in the external storage changes, the hash of the data also changes, and thus, data manipulations could be detected.

However, there is a deletion risk of external data when the data is stored off-chain. The rollup technology in Ethereum could be an alternative to this solution. Rollups move the computation off-chain but retain some data per transaction on-chain. It also provides a solution to the storage problem as the amount of data published on the chain is the minimum amount required to validate the rollups transaction (Vitalik, 2021) locally.

Challenge 3. Blockchain poses performance (Dubovitskaya et al., 2017; Ekblaw et al., 2016; Muniat et al., 2021; Musamih et al., 2021; Pham et al., 2019; Vora et al., 2019) and scalability challenges (Pandey & Litoriya, 2020a; Uddin, 2021). As a performance issue, the read latency increases with the growth of ledgers (Gong & Zhao, 2020; Xiao et al., 2021a). Public blockchains suffer from scalability issues due to ledger replication in all network participants and consensus mechanisms (Hashim et al., 2021) and the need for significant computing power and storage space required on each node (Pandey & Litoriya, 2020a). As each node repeats the same process for mining the next block, it is impossible to perform parallel executions in a blockchain, which reduces system efficiency, and therefore may cause bandwidth and response time problems.

Solution 3.a. Architectural design decisions such as using consensus models impact blockchain system performance (Musamih et al., 2021). The choice of consensus algorithms affects both scalability and computing performance. For example, Practical Byzantine Fault Tolerance (PBFT) consensus algorithm is not that scalable but offers superior performance than Proof of Work (PoW) consensus algorithm. For fewer nodes, the PBFT consensus algorithm may provide performance and scalability within acceptable limits (Muniat et al., 2021; Pandey & Litoriya, 2020a). Instead of the Proof of Work (PoW), the Delegate Proof of Stake (DPOS) algorithm could be employed in medical blockchain since there would be no competition over discovering the blocks (Chen et al., 2019). Another design decision is to make the blockchain public, consortium or fully private (Xu et al., 2017). Consortium blockchain networks with trusted nodes may be preferred if high performance is expected from an application. They have much higher execution and processing efficiency (35000 transactions per second) and higher computing power than public blockchain solutions (Uddin, 2021).

Solution 3.b. Dividing the network into small groups, called shards, could be used to address scalability issues (Hashim et al., 2021). Hyperledger Fabric supports multiple channels, each maintaining a separate ledger and smart contract (Choudhury et al., 2019). Musamih et al. state that Ethereum has sharding feature as a scaling solution (Musamih et al., 2021). Currently, sharding feature is in development in Ethereum (Hashim et al., 2021). Transactions can be processed in parallel while running consensus within each shard with a subset of blockchain nodes. Although this technique could help solve scalability issues, the communication overhead between shards can degrade network performance. Minimization of cross-shard communication is possible by creating complete shards based on "the need to participate" nodes per patient (Hashim et al., 2021).

Solution 3.c. The efficiency of the blockchain is highly dependent on the coding of smart contracts. A smart contract which is coded properly (e.g. reduced external data storage access) could be executed in a quick and efficient manner (Musamih et al., 2021).

Solution 3.d. Standardizing the data to be stored and exchanged on a blockchain could be a solution to achieve better performance and efficiency. Ledgers could align and define data's type, size, and format. Restricting access to the blockchain network also helps standardize the data (Uddin, 2021).

Challenge 4. Data providers may not have a culture of handing over the control of the data (Kshetri, 2018). Furthermore, not everyone is capable of managing their personal health data. Studies conducted by the Connected Health Cities Programme and

Wellcome Trust Fund have shown that most citizens are not interested in managing their data (Leeming et al., 2019). On the other hand, a vast majority of the population is unfamiliar with blockchain technology. If patients lose their private keys, the associated resources become inaccessible to these patients and this issue requires recovery solutions outside of blockchain to re-establish ownership of the patient (Patel, 2019). To fully obtain the potential benefits of blockchain in the health domain, all parties involved in a health system need to be part of blockchain-based solutions (Kumar et al., 2020; Wong et al., 2019). Some stakeholders may be reluctant to join the network for fear of losing their competitive advantage (M. Uddin, 2021).

Solution 4. Solutions to these problems have not yet been proposed.

Challenge 5. Blockchain development imposes certain constraints on the development processes. **Challenge 5.1** A smart contract code cannot be changed once it is added to a network. When a change request is received, a new contract needs to be deployed (upgrading) (Koul, 2018a; Sillaber & Waltl, 2017).

Solution 5.1 While this issue reminds us running a waterfall-like plan-driven development process for smart contract development; it does not guarantee error-free features. However, this problem can be addressed by establishing new software design principles to assist the development of high-quality smart contracts.

Challenge 5.2 Smart contracts needs to be tested in a production environment as part of the development process. Testing in the production environment includes an execution fee (called gas price in Etherium). This fee varies depending on the operations performed by the smart contract. Calculating the cost of executing a smart contract on a blockchain network may be challenging, particularly for large-scale projects with complex coding (Miraz & Ali, 2020a).

Solution 5.2 There is no solution addressing this problem in our resource pool. Smart contract testing is free in test networks. Before deploying smart contracts to production environment, testing practices need to be applied in the test network to reduce the costs.

Challenge 5.3. Gas costs are proportional to the number of stored data and operations (i.e. memory and storage access) in smart contracts. Storage access needs increase gas cost dramatically (Musamih et al., 2021).

Solution 5.3. There are tools (e.g., Remix IDE) that could estimate execution and transaction costs and helps adjust these costs (Musamih et al., 2021). Additionally, this problem may be solved by establishing cost-efficient smart contract programming practices and a software development life cycle specific to blockchain-based applications to manage the development process better.

Challenge 6. There is a trade-off between transparency and confidentiality. Blockchain is intended to increase trust and enable transparency by sharing health data.

Access control imposes limits on data sharing and provides a level of confidentiality (Antwi et al., 2021).

Solution 6. When developing a blockchain platform, access control should only be on the identifiable data, yet a level of transparency should be allowed on the blockchain for other data types/categories (Antwi et al., 2021).

Challenge 7. Blockchain keeps log of all the activities taken place in the chain. Data is stored in every block of the blockchain; so, there is no chance of losing data, but there is a possibility of creating redundant data (Kaur et al., 2018).

Solution 7. The blockchain technology would require regular upgrades to solve the redundant data creation problem (Kaur et al., 2018).

Challenge 8. Blockchain networks work in their unique way, leading to interoperability issues where different blockchains cannot communicate (Musamih et al., 2021).

Solution 8. This problem can be avoided if a unified blockchain-based solution is used between healthcare centers. However, it will be very difficult to make them interoperable if healthcare centers decide to use different blockchain-based solutions in varying platforms (Musamih et al., 2021).

Challenge 9. Many countries have strong regulations for storing or transmitting medical data (Kim et al., 2021). Therefore, storing and transmitting personal data in a transparent medium is not allowed.

Solution 9. Rather than storing the actual data, its hash value could be stored or could be transmitted in a blockchain (Azaria et al., 2016; Esposito et al., 2018; Foundation, n.d.; Juneja & Marefat, 2018; Kim et al., 2021; Leeming et al., 2019). Whether hashed data being considered as personal data is an ongoing debate. If it is considered as personal data, hash sharing becomes another challenge. In this regard, it is important that regulatory guidance is issued on this subject (Finck, 2018). Kim et al. also mention that medical data is only kept by certified bodies in some countries including South Korea, and member states of the European Union. As a solution to this problem, they suggest keeping the hash of the data in a blockchain and leaving the storage of the data only to certified medical bodies, in separate databases (Kim et al., 2021). On the other hand, hash itself may not be secure enough, as the hash can be linked with patients, and is subject to brute force attack. In such circumstances, a keyed-hash maybe a better alternative, as it uses a secret key as an additional input to hashing.

Challenge 10. In blockchain solutions, it may be difficult to define the legal boundaries in blockchain technology components, which complicates the role of health authorities. For instance, when a new drug-related transaction is executed on a blockchain network, health authorities need to define legal obligations for the stakeholders involved in the transaction. Although there is still no definitive provision in the current laws and regulations for blockchain technology in healthcare (M. Uddin, 2021), blockchain networks need to comply with the existing regulatory requirements, such as the U.S. Drug Supply Chain Security Act (DSCA) and General Data Protection Regulation (GDPR) (Uddin, 2021).

Solution 10. Blockchain frameworks need to be developed to comply with existing regulatory frameworks. Hyperledger Fabric can be given as an example which was designed compliant with HIPAA and GDPR (Hyperledger, n.d.). Additionally, the policymakers need to consider addressing issues such as block ownership and access permissions on blockchain networks.

3.5.Discussion on SLR and MLR Comparison

The discussions for research questions are provided below.

RQ1: What are the potential health applications of blockchain technology and what are the main motivations for its adoption?

The outcomes of both the Systematic Literature Review (SLR) and the Multivocal Literature Review (MLR) underscore the common use of blockchain technology in Electronic Health and Medical Record Management as a major application domain. Specifically, a majority of publications in both reviews (13 papers in SLR, 47 FL and 16 GL sources in MLR) emphasize the significance of employing blockchain for ensuring secure systems handling sensitive patient data in electronic health records (EHR). Additionally, the necessity for maintaining up-to-date patient data emerges as a common subject across both reviews.

However, while the SLR primarily identifies the Internet of Medical Things as the second most explored application area after Electronic Health/Medical Record Management, the MLR emphasizes Remote Patient Monitoring as the immediate follow-up domain with twelve formal literature sources.

Furthermore, both reviews acknowledge Medicine Supply Chain Management and Clinical Trials as notable application areas, yet the distribution of emphasis differs slightly. SLR highlights medicine supply chain management as the third popular area (3 papers), while the MLR positions it as a more prevalent domain with 7 FL and 4 GL sources. Similarly, Clinical Trials receive attention in both reviews, with SLR citing 2 papers and MLR identifying 7 FL sources focusing on this domain.

Additionally, Precision Medicine emerges as a domain of interest in both reviews, though with varying emphasis. SLR reports 2 papers on Precision Medicine, whereas the MLR identifies 3 FL sources discussing this area.

Moreover, the MLR expands the scope by highlighting Blockchain in Strengthening Public Health Surveillance and Health Insurance, including applications not covered within the SLR. These areas encompass the need for disease monitoring, data validation, and information exchange in public health management and health insurance systems, respectively.

Overall, while both reviews converge on the significance of blockchain technology in Electronic Health and Medical Record Management, the MLR provides a broader spectrum by encompassing additional application domains and a more expansive array of formal literature sources, offering a comprehensive insight into the diverse facets of blockchain implementation in health domain.

RQ2: What challenges comprise the process of developing health software? RQ3: To what degree does blockchain technology aid in addressing of current software development challenges within the health domain?

Comparing the challenges and solutions addressed in both the Systematic Literature Review (SLR) and the Multivocal Literature Review (MLR) reveals notable similarities and differences across various domains in healthcare and blockchain integration.

Both reviews acknowledge the criticality of regulating medicine supply chains to prevent the distribution of falsified drugs (Challenge 1.1). The use of blockchain technology with smart contracts stands out as a common solution to monitor product supply chains and detect anomalies, unauthorized data insertions, and missing raw materials. Both reviews emphasize the potential of blockchain to authenticate transactions, enabling effective monitoring of medicine movement across the supply chain.

Regarding Clinical Trials (Challenge 1.3, Challenge 4.1), both reviews recognize the vulnerability to data manipulation and the imperative for increased transparency. Blockchain's role in preventing data manipulation and promoting transparency through smart contracts during the trial life cycle is a shared focus in both SLR and MLR.

Both of the studies addresses HIPAA's privacy requirement for healthcare electronic transactions (Challenge 1.5). Blockchain offers a partial solution with pseudo-anonymity, allowing users to hide their identities but not their account identifiers. Smart contracts regulate access control policies, achieving HIPAA compliance by enabling pseudo-anonymized data.

The need for secure and reliable storage and transmission of health data (Challenge 2.1, 2.2) resonates across both reviews. Blockchain's decentralized structure and encrypted data transactions are highlighted as solutions to enhance data security and prevent unauthorized access or data theft.

Patient data control and privacy (Challenge 2.3) emerge as key concerns in both reviews. Blockchain's role in enabling patients to control their health data access while ensuring confidentiality is a shared emphasis, highlighting the use of asymmetric encryption and smart contracts for access management.

The challenge of lack of well-defined regulations on data transfer among healthcare providers and interoperability issues is addressed in both studies (Challenge 3.1). A blockchain application can eliminate the need for data transfer and allow patients to control their health data. A single ledger can store agreements and ensure interoperability. The MLR extends this perspective by proposing solution involving nationwide blockchain applications and agreements stored via smart contracts to enhance interoperability.

Both studies highlighted the challenge of cross-border patient data exchange, requiring different data privacy, security, and sharing policies (Challenge 3.2). A structure allowing each country to implement specific policies for the protection and control of health-related data is suggested.

However, the reviews also exhibit differences in coverage. The challenges and solution suggestions presented below have been identified during the examination of new sources and are included in the MLR study.

Due to time restrictions and the urgent need for resources, the COVID-19 pandemic has forced healthcare organizations to find alternate suppliers and sources of equipment and speed up decision-making procedures (Challenge 1.2). The MLR discusses blockchain's function in creating supply chains and locating non-traditional suppliers in order to address this difficulty.

Clinical researchers may record incorrect data into case report forms, leading to fraud and insurance fraud (Challenge 1.4). The MLR contains information about addressing this issue, encourage early data submission to blockchain, eliminating data tampering. Statistical analyses can then verify the data, detecting discrepancies that signal data manipulation at the source.

Patients' health data may not always be electronically recorded in healthcare systems, affecting the quality of care (Challenge 2.4). Blockchain provides patients the right to report their health records on ledgers, allowing medical research with permission.

IoT devices are vulnerable to cyber-attacks and data theft (Challenge 2.5). Blockchain cannot prevent attacks, but audit trails in blockchain allow tracking of changes and the most recent version of records. Cryptographic hash functions ensure the most recent version is used.

Trust-based cross-site medical imaging data transfers require third-party intermediaries (Challenge 3.3). Blockchain application could eliminate third-party access, protecting health information.

Patients struggle with medication history management due to independent databases (Challenge 4.2). Electronic health records securely published on blockchain-based applications with patients' consent, allowing healthcare providers to update and query patient's health data.

Healthcare organizations struggle with patients' consent, requiring blockchain storage for immutable, individualized data sharing (Challenge 4.3). This dynamic structure allows individuals to override consent terms as needed.

Maintaining a patient's medical history or informed consent is costly, time-consuming, and labor-intensive (Challenge 4.4). Blockchain network's permanent health records ensure data availability at the required moment and place.

Maintaining accurate healthcare provider directories is time-consuming and expensive. Inaccurate data can delay claim and payment processing (Challenge 4.5). Blockchain can improve administrative costs and data quality by sharing provider data and changes between parties, enabling the identification of data inaccuracies.

The MLR presents a broader scope of challenges and solutions, incorporating a wider array of healthcare aspects and potential blockchain applications.

RQ4: Does the implementation of blockchain technology introduce new challenges to the development of software in the health domain? RQ5: What are existing solution suggestions that address the challenges associated with blockchain technology in the health domain?

Both MLR and SLR acknowledge the challenge regarding data alteration or deletion in blockchain after storage (Challenge 1). However, MLR highlights the conflict with health data protection laws, emphasizing the need for data deletion upon request or for data alteration in certain cases. Both propose a solution involving storing actual health data in external storage and embedding its hash in the blockchain to facilitate data deletion while preserving the hash in the blockchain.

Regarding the storage of large data sets, both reviews acknowledge the potential storage issues (Challenge 2) and propose a similar solution of storing large-scale data externally while embedding its hash in the blockchain, ensuring the tamper-resistant nature of the blockchain.

In terms of performance, the SLR and MLR acknowledge blockchain-related performance challenges (Challenge 3). The MLR contains more in-depth information about architectural decisions that impact system efficiency. It discusses consensus model choices, advocating for public/private blockchain options, and emphasizes the impact of these decisions on scalability and computing performance.

Regarding user capability and data control, both reviews identify challenges concerning users' ability to manage medical data and data providers' reluctance to release control (Challenge 4). However, neither review presents solutions to address these challenges, as solutions to these problems have not yet been proposed in the literature.

In discussing the constraints of blockchain development, both the MLR and SLR touch upon limitations in smart contract modification and testing (Challenge 5). They suggest the need for new software design principles and specific Software Development Life Cycles (SDLC) tailored to blockchain applications.

While the SLR study presented five challenges, the MLR study included 10 challenges, providing additional challenge scenarios and corresponding solution approaches.

MLR identifies a trade-off between transparency and confidentiality in blockchain, emphasizing that while blockchain aims to increase trust and transparency, access control limits data sharing, ensuring a certain level of confidentiality (Challenge 6). The proposed solution suggests implementing access control specifically on identifiable data while allowing a level of transparency for other data types/categories.

Blockchain's log maintenance for all activities results in data being stored in every block, leading to potential redundant data creation (Challenge 7). The proposed solution advocates for necessary upgrades in blockchain technology to address the issue of redundant data. Additionally, leveraging the InterPlanetary Filesystem (IPFS) in conjunction with blockchain is suggested to benefit from IPFS's inherent deduplication feature.

MLR highlights interoperability issues arising from distinct functionalities of different blockchains, inhibiting seamless communication between them (Challenge 8). The proposed solution suggests the adoption of a unified blockchain-based solution across healthcare centers. However, it acknowledges the difficulty in achieving interoperability if diverse blockchain solutions are used across different platforms within healthcare settings.

MLR points out strong regulations in many countries regarding the storage and transmission of medical data, posing challenges in transparent data storage or transmission (Challenge 9). The proposed solution revolves around storing or transmitting the hash value rather than the actual data in a blockchain. The ongoing debate about hashed data's classification as personal data is highlighted, necessitating regulatory guidance on the subject. The proposal also explores using a keyed-hash as a potentially more secure alternative.

MLR underlines the difficulty in defining legal boundaries for blockchain technology components, particularly in healthcare scenarios, necessitating clear definitions by health authorities (Challenge 10). The proposed solution advocates for the development of blockchain frameworks that comply with existing regulatory requirements like HIPAA and GDPR. It stresses the need for policymakers to address issues regarding block ownership and access permissions on blockchain networks.

We recommend considering the challenges and recommendations related to blockchain outlined in the MLR when developing a blockchain application in the health domain.

CHAPTER 4

DEVELOPMENT OF BLOCKCHAIN DAPP PROCESS REFERENCE MODEL

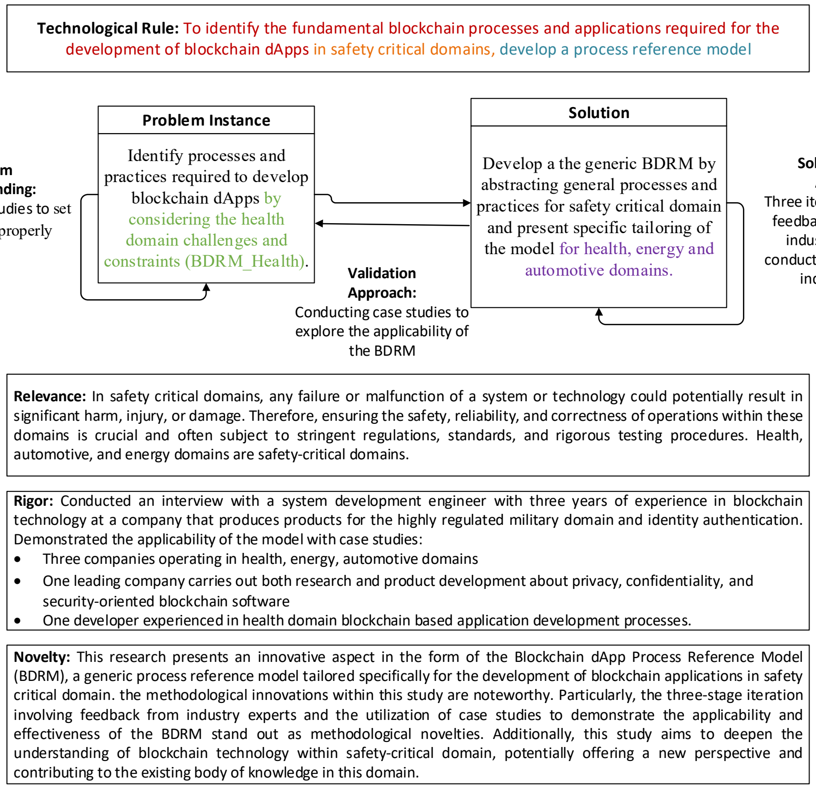
In this chapter, our primary aim is to provide the application and execution of Design Science Research (DSR) methodology, specifically in the context of developing a BDRM tailored for safety-critical domains such as health, energy, and automotive domains.

Section 4.1 provides information about research methodology. In subheadings, we present the stages of the DSR process followed, the iterative development and validation of the BDRM including expert consultations, interviews, and case studies to ensure the model's suitability and applicability across diverse domains.

4.1. Research Methodology

Design Science Research (DSR) is a methodology that aims to guide the creation of new knowledge through the design, development, and evaluation of novel artifacts, processes, or systems. DSR enables the creation and evaluation of new design artifacts, such as software systems, models, and methodologies, that can be used to solve problems or achieve goals in diverse domains (Hevner & Chatterjee, 2010; Hevner et al., 2004). Runeson *et al*'s (2020) Design Science Research Methodology (DSRM) provides a framework for implementing Design Science Research (DSR) in the software engineering domain.

We followed Runeson *et al.*'s (2020) DSR methodology, which comprises five stages: problem conceptualization, solution design, abstraction, instantiation, and empirical validation. To illustrate the main constructs of the design science research, we used the template provided by Runeson *et al.*'s (2020). The adapted version of the template within the scope of our study is presented in Figure 11.



Technological Rule: To identify the fundamental blockchain processes and applications required for the development of blockchain dApps in safety critical domains, develop a process reference model

Problem Understanding: SLR and MLR studies to set the problem properly

Problem Instance

Identify processes and practices required to develop blockchain dApps by considering the health domain challenges and constraints (BDRM_Health).

Solution

Develop a the generic BDRM by abstracting general processes and practices for safety critical domain and present specific tailoring of the model for health, energy and automotive domains.

Solution Design Approach: Three iterations, receiving feedback from domain/ industry specialists, conducting interview with industry expert

Validation Approach: Conducting case studies to explore the applicability of the BDRM

Relevance: In safety critical domains, any failure or malfunction of a system or technology could potentially result in significant harm, injury, or damage. Therefore, ensuring the safety, reliability, and correctness of operations within these domains is crucial and often subject to stringent regulations, standards, and rigorous testing procedures. Health, automotive, and energy domains are safety-critical domains.

Rigor: Conducted an interview with a system development engineer with three years of experience in blockchain technology at a company that produces products for the highly regulated military domain and identity authentication. Demonstrated the applicability of the model with case studies:

- Three companies operating in health, energy, automotive domains
- One leading company carries out both research and product development about privacy, confidentiality, and security-oriented blockchain software
- One developer experienced in health domain blockchain based application development processes.

Novelty: This research presents an innovative aspect in the form of the Blockchain dApp Process Reference Model (BDRM), a generic process reference model tailored specifically for the development of blockchain applications in safety critical domain. the methodological innovations within this study are noteworthy. Particularly, the three-stage iteration involving feedback from industry experts and the utilization of case studies to demonstrate the applicability and effectiveness of the BDRM stand out as methodological novelties. Additionally, this study aims to deepen the understanding of blockchain technology within safety-critical domain, potentially offering a new perspective and contributing to the existing body of knowledge in this domain.

Figure 11: Visual abstract of main constructs of the design science research

4.1.1. Problem Conceptualization

The initial stage of DSR methodology is identifying a technological rule. A technological rule captures generalized knowledge concerning the relationships between specific problem instances and their respective solutions, thereby facilitating knowledge transfer across different contexts. The validity scope of a solution is defined in terms of a desired effect of a proposed intervention within a specific context. Thus, a technological rule could be expressed in the form:

To achieve <Effect > in <Context > apply <Intervention>.

Our objective is to identify development processes of blockchain-based decentralized applications in safety-critical domains; therefore, we formulated the technological rule as follows:

Technological Rule: To identify the fundamental blockchain processes and applications required for the development of blockchain dApps in safety critical domains, develop a process reference model.

We approached the question of "how could blockchain technology potentially benefit in developing applications in safety critical domains?" from the health domain perspective. We chose the health domain for **exploring the problem** domain as it contains various applications and represents the challenges in the field from a broad perspective:

Problem Instance: Identify processes and practices required to develop blockchain dApps by considering the health domain challenges and constraints (BDRM_Health).

We conducted a systematic literature review (SLR) (Baysal et al., 2021), and multivocal literature review (MLR) (Baysal et al., 2023) for **problem understanding**, and investigated the challenges and benefits of using blockchain technology in the health domain, as well as the application areas of blockchain technology in the health domain and existing solutions that could be applied to health domain-related challenges. We focused on determining the extent to which blockchain could address the challenges inherent to the health domain and whether blockchain technology may introduce new obstacles to the development of health applications. The study results were presented in Chapter 3.

As revealed by the SLR and MLR studies, numerous studies have been published on blockchain dApps in the health domain, and they have received considerable attention from industry practitioners, academics, and governments. Despite this extensive research, few studies have examined the development processes of blockchain-based decentralized applications. In order to fill this gap, we decided to conduct this research in order to develop a generic process reference by abstracting general processes and practices for safety critical domain and present specific tailoring of the model for health, energy and automotive domains. In this regard, we have identified the research questions presented in the introduction of this thesis:

- RQ1. What are the fundamental processes and practices involved in the development of blockchain dApps?
- RQ2. What are the differences in the development process and practices between blockchain dApp development and traditional software development?
- RQ3. How could the development process and practices of blockchain dApp be specialized to ensure adherence to regulatory requirements in the safety critical domains (i.e. health, automotive, energy)?

4.1.2. Design and Development of the BDRM and Abstraction

We determined a **solution** aimed to address the identified problem. To understand problem we investigated health domain challenges and constraints. Due to their similar safety-critical characteristics, alongside the health domain, we included the energy and automotive domains in both the solution and validation processes.

Solution: Develop a the generic BDRM by abstracting general processes and practices for safety critical domain and present specific tailoring of the model for health, energy and automotive domains.

The **solution design approach** we followed involved analyzing various formal and grey literature sources related to blockchain dApp processes, analyzing related standards (ISO/IEC 12207, IEC 82304, IEC 62304, ISO 14971, Automotive SPICE, ISO 26262, and IEC 61508), collecting feedback from domain/industry specialists through two iterations to refine the model, and conducting interview with industry expert. Details of this process are presented below.

The BDRM was developed incrementally through three iterations. At the conclusion of each iteration, a new model version was released. These versions were subjected to rigorous validation processes to ensure the model's applicability, completeness, accuracy, consistency, readability, and usability. This process included receiving feedback from domain/industry specialists and conducting interview with domain/industry expert. The model was refined through these efforts to ensure its applicability, completeness, accuracy, consistency, readability, and usability, as described in the following sections.

In the first iteration, we developed the initial version of the model BDRM_v0 defining 46 practices associated with 13 processes. We have analyzed various formal and gray literature sources including blockchain dApp processes.

Afterwards, we solicited feedback on the model by distributing the initial version of the BDRM to two blockchain development specialists for review. In addition to holding Ph.D.s and having at least three years of experience in blockchain technology, these professionals have an extensive publication history.

We provided the BDRM_v0 to the experts and asked them to assess the model's completeness. We received nine responses from experts regarding the completeness of the BDRM processes and practices. Based on the feedback from the first iteration, the following modifications were made to the model, and BDRM_v1 has been created. BDRM_v1 included 13 processes 49 practices.

- Content improvement was made in the following three practices:
    - 1.2 Evaluate blockchain suitability – Added a note about supportive studies when assessing suitability,
    - 7.3 Decide on framework – Added a note about overcoming scalability problems and increasing performance, and
    - 11.2 Verify the blockchain dApp product - Added a note about some notable blockchain testing tools.
- The following three practices were found missing and included in the BDRM:
    - 5.6 Specify blockchain dApp privacy requirements,

- 7.8 Ensure the security of the system, and
- 7.8 Apply anonymity mechanisms if needed.

In the second iteration, we created the second version of the model BDRM_v2 by incorporating the specific health software development practices outlined in the (IEC 82304, 2016) and (IEC 62304, 2006) standards, as well as by taking into account the above-mentioned expert review results.

BDRM_v1 was subjected to a second round of expert review. The model was evaluated by a total of six experts, including one who provided feedback during the previous review round and five new experts with Ph.D.s (three experts affiliated with universities and two experts working for companies specializing in blockchain dApp development). Four of the experts have extensive experience in blockchain technology, the other two experts are experienced in safety critical domain software development processes. This strategy enabled us to incorporate a variety of perspectives into the BDRM.

To obtain expert feedback, we first shared the BDRM_v1 with them and requested them to evaluate it based on its applicability, completeness, correctness, consistency, readability, and usability. During the evaluation of the initial version of the model, we sought primarily expert opinions on its completeness. In order to conduct a more comprehensive verification, we asked experts to evaluate the model across all six of the aforementioned criteria. We collected 78 negative comments from experts and correlated them with the six aspects. For expert judgment, a five-point Likert scale was developed: Strongly Agree, Agree, Neutral, Disagree, and Strongly Disagree. In Table 7, we present the aspects, their descriptions, and the expert opinions regarding the aspects. Underneath each decision, the values enclosed in parenthesis represent the number of comments received from experts regarding each factor.

Table 7: Expert Decisions and Perspectives

Aspect	Description	E1 Decision	E2 Decision	E3 Decision	E4 Decision	E5 Decision	E6 Decision
Applicability	The model's practical applicability in the safety critical doman projects	Strongly Agree (0)	Strongly Agree (0)	Strongly Agree (0)	Strongly Agree (0)	Strongly Agree (0)	Strongly Agree (0)

Completeness	Comprehensive documentation of process IDs, process names, process purposes, practices, and special notes in the model	Neutral (8)	Neutral (12)	Neutral (9)	Neutral (13)	Agree (5)	Strongly Agree (1)
Correctness	The accuracy of the information contained in the model	Agree (3)	Agree (3)	Agree (2)	Neutral (8)	Strongly Agree (0)	Strongly Agree (0)
Consistency	Internal consistency refers to the absence of conflict between its guidelines	Strongly Agree (1)	Strongly Agree (1)	Strongly Agree (1)	Strongly Agree (1)	Strongly Agree (0)	Strongly Agree (0)
Understandability	Provide clear and comprehensive guidelines and requirements for processes and practices. Unambiguous and easily understandable by all stakeholders	Strongly Agree (1)	Agree (3)	Agree (2)	Agree (3)	Strongly Agree (0)	Strongly Agree (0)
Usability	Usable and practical for developers and project teams Provide guidance that can be readily applied in practice	Strongly Agree (1)	Strongly Agree (0)	Strongly Agree (0)	Strongly Agree (0)	Strongly Agree (0)	Strongly Agree (0)

The following revisions were made in the model according to the received feedbacks, and BDRM_v2 has been created. BDRM_v2 included 15 processes 68 practices. 19 of them are health domain related practices.

- Content correctness was made in the six practices:

    - 2.6 Decide on the need for using digital assets – the term “cryptotoken” is corrected as “digital token”.
    - 4.2 Elicit stakeholder requirements - the phrase “identifying project needs as quickly as possible” has been removed,
    - 5.2 Identify a consensus mechanism – the consensus algorithm name corrected as Performance Byzantine Fault Tolerance (PBFT) consensus algorithm,
    - 6.2 Define risks to the blockchain dApp product – the safety class classification is corrected as [Class B, C],
    - 7.1 Define and describe the blockchain dApp architecture - a security-related sentence is made consistent with other security expressions in the model,
    - 7.3 Decide on framework – the term “frequency is corrected as “target time span between blocks”.
- Content improvement was made in the seven practices:
    - 1.3 Evaluate the feasibility of the blockchain dApp project – Added a note about the project’s financial feasibility,
    - 4.2 Elicit stakeholder requirements – Added a note about the community discussion method,
    - 4.3 Review stakeholder requirements – Added a note about example techniques,
    - 7.2 Decide on blockchain network type – Added a note that permissioned networks may be preferred in high performance expectations,
    - 7.4 Decide on storage method - hybrid storage method is added,
    - 8.2 Design the backend - designing the cryptographic algorithms is added, and
    - 8.3 Design the frontend - establishing traceability is added.
- The following two processes and 19 practices were found missing and added to the BDRM:
    - 3. Blockchain dApp monitoring and control process,
    - 13. Blockchain dApp quality assurance,
    - 2.1 Create blockchain dApp scope, schedule, budget, and resources management plans,
    - 2.2 Create a communication plan,
    - 2.3 Create a change management plan,
    - 3.1 Monitor the blockchain dApp project against the plan,
    - 3.2 Control the blockchain dApp project,
    - 3.3 Manage corrective actions to closure,
    - 4.4 Agree on requirements,
    - 5.3 Include tokenomics in blockchain dApps including digital tokens,
    - 5.7 Specify blockchain dApp safety requirements,
    - 7.6 Decide on incentives if there is a need for digital assets,
    - 11.1 Prepare for verification,
    - 11.3 Manage verification results,
    - 12.3 Manage validation results,
    - 13.1 Specify blockchain dApp product quality requirements,
    - 13.2 Assure blockchain dApp product quality,
    - 14.3 Deploy the blockchain dApp product on the test network,
    - 14.4 Deploy the blockchain dApp product on the main network,
    - 15.1 Develop a maintenance plan, and
    - 15.4 Retire the blockchain dApp product practices.

In the third iteration, we reviewed various literature sources encompassing blockchain technology in automotive and energy domains. Similar to what was done in the health domain, standards to be considered during software development in these two safety-critical domains were identified as Automotive SPICE, ISO 26262, and IEC 61508. Information regarding development processes and practices derived from these standards was gathered and integrated into the BDRM.

We abstracted general processes and practices for safety critical domain and presented a generic BDRM, BDRM_v3. This abstraction process involves transforming the specific information focused on certain industrial domains (health, automotive, and energy) into a more general and inclusive framework. In BDRM_v2, detailed examination of health domain and identification of the requirements of the health domain were conducted. However, in BDRM_v3, the requirements of automotive and energy domains are also examined, and abstraction of these specific health, automotive and energy applications results in the emergence of more general processes and practices. This enables the identification of processes and practices that are not specific to a particular safety critical domain but are generally applicable. Abstraction leads to the number of practices remaining unchanged. The lack of change in the number of practices in BDRM_v3 is a result of an expansion process, as it is designed to cover a wider scope. Hence, it is quite natural that there is no change in the number of practices in this new version compared to the previous version. In the generic BDRM, we created sections dedicated to health, automotive, and energy domains and included specific information relevant to each domain.

BDRM_v3, which is the model's final version includes 68 practices associated with 15 processes, as well as special notes from the related domain software development standards. 19 practices contain information about safety critical domain requirements (health, automotive and energy). Table 8 contains the complete list of BDRM processes and practices.

4.1.3 Revised version of the BDRM

BDRM is based on the metamodel of the ISO/IEC 12207 standard for Software Life Cycle Processes. The BDRM consists of processes and practices. The model's processes provide an all-encompassing framework for managing the software life cycle, from acquisition to maintenance, thereby ensuring the delivery of high-quality software systems. The processes include practices that emphasize the development of dApp products to meet the requirements of customers and end users. The following structure is used to define each individual process.

Process ID	Each process has a unique ID.
Process Name	Each process has a name.
Purpose of the Process	The purpose outlines the goals of executing the process.

Outcomes	The outcomes refer to the observable results that are expected to be achieved via the successful implementation of the process.
Base Practices and Special Notes	Each practice is defined with a unique ID. The practices are sets of cohesive tasks of a process. The model integrates the requirements of the ISO/IEC 12207 alongside health-focused standards (i.e. IEC 62304, IEC 82304, ISO 14971) automotive-specific standards (i.e. ASPICE, ISO 26262), and energy domain-related standards (i.e IEC 61508). Information specific to blockchain development are highlighted in blue in the BDRM. The notes are recommendations to support the achievement of blockchain dApp outcomes and to ensure Safety Classification (given in brackets, [Class A, B, C] for health domain, [ASIL A, B, C, D] for automotive domain, [SIL 1, 2, 3, 4] for energy domain if applicable) The model includes specific information related to the health, energy, and automotive domains as additional documents. Information related to the health, automotive, and energy domains is highlighted in gray, orange, and green, respectively.
Inputs and Outputs	There are inputs necessary to execute each process and outputs generated as a result of conducting the process activities.

The following headings discuss the answers to the research questions.

RQ1. What are the fundamental processes and practices involved in the development of blockchain dApps?

The BDRM processes and practices are listed in Table 8. The first-level headings in the model in this table are processes, while the second-level headings are base practices. In total, the model covers 15 processes and 68 practices. In Table 8, practices that include information that is specific to blockchain development is highlighted in blue, and practices that are related to the safety-critical domain are indicated in purple. We presented the **BDRM in Appendix A** of this thesis.

Table 8: The BDRM processes and practices

Processes	**Base Practices**
1. Blockchain dApp project initiation process	1.1 Identify objectives and key performance indicators 1.2 Evaluate blockchain suitability 1.3 Evaluate the feasibility of the blockchain dApp project
2. Blockchain dApp planning	2.1 Create blockchain dApp project scope, schedule, budget, and resources management plans 2.2 Create a communication plan 2.3 Create a change management plan 2.4 Decide on the blockchain development life cycle model 2.5 Decide on the safety class of the product

	2.6 Decide on the need for using digital assets
3. Blockchain dApp monitoring and control	3.1 Monitor the blockchain dApp project against the plan 3.2 Control the blockchain dApp project 3.3 Manage corrective actions to closure
4. Blockchain dApp requirements elicitation	4.1 Identify stakeholders 4.2 Elicit stakeholder requirements 4.3 Review stakeholder requirements 4.4 Agree on requirements 4.5 Manage changes made in the stakeholder requirements
5. Blockchain dApp requirements analysis	5.1 Specify blockchain dApp system requirements 5.2 Identify the consensus mechanism 5.3 Include tokenomics in blockchain dApps including digital tokens 5.4 Specify blockchain dApp software requirements 5.5 Specify blockchain dApp security requirements 5.6 Specify blockchain dApp privacy requirements 5.7 Specify blockchain dApp safety requirements 5.8 Validate the requirements, and update when necessary 5.9 Develop approval criteria for testing
6. Blockchain dApp risk management	6.1 Identify the software that could contribute to a hazardous situation and potential causes 6.2 Define risks to the blockchain dApp product 6.3 Apply risk mitigation plan and risk contingency plan 6.4 Analyze the process and product risks 6.5 Resolve the process and product risks 6.6 Manage the process and product risks that may be raised by changes
7. Blockchain dApp architectural design	7.1 Define and describe the blockchain dApp architecture 7.2 Decide on blockchain network type 7.3 Decide on framework 7.4 Decide on storage method 7.5 Decide where to deploy the modules of the system 7.6 Decide on incentives if there is a need for digital assets 7.7 Ensure the security of the system 7.8 Apply anonymity mechanism if needed 7.9 Verify the architecture
8. Blockchain dApp detailed design	8.1 Prepare for detailed design 8.2 Design the backend 8.3 Design the frontend
9. Blockchain dApp implementation	9.1 Develop unit verification procedures 9.2 Build APIs 9.3 Develop the backend 9.4 Develop the frontend, user interface
10. Blockchain dApp integration	10.1 Integrate the backend and frontend units 10.2 Verify and test the integration
11. Blockchain dApp verification	11.1 Prepare for verification 11.2 Verify the blockchain dApp product 11.3 Manage verification results

12. Blockchain dApp validation	12.1 Prepare for validation 12.2 Validate the blockchain dApp product 12.3 Manage validation results
13. Blockchain dApp quality assurance	13.1 Specify blockchain dApp product quality requirements 13.2 Assure blockchain dApp product quality
14. Blockchain dApp transition	14.1 Develop a transition strategy 14.2 Confirm the blockchain dApp product is ready 14.3 Deploy the blockchain dApp product on the test network 14.4 Deploy the blockchain dApp product on the main network 14.5 Make the blockchain dApp product available to the users 14.6 Manage results of transition
15. Blockchain dApp maintenance	15.1 Develop a maintenance plan 15.2 Analyze, assess, and accept or reject change requests 15.3 Implement, test, and deploy modifications 15.4 Retire the blockchain dApp product

RQ2. What are the differences in the development process and practices between blockchain dApp development and traditional software development? RQ3. How could the development process and practices of blockchain dApp be specialized to ensure adherence to regulatory requirements in the safety critical domains (i.e. health, automotive, energy)?

32 of the 68 practices in the BDRM contain information specific to blockchain development. In addition, the model includes 19 practices containing specific information about safety critical domain software. The remaining practices are those applicable to conventional software development.

We presented all processes and practices **in Appendix A** of this thesis. Information related to the blockchain development, health, automotive, and energy domains is highlighted in blue, gray, orange, and green respectively in the BDRM.

In the model, we have also provided information regarding the safety classesifications for the practices. The safety classes for practices are indicated between brackets, such as [Class A, B] if applicable. Table 9 includes information about the classifications.

Table 9: Safety Classifications

IEC 62304 standard (2006) specifies three safety classes for software in health domain.	**ISO 26262 standard (2018) determine four safety integrity levels for software in the automotive domain.**	**ISO 61508 (2010) standard could be used to determine four safety integrity levels for energy domain software.**
• Safety Class A: the software system may contribute to a hazardous situation; or it may contribute to a hazardous	• ASIL A: The failure of the system would not cause severe injury or death.	• SIL 1: The failure of the system have nuisance or minor consequences.

situation without posing an unacceptable risk. • Safety Class B: the software system can contribute to a hazardous situation resulting in unacceptable risk, but possible harm is not a serious injury. • Safety Class C: the software system may contribute to a hazardous situation resulting in an unacceptable risk, with severe injury or death as a possible consequence.	• ASIL B: The failure of the system could cause severe injury or death, but only in rare cases. • ASIL C: The failure of the system could cause severe injury or death, but only in very rare cases. • ASIL D: The failure of the system could cause severe injury or death, and the failure is likely to occur.	• SIL 2: The failure of the system have serious or moderate consequences. • SIL 3: The failure of the system can be fatal or have severe consequences. • SIL 4: Failures have catastrophic consequences, extremely high level of reliability is required.

4.1.4 Solution Presentation and Validation

We conducted a comprehensive face-to-face interview with a system development engineer with three years of experience in blockchain technology at a company with 300 R&D personnel that produces products for the highly regulated military domain and identity authentication. The purpose of the semi-structured interview was to assess the suitability of the model for a company that develops blockchain-based solutions. Despite the fact that the company primarily operates in the military domain, we were able to assess the suitability of our model by considering the importance of requirements for safety-critical projects. Before the interview, we gave the engineer access to the model and explained the objectives of the interview. The duration of the interview was 1.5 hours.

We posed the following free-form inquiries:

Q1: Which BDRM processes and practices are implemented in your organization?

Q2: When developing safety-critical blockchain applications not covered by the model, do you adhere to any particular processes or practices?

Based on the responses, it was determined that the company develops blockchain applications using 12 BDRM processes (including planning, requirements analysis, design, implementation, and maintenance) and their associated practices. However, there were four processes (i.e. project initiation, quality assurance, risk management, and monitoring) and their practices that were not yet implemented in the projects. The BDRM assisted in the identification of these missing processes and practices in blockchain projects. The company intends to implement these processes and practices in future projects.

Additionally, it was noted that the organization did not implement any additional processes or practices beyond those outlined in the BDRM. This result indicates that the model is sufficiently inclusive.

The application status of the organization's processes in the BDRM was determined by examining each process separately with the organization. The model emphasizes the process dimension, and its purpose does not include capability evaluation. To address the capability dimension, it is possible to use the BDRM in conjunction with the ISO/IEC TS 33061:2021 to address the capability dimension (2021).

Our **validation approach** involved conducting case studies to explore the applicability of the BDRM, encompassing:

- Three companies operating in health, energy, automotive domains.
- One leading company engaged in research and product development focused on privacy, confidentiality, and security-oriented blockchain software.
- One developer experienced in developing blockchain-based applications within the health domain.

We obtained information about the processes that organizations follow in their blockchain dapp projects and shared the results of the case studies as improvement suggestions with the organizations.

Details about the case study process are included in the Chapter 5.

4.1.5 Communication

Our study is the first of its kind in this area, and it was undertaken with the understanding that it is essential to establish a systematic approach within the blockchain ecosystem, where uneven growth is taking place as blockchain technologies are relatively new and standardization is still in its early stages.

For effectively communicate the research process and findings to reach the intended audience we have prepared three papers:

- The SLR paper (Baysal et al., 2021) "Implications of Blockchain Technology in the Health Domain" has been published in Advances in Software Engineering, Education, and e-Learning in 2021 (DOI: 10.1007/978-3-030-70873-3_45).

- The MLR study (Baysal et al., 2023) "Blockchain technology applications in the health domain: a multivocal literature review" has been published in The Journal of supercomputing in 2023 (DOI: https://doi.org/10.1007/s11227-022-04772-1). We have also presented this research as a poster at the event: 3rd Open Research Day, which was held on June 17, 2022 at the METU Informatics Institute.

- We lastly prepared a paper including our studies BDRM creation process. This paper includes information specific to the health domain. We submitted the paper to Journal of Supercomputing in October 15, 2023. The paper is currently in the peer review process (preprint: https://doi.org/10.21203/rs.3.rs-3449851/v1).

CHAPTER 5

VALIDATION OF BLOCKCHAIN DAPP PROCESS REFERENCE MODEL

This chapter presents the applicability of BDRM with case studies for achieving validity. Section 5.1 describes the design of case studies; Section 5.2 includes validity threads; Section 5.3 includes the conduct of case studies; and section 5.4 includes the findings of the case studies.

5.1. Case Study Design

A plan for a case study should at least contain the following elements (Runeson & Höst, 2009). We planned the case studies according to these elements:

1. Objective—what to achieve?
2. The case—what is studied?
3. Theory—frame of reference
4. Research questions—what to know?
5. Methods—how to collect data?
6. Selection strategy—where to seek data?

The objective of the case study is to explore the applicability of the BDRM in organizations, which develop blockchain dApp in the safety critical domain. This involves understanding how well the model aligns with the real-world practices, and gaining insights into its effectiveness and practicality within these companies. We aimed to obtain information about the processes that organizations follow in their blockchain dapp projects and share the results of the case study as improvement suggestions with the organizations. The model emphasizes the process dimension, and the objective of the model does not entail capability assessment. It is possible to use the BDRM in conjunction with the ISO/IEC TS 33061:2021 standard to address the capability dimension.

The case involves organizations developing privacy, security, confidentiality, and safety focused critical blockchain dApp solutions.

The theory is that the proposed BDRM can benefit developers, researchers, and decision-makers by providing a useful resource for the development of blockchain applications in safety critical domains. There is currently a lack of comprehensive studies presenting the essential blockchain processes, practices, and guides for development teams for ensuring related regulations. BDRM aims to address this gap. The BDRM not only guides the development activities but also ensures adherence to related standards, which may usually require significant effort and time to adapt. The BDRM also addresses specific constraints that blockchain introduces to development processes in the safety critical domain.

The research questions we created for the case studies are:

CSRQ1: Which BDRM processes and practices are applied in the organization?

CSRQ2: Does the organization follow any specific processes or base practices when developing blockchain dApps that are not covered by the questions?

Methods To collect data and answer the research questions, we preferred qualitative methods. We conducted in-depth interviews with key stakeholders within the organizations, such as project managers, business analysts, architects, developers, and other relevant team members. For each practice, we determined the application status using a 4-point scale, and we determined "Not Applicable (N/A)" for items that are not applicable.

- Not Achieved (NA): Expected information is absent or the provided information is unacceptable.
- Partially Achieved (PA): Expected information exists but not detailed, and not systematic.
- Largely Achieved (LA): There is a systematic approach, but not complete.
- Fully Achieved (FA): There is a complete and systematic approach.

To determine the application status of the processes, we characterized the processes with 4 levels, and we determined "Not Applicable" for items are not applicable:

- Not Implemented (NI): At least one practice is Not Achieved.
- Partially Implemented (PI): No practice is Not Achieved; at least one practice is Partially Achieved.
- Largely Implemented (LI): No practice is Not Achieved or Partially Achieved; at least one practice is Largely Achieved.
- Fully Implemented (FI): No practice is Not Achieved, Partially Achieved or Largely Achieved. All practices are Fully Achieved.

We prepared 146 interview **questions in Appendix B** to ask key stakeholders within the organizations. The results were documented and disseminated to the members of organizations participating in the case studies. The aim of the case studies was not an assessment of the level of application. The practices and processes in the model were categorized according to whether practices and processes were implemented in the organization or not.

Selection Strategy involves selecting a representative sample of companies to provide a comprehensive understanding of the BDRM's applicability across the industry. We prepared the following questions for selection:

- Can you provide an overview of your organization's experience in managing projects, especially in the domain of blockchain health dApps? How long have you been developing?
- How many blockchain health dApp projects has your organization successfully completed so far?

- Can you share some examples of the most notable blockchain health dApp projects your organization has worked on? Are the applications you developed in use?
- Do you have in-house expertise for blockchain development, or do you collaborate with external partners?
- How many dedicated project staff members do you have in your organization, and what are their roles in project management?
- Could you describe the project life cycle(s) that your organization uses for managing blockchain health dApp projects? Do you follow a standardized life cycle, or is it tailored based on project requirements?
- Do you have any certifications or recognitions related to project management that showcase your organization's expertise?

Ethical Considerations: We obtained ethics committee approval for collecting data with case studies and presented it in the **Appendix C**. Organizations must explicitly agree to participate in the case study; thus, we gave informed consent in our study. The collected data is considered as confidential by organizations. In order to solve this problem, the collected data is anonymized, and information identifying the company is not included in the thesis study.

5.2. Validity Threads

During the design phase of this research, we considered the implementation of mitigation strategies to address potential threats to validity. The case study approach, being a qualitative research methodology, is subject to specific challenges related to its validity. In order to ensure the credibility of our research outcomes, we have identified and implemented strategies to mitigate potential risks to internal, external, and construct validity.

5.2.1 Construct Validity

Construct validity evaluates the accuracy with which research instruments measure the variables or constructs they are intended to evaluate (Runeson & Höst, 2009). The processes and practices used in creating blockchain-based dApps and their conformance with safety critical domain regulations are the main concepts in the context of this study. The BDRM's construct validity is considered to be demonstrated by the following aspects:

The BDRM's constructs must be clearly operationalized before construct validity can be established. The development team guidelines, formal and gray literature reviews, and blockchain processes and practices formed the basis for the careful definition of the model's constructs. Moreover, the integration of feedback from specialists in the field guaranteed that these concepts were precisely and fully reflected in the model. The model was evaluated by a total of six experts with Ph.D.s (four experts affiliated with universities and two experts working for companies specializing in blockchain dApp development). Four of the experts have extensive experience in blockchain technology, the other two experts are experienced in safety critical domain software development processes. This strategy enabled us to incorporate a variety of perspectives into the BDRM model. Through an iterative process including experts in blockchain technology and safety critical domains, the BDRM's content validity was verified. Their knowledge, feedback, and ideas help to ensure construct validity.

The construct validity assessment also benefited from the BDRM's practical use in case studies. Construct validity of the BDRM is concretely demonstrated by the way it applies in real-world circumstances.

5.2.2 Internal Validity

Internal validity refers to the extent to which the observed effects in a study can be attributed to the manipulated variables or interventions, rather than being influenced by external factors (Runeson & Höst, 2009). Key stakeholders participated in the case study meetings. During these meetings, a consensus was reached among all key stakeholders regarding the responses given. The potential for participants to provide responses that align with the expectations of managers of the organizations was taken into consideration. In order to address this potential bias, data from interviews and observations is sent as a report to the participants to enable correction of information. The participants were informed that they could submit their proposed changes, with assurances that their suggestions would be treated with confidentiality. It is important to take into account the views of each stakeholder who participated in the meetings. This approach is believed to mitigate participant bias.

Giving feedback to the participants of a study is also critical for the long term trust and for the validity of the research. Participants must not necessarily agree to the results of case studies, we aimed to increase the validity of the study by feeding back the results.

5.2.3 External Validity

External validity refers to the generalizability of research findings beyond the specific context or sample in which the study was conducted (Runeson & Höst, 2009). The careful selection of cases is a crucial factor that enhances the research's external validity. The case studies were carried out in order to validate the BDRM. Questions were determined to select a representative sample of organizations. We have conducted case studies in various domains, including companies operating in the health domain, energy domain, automotive domain, as well as a general domain focused on privacy and security. We performed interviews with key stakeholders within the organizations, such as project managers, business analyst, architects, developers, quality assurance personnel, and other relevant team members. We encompassed a wide diversity of roles. This allowed us to obtain more comprehensive insights.

Encountering challenges in finding companies that have successfully developed safety critical domain related blockchain solutions, and persuading them to participate in interviews presents significant obstacles. The challenge lies in the scarcity of such companies with proven success in the blokchain safety critical domain.

5.2.4 Reliability

This aspect addresses the extent to which the data and analysis depend on the specific researchers. Hypothetically, if another researcher conducts the same study in the future, the outcome is expected to be same (Runeson & Höst, 2009).

To enhance the reliability of this research, standardized methodologies were employed in data collection, analysis, and the development of the BDRM. These methodologies were well-documented and systematically followed throughout the research process.

Comprehensive documentation of research procedures -including data collection, data analysis, and model development- ensures transparency and facilitates potential replication by other researchers.

5.3. Multiple Case Study Conduct

We applied the model in five cases. The cases and outcomes of each case study are detailed below. We maintained the anonymity of all organizations and initiatives due to concerns regarding confidentiality. For each practice and proecss, we determined the application status using a 4-point scale. Details of the scales are included in 5.1 Case Study Design.

Table 10 includes various locations of cases, areas of expertise, experiences, personnel details, methodologies, certifications, interview durations, and related safety-critical domain software categories. Each case exhibits a different level of expertise in specific domains and varies in their focus areas.

5.3.1 Challenges we faced during the conduct of case studies

We have observed that approaching team members with open-ended questions is a better approach for eliciting their implicit knowledge. However, this strategy is not without its drawbacks. Transcribing the discussions from the interviews into text and compiling them into a report to share with the organizations was lengthy process. In addition acquiring precise details about development processes was not an straightforward, it was necessary to guide the interviewers with specific examples during the interview.

Table 10: Overview of Cases

Case no	Organization	Location	Case Domain	Blockchain Type	Expertise	Company Size	Certification	Interview Duration (hrs)	Interviewees
1	OE	Ankara	Blockchain based renewable energy solution	Public	New blockchain adapter organization, completed one blockchain product, developing the second version	4 blockchain and energy software focused personnel	No certifications, PMI training courses taken	2	Project manager and blockchain developer
2	AZ	İstanbul	Blockchain based international transportation solution for automotive domain	Hybrid	Completed eight blockchain products	47 dedicated blockchain-focused personnel	PMI certificate, ISO 9001, ISO 27001	3	Project manager, blockchain developer and quality expert
3	ER	İstanbul	Blockchain based health data management	Private	Wide range of health domain software products, one blockchain-based health dApp is developing	19 blockchain and health software focused personnel	PMI certificate, ISO 9001, ISO 27001	2.5	Project manager, blockchain developer and information security expert
4	SC	Ankara	Blockchain based health data management	Private	Completed one blockchain health application	N/A	N/A	1	Blockchain developer
5	BG	Ankara	Blockchain-based digital identity management system	Private	Completed seven privacy and security oriented blockchain products	25 blockchain software-focused personnel	PMI certificate, CMMI5	3	Project manageri analyst and test engineer

5.3.2 Findings of the case studies

5.3.2.1 First Case Study: Organization OEWe wanted to observe the applicability of the model in a new blockchain adapter organization that has developed a blockchain solution in the renewable energy domain, which is one of the safety-critical areas.

Overview of Organization OE

Location: Ankara, Turkey

Expertise: A new blockchain adapter organization, completed one blockchain product, developing the second version of the same product.

Experience: 2 years of developing blockchain dApps.

Personnel: 4 personnels: 2 Software Experts (web and blockchain software) and 2 Electrical Engineers (project management, market analysis, industry needs, business development).

Methodologies: Not being followed.

Certifications: No certifications, the PMI training courses have been taken.

Overview of Case

Project: A blockchain solution in the renewable energy domain, prosumers (consumers who produce their own energy) are certified by instantly matching production and consumption data of facilities with blockchain technology-based software in real time. Completed first version of the product, developing the second version of the same product.

Project Duration: 24 months

Project Personnel: 2 Software Experts (web and blockchain software) and 2 Electrical Engineers (project management, market analysis, industry needs, business development).

Interview Participants:

- Entrepreneur who is the founder of the organization - 15 years of experience in energy domain, 2 years of experience as project manager in blockchain based energy projects

- Web and blockchain software developer – 12 years of experience as software developer, 2 years of experience in developing blockchain applications.

Interview duration: 2 hours.

Related safety critical domain software category: Energy management and operation software.

Application/Implementation Status: Presented in the following table. We have added brief explanations to the table for all situations where ‘Fully Achieved’ has not been specified in practices. We have also presented the implementation status of the processes.

Processes	Base Practices	Process Implementation Status N/A, NI, PI, LI, FI	Practice Application Status N/A, NA, PA, LA, FA
1. Blockchain dApp project initiation process	1.1 Identify objectives and key performance indicators	PI	PA (objectives are identified but identification of key performance indicators are missing)
	1.2 Evaluate blockchain suitability		FA
	1.3 Evaluate the feasibility of the blockchain dApp project		FA
2. Blockchain dApp planning	2.1 Create blockchain dApp project scope, schedule, budget, and resources management plans	NI	FA
	2.2 Create a communication plan		NA (A communication plan is not created.)
	2.3 Create a change management plan		NA (A change management plan is not created.)
	2.4 Decide on the blockchain development life cycle model		NA (A life cycle model is not applied during the development of dApps.)
	2.5 Decide on the safety class of the product		FA
	2.6 Decide on the need for using digital assets		N/A (No digital assets have been used in the developed applications yet.)
3. Blockchain dApp monitoring and control	3.1 Monitor the blockchain dApp project against the plan	NI	LA (They are reporting to the public institution on the blockchain project’s adherence to the plan as they received support from the government, However, there can be deficiencies in the reporting process.)
	3.2 Control the blockchain dApp project		NA (No control-related activities are performed.)
	3.3 Manage corrective actions to closure		PA (Considering that the initial target output at the project’s onset might not fully meet market needs, action was taken to develop

			Version 2. No other actions were specified.)
4. Blockchain dApp requirements elicitation	4.1 Identify stakeholders	NI	FA
	4.2 Elicit stakeholder requirements		PA (Requirements are being collected, but a systematic approach is not followed.)
	4.3 Review stakeholder requirements		PA (Reviews are conducted, but there is no systematic approach.)
	4.4 Agree on requirements		NA (No activities are performed.)
	4.5 Manage changes made in the stakeholder requirements		NA (A systematic approach is not followed for change management.)
5. Blockchain dApp requirements analysis	5.1 Specify blockchain dApp system requirements	NI	FA
	5.2 Identify the consensus mechanism		FA
	5.3 Include tokenomics in blockchain dApps including digital tokens		N/A (Tokenomics have not yet been included)
	5.4 Specify blockchain dApp software requirements		FA
	5.5 Specify blockchain dApp security requirements		NA (No security requirements-related activities are performed.)
	5.6 Specify blockchain dApp privacy requirements		NA (No privacy requirements-related activities are performed.)
	5.7 Specify blockchain dApp safety requirements		NA (No privacy requirements-related activities are performed.)
	5.8 Validate the requirements, and update when necessary		NA (A systematic approach is not being followed for validation)
	5.9 Develop approval criteria for testing		NA (No approval criteria is developed)
6. Blockchain dApp risk management	6.1 Identify the software that could contribute to a hazardous situation and potential causes		NA (risk management process is not performed)
	6.2 Define risks to the blockchain dApp product		NA (risk management process is not performed)
	6.3 Apply risk mitigation plan and risk contingency plan		NA (risk management process is not performed)
	6.4 Analyze the process and product risks		NA (risk management process is not performed)

	6.5 Resolve the process and product risks	NI	NA (risk management process is not performed)
	6.6 Manage the process and product risks that may be raised by changes		NA (risk management process is not performed)
7. Blockchain dApp architectural design	7.1 Define and describe the blockchain dApp architecture	NI	FA
	7.2 Decide on blockchain network type		FA
	7.3 Decide platform use or network creation		FA
	7.4 Decide on storage method		FA
	7.5 Decide where to deploy the modules of the system		FA
	7.6 Decide on incentives if there is a need for digital assets		N/A (No digital assets have been used in the developed applications yet.)
	7.7 Ensure the security of the system		NA (The security have been stated to be covered by the blockchain platform; No activities are performed in this regard)
	7.8 Apply anonymity mechanism if needed		N/A (No anonymity mechanism have been applied in the developed applications yet.)
	7.9 Verify the architecture		NA (No activities are performed.)
8. Blockchain dApp detailed design	8.1 Prepare for detailed design	NI	NA (No activities are performed.)
	8.2 Design the backend		FA
	8.3 Design the frontend		FA
9. Blockchain dApp implementation	9.1 Develop unit verification procedures	NI	NA (No activities are performed.)
	9.2 Build APIs		N/A (APIs were not buit in the existing applications)
	9.3 Develop the backend		FA
	9.4 Develop the frontend, user interface		FA
10. Blockchain dApp integration	10.1 Integrate the backend and frontend units	LI	FA
	10.2 Verify and test the integration		LA (Information regarding smart contract testing was provided, there is no record kept.)
11. Blockchain dApp verification	11.1 Prepare for verification		NA (Verification strategy and procedures are not developed)

	11.2 Verify the blockchain dApp product	NI	LA (It was mentioned that developers conduct their own unit tests, but there is no activity of creating test cases and running a series of tests)
	11.3 Manage verification results		NA (The records of verification results are not being maintained.)
12. Blockchain dApp validation	12.1 Prepare for validation	NI	NA (Verification strategy and procedures are not developed.)
	12.2 Validate the blockchain dApp product		LA (Smart contracts are validated by review and analysis of their code logic, ensuring that they function as intended.)
	12.3 Manage validation results		NA (The records of validation results are not being maintained.)
13. Blockchain dApp quality assurance	13.1 Specify blockchain dApp product quality requirements	NI	NA (quality assurance process is not performed)
	13.2 Assure blockchain dApp product quality		NA (quality assurance process is not performed)
14. Blockchain dApp transition	14.1 Develop a transition strategy	NI	NA (transition strategy is not developed)
	14.2 Confirm the blockchain dApp product is ready		FA
	14.3 Deploy the blockchain dApp product on the test network		FA
	14.4 Deploy the blockchain dApp product on the main network		N/A (The dApp has not yet been deployed to the mainnet)
	14.5 Make the blockchain dApp product available to the users		N/A (The dApp has not yet been made available to users)
	14.6 Manage results of transition		N/A (The results of transition has not yet been managed)
15. Blockchain dApp maintenance	15.1 Develop a maintenance plan	NI	NA (maintenance plan is not developed)
	15.2 Analyze, assess, and accept or reject change requests		NA (The change request process is not systematically carried out, discussions are conducted through weekly or monthly meetings.)
	15.3 Implement, test, and deploy modifications		PA (Modifications are implemented and deployed, but there is no systematic approach)

15.4 Retire the blockchain dApp product	N/A (No retirement process has been carried out)

Overall Evaluation: The organization OE is a software company that focuses on renewable energy and blockchain technologies. A two-year-old company has started developing blockchain applications in the energy domain with its four employees. The first version of the product has been completed, and work is underway on the second version. It has been noted that the two of the staff members have 15 years of experience in the energy domain.

It cannot be said that the organization develops blockchain dApps compatible with the BDRM. Out of 146 questions (7 organization questions, 139 process questions), 75 have been directly or indirectly answered in the interview.

Considering the answers given by the organization BG, the research questions of the case study and the answers to the questions are presented below.

CSRQ1: Which BDRM processes and practices are applied in the organization?

- The 20 practices in the model are “Fully Applied”
- The 5 practices are“Partially Applied”.
- The 4 practices are “Largely Applied”
- The 29 practices are “Not Applied”.
- The 10 practices that have not yet been implemented in their dApps are marked as “Not Applicable.”

The Blockchain dApp integration process is “Largely Implemented”, Blockchain dApp project initiation process is “Partially Implemented” the remaining 13 processes are Not Implemented.

CSRQ2: Does the organization follow any specific processes or base practices when developing blockchain dApps that are not covered by the questions?

The organization OE stated that the questions are highly comprehensive, and they do not have any additional suggestions to add.

Improvement suggestions to the organization: Focus on processes related to identifying, analyzing, and mitigating risks. Emphasize on DApp security and quality. Take steps to determine security requirements and ensure the quality of DApp products. Concentrate on processes like creating communication plans and defining change management strategies. This focus can ensure the integrity of the projects and effective management of processes.

5.3.2.2 Second Case Study: Organization AZ

Organization AZ is one of the leading companies in Turkey that carries out blockchain based product development. The company has logistics and supply chain blockchain applications in the automotive domain, and they export them to several countries. We selected Organization AZ since they are experienced and we obtained following information in line with our questions in the "selection strategy" title.

Overview of Organization AZ

Location: İstanbul, Turkey

Expertise: Leading company in blockchain technology, completed eight blockchain products that have been delivered and started to be used. The company operates with blockchain solutions domestically and abroad.

Experience: 6 years of developing blockchain dApps

Personnel: 47 dedicated blockchain-focused professionals (project managers, system engineers, blockchain architects, blockchain developers, business analyst cryptologists, network infrastructure managers, software developers, quality experts, candidate engineers)

Methodologies: Agile, Scrum

Certifications: PMI certificate, ISO 9001, ISO 27001

Overview of Case

Project: A blockchain-based application including Blockchain compatible IoT devices for vehicles performing international transportation by road.

Project Duration: 14 months

Project Personnel: 11 dedicated employees (project manager, system engineer, blockchain architect, three blockchain developers, two software developers, business analyst, test engineer, quality expert)

Interview Participants:

- Project manager - 37 years of experience in customs and logistics processes, the owner of the company has been developing blockchain-based software. 6 years of experience as project manager in blockchain projects.

- Blockchain developer – 10 years of experience as software developer, 5 years of experience in developing blockchain applications.

- Quality expert - 15 years of expertise in quality management, a comprehensive background in ensuring the standards across various domains.

Interview duration: 3 hours

Related safety critical domain software category: Vehicle operational software

Application/Implementation Status: Presented in the following table. We have added brief explanations to the table for all situations where 'Fully Achieved' has not been specified in practices. We have also presented the implementation status of the processes.

Processes	Base Practices	Process Implementation Status N/A, NI, PI, LI, FI	Practice Application Status N/A, NA, PA, LA, FA
1. Blockchain dApp project initiation process	1.1 Identify objectives and key performance indicators	FI	FA
	1.2 Evaluate blockchain suitability		FA
	1.3 Evaluate the feasibility of the blockchain dApp project		FA
2. Blockchain dApp planning	2.1 Create blockchain dApp project scope, schedule, budget, and resources management plans		FA
	2.2 Create a communication plan	FI	FA
	2.3 Create a change management plan		FA
	2.4 Decide on the blockchain development life cycle model		FA
	2.5 Decide on the safety class of the product		FA
	2.6 Decide on the need for using digital assets		FA
3. Blockchain dApp monitoring and control	3.1 Monitor the blockchain dApp project against the plan		FA
	3.2 Control the blockchain dApp project	FI	FA
	3.3 Manage corrective actions to closure		FA
4. Blockchain dApp requirements elicitation	4.1 Identify stakeholders		FA
	4.2 Elicit stakeholder requirements		FA
	4.3 Review stakeholder requirements	FI	FA
	4.4 Agree on requirements		FA
	4.5 Manage changes made in the stakeholder requirements		FA
5. Blockchain dApp requirements analysis	5.1 Specify blockchain dApp system requirements		FA
	5.2 Identify the consensus mechanism		FA
	5.3 Include tokenomics in blockchain dApps including digital tokens		FA
	5.4 Specify blockchain dApp software requirements		FA
	5.5 Specify blockchain dApp security requirements	FI	FA
	5.6 Specify blockchain dApp privacy requirements		FA
	5.7 Specify blockchain dApp safety requirements		FA
	5.8 Validate the requirements, and update when necessary		FA

	5.9 Develop approval criteria for testing		FA
6. Blockchain dApp risk management	6.1 Identify the software that could contribute to a hazardous situation and potential causes		FA
	6.2 Define risks to the blockchain dApp product		FA
	6.3 Apply risk mitigation plan and risk contingency plan	FI	FA
	6.4 Analyze the process and product risks		FA
	6.5 Resolve the process and product risks		FA
	6.6 Manage the process and product risks that may be raised by changes		FA
7. Blockchain dApp architectural design	7.1 Define and describe the blockchain dApp architecture		FA
	7.2 Decide on blockchain network type		FA
	7.3 Decide platform use or network creation		FA
	7.4 Decide on storage method		FA
	7.5 Decide where to deploy the modules of the system	FI	FA
	7.6 Decide on incentives if there is a need for digital assets		FA
	7.7 Ensure the security of the system		FA
	7.8 Apply anonymity mechanism if needed		FA
	7.9 Verify the architecture		FA
8. Blockchain dApp detailed design	8.1 Prepare for detailed design		FA
	8.2 Design the backend	FI	FA
	8.3 Design the frontend		FA
9. Blockchain dApp implementation	9.1 Develop unit verification procedures		FA
	9.2 Build APIs		FA
	9.3 Develop the backend	FI	FA
	9.4 Develop the frontend, user interface		FA
10. Blockchain dApp integration	10.1 Integrate the backend and frontend units		FA
	10.2 Verify and test the integration	FI	FA
11. Blockchain dApp verification	11.1 Prepare for verification		FA
	11.2 Verify the blockchain dApp product	FI	FA
	11.3 Manage verification results		FA
12. Blockchain dApp validation	12.1 Prepare for validation		FA
	12.2 Validate the blockchain dApp product	FI	FA
	12.3 Manage validation results		FA
	13.1 Specify blockchain dApp product quality requirements	FI	FA

13. Blockchain dApp quality assurance	13.2 Assure blockchain dApp product quality		FA
14. Blockchain dApp transition	14.1 Develop a transition strategy	FI	FA
	14.2 Confirm the blockchain dApp product is ready		FA
	14.3 Deploy the blockchain dApp product on the test network		FA
	14.4 Deploy the blockchain dApp product on the main network		FA
	14.5 Make the blockchain dApp product available to the users		FA
	14.6 Manage results of transition		FA
15. Blockchain dApp maintenance	15.1 Develop a maintenance plan	FI	FA
	15.2 Analyze, assess, and accept or reject change requests		FA
	15.3 Implement, test, and deploy modifications		FA
	15.4 Retire the blockchain dApp product		N/A (No retirement process has been carried out)

Overall Evaluation: Organization AZ was founded by a team with more than 20 years of experience in fields such as logistics, supply chains, international trade, customs procedures, importer and exporter integration, finance and accounting integration. The company has an R&D center specifically for blockchain technology.

The organization develops blockchain dApps compatible with the BDRM. Out of 146 questions (7 organization questions, 139 process questions), 145 have been directly or indirectly answered in the interview. The only question related to the retirement of products is unanswered as no retirement process has been carried out in current dApp products.

Considering the answers given by the organization AZ, the research questions of the case study and the answers to the questions are presented below.

CSRQ1: Which BDRM processes and practices are applied in the organization?

- One practice that have not yet been implemented is marked as “Not Applicable”: 15.4 Retire the blockchain dApp product.

- The remaining 67 practices are categorized as “Fully Achieved”.

All of the processes are “Fully Implemented” by the organization.

The organization is experienced in carrying out application development processes and complying with relevant standards.

The case study findings at Organization AZ demonstrate the applicability of the BDRM in blockchain projects. The company’s extensive experience, skilled personnel, and adherence to best practices contribute to their success in developing and deploying blockchain applications.

CSRQ2: Does the organization follow any specific processes or base practices when developing blockchain dApps that are not covered by the questions?

According to the organization AZ, their questions are highly comprehensive and they have no further recommendations to offer.

5.3.2.3 Third Case Study:Organization ER

Organization ER develops a wide range of R&D-based products such as virtual reality, augmented reality, erp, artificial intelligence applications, cryptology, blockchain, cyber security, mobile games, and mobile application. The company has developed many products in the field of healthcare, such as clinical automation for healthcare personnel, patient tracking system, and software-based decision support system for diagnosis of attention deficit and hyperactivity disorder. They are also developing their latest product in the health domain based on blockchain.

Overview of Organization ER

Location: İstanbul, Turkey

Expertise: A wide range of health domain software products, one of them is blockchain-based.

Experience: 5 years of software development, 1 year of blockchain dApp development

Personnel: 19 personnels (project managers, system engineers, blockchain developers, software developers, information security experts, biomedical engineers, test engineer, quality expert)

Methodologies: Agile

Certifications: PMI certificate, ISO 9001, ISO 27001

Overview of Case

Project: Blockchain-based application for management of patient health data in in vitro fertilization centers

Project Duration: 18 months

Project Personnel: 10 dedicated employees (project manager, system engineer, two blockchain developers, three software developers, information security experts, test engineer, quality expert)

Interview Participants:

- Project manager - 14 years of experience as developer, analyst, and project manager in software development projects, 1 year of experience as project manager in blockchain projects, the owner of the company.

- Blockchain and software developer –5 years of experience as software developer, 1 year of experience in developing blockchain applications.

- Information security expert - 5 years of expertise in information security, Have the skills to understand, prevent and manage cyber threats. 1 year of experience in blockchain based applications.

Interview duration: 2.5 hours

Related safety critical domain software category: Health Software.

Application/Implementation Status: Presented in the following table. We have added brief explanations to the table for all situations where 'Fully Achieved' has not been specified in practices. We have also presented the implementation status of the processes.

Processes	**Base Practices**	**Process Implementation Status N/A, NI, PI, LI, FI**	**Practice Application Status N/A, NA, PA, LA, FA**
1. Blockchain dApp project initiation process	1.1 Identify objectives and key performance indicators		FA
	1.2 Evaluate blockchain suitability	FI	FA
	1.3 Evaluate the feasibility of the blockchain dApp project		FA
2. Blockchain dApp planning	2.1 Create blockchain dApp project scope, schedule, budget, and resources management plans		FA
	2.2 Create a communication plan		FA
	2.3 Create a change management plan	FI	FA
	2.4 Decide on the blockchain development life cycle model		FA
	2.5 Decide on the safety class of the product		FA
	2.6 Decide on the need for using digital assets		FA
3. Blockchain dApp monitoring and control	3.1 Monitor the blockchain dApp project against the plan		FA
	3.2 Control the blockchain dApp project	FI	FA
	3.3 Manage corrective actions to closure		FA
4. Blockchain dApp requirements elicitation	4.1 Identify stakeholders		FA
	4.2 Elicit stakeholder requirements		FA
	4.3 Review stakeholder requirements		FA
	4.4 Agree on requirements	FI	FA

	4.5 Manage changes made in the stakeholder requirements		FA
5. Blockchain dApp requirements analysis	5.1 Specify blockchain dApp system requirements	FI	FA
	5.2 Identify the consensus mechanism		FA
	5.3 Include tokenomics in blockchain dApps including digital tokens		FA
	5.4 Specify blockchain dApp software requirements		FA
	5.5 Specify blockchain dApp security requirements		FA
	5.6 Specify blockchain dApp privacy requirements		FA
	5.7 Specify blockchain dApp safety requirements		FA
	5.8 Validate the requirements, and update when necessary		FA
	5.9 Develop approval criteria for testing		FA
6. Blockchain dApp risk management	6.1 Identify the software that could contribute to a hazardous situation and potential causes	FI	FA
	6.2 Define risks to the blockchain dApp product		FA
	6.3 Apply risk mitigation plan and risk contingency plan		FA
	6.4 Analyze the process and product risks		FA
	6.5 Resolve the process and product risks		FA
	6.6 Manage the process and product risks that may be raised by changes		FA
7. Blockchain dApp architectural design	7.1 Define and describe the blockchain dApp architecture	FI	FA
	7.2 Decide on blockchain network type		FA
	7.3 Decide platform use or network creation		FA
	7.4 Decide on storage method		FA
	7.5 Decide where to deploy the modules of the system		FA
	7.6 Decide on incentives if there is a need for digital assets		FA
	7.7 Ensure the security of the system		FA
	7.8 Apply anonymity mechanism if needed		FA
	7.9 Verify the architecture		FA
8. Blockchain dApp detailed design	8.1 Prepare for detailed design	FI	FA
	8.2 Design the backend		FA
	8.3 Design the frontend		FA

9. Blockchain dApp implementation	9.1 Develop unit verification procedures		FA
	9.2 Build APIs	FI	FA
	9.3 Develop the backend		FA
	9.4 Develop the frontend, user interface		FA
10. Blockchain dApp integration	10.1 Integrate the backend and frontend units	FI	FA
	10.2 Verify and test the integration		FA
11. Blockchain dApp verification	11.1 Prepare for verification		FA
	11.2 Verify the blockchain dApp product	FI	FA
	11.3 Manage verification results		FA
12. Blockchain dApp validation	12.1 Prepare for validation		FA
	12.2 Validate the blockchain dApp product	FI	FA
	12.3 Manage validation results		FA
13. Blockchain dApp quality assurance	13.1 Specify blockchain dApp product quality requirements		FA
	13.2 Assure blockchain dApp product quality	FI	FA
14. Blockchain dApp transition	14.1 Develop a transition strategy		FA
	14.2 Confirm the blockchain dApp product is ready		FA
	14.3 Deploy the blockchain dApp product on the test network		FA
	14.4 Deploy the blockchain dApp product on the main network		FA
	14.5 Make the blockchain dApp product available to the users	FI	N/A (The development of the blockchain application in the health domain has not been completed yet.)
	14.6 Manage results of transition		N/A (The development of the blockchain application in the health domain has not been completed yet.)
15. Blockchain dApp maintenance	15.1 Develop a maintenance plan		N/A (The development of the blockchain application in the

		health domain has not been completed yet.)
15.2 Analyze, assess, and accept or reject change requests	N/A	N/A (The development of the blockchain application in the health domain has not been completed yet.)
15.3 Implement, test, and deploy modifications		N/A (The development of the blockchain application in the health domain has not been completed yet.)
15.4 Retire the blockchain dApp product		N/A (No retirement process has been carried out)

Overall Evaluation: Organization ER develops a wide range of R&D-based products in the health domain. They apply the project management experience they have gained in other applications to the blockchain health application development process.

The organization develops blockchain dApps compatible with the BDRM. Out of 146 questions (7 organization questions, 139 process questions), 136 have been directly or indirectly answered in the interview. Only questions related for making the blockchain dApp product available to the users, managing the results of transition, and maintenance process is unanswered as the development process of the blockchain application in the health domain is still ongoing.

Considering the answers given by the organization ER, the research questions of the case study and the answers to the questions are presented below.

CSRQ1: Which BDRM processes and practices are applied in the organization?

- Six practices that have not yet been implemented are marked as “Not Applicable”.
- The remaining 62 practices are categorized as “Fully Achieved”.

Blockchain dApp maintenance process has practices that have not yet been implemented, and this process is marked as “Not Applicable”. The remaining 14 processes are “Fully Implemented” by the organization.

The company has expertise implementing application development processes and adhering to appropriate standards. The case study findings at Organization ER demonstrate the applicability of the BDRM in blockchain projects.

CSRQ2: Does the organization follow any specific processes or base practices when developing blockchain dApps that are not covered by the questions?

According to the organization ER, questions are extremely detailed, and they have no additional recommendations.

5.3.2.4 Fourth Case Study: Developer SC

We observed the applicability of the model by conducting a case study with a developer experienced in blockchain-based application development within the health domain, which is one of the safety-critical areas. In interviews with the organizations, all practices of the BDRM are being individually reviewed. However, during the interview with the SC, we directed the questions towards 19 specific practices involving health-related information in the model. The aim was to validate the health related practices.

Overview of Case SC

Location: Ankara, Turkey

Project: A blockchain based application where health data of patients (COVID-19) is kept on the private blockchain

Project Duration: 8 months

Expertise: Completed one blockchain solution.

Interview Participant:

- Blockchain and software developer – 12 years of experience as computer engineer, researcher in defense industry. One year of experience in developing blockchain based health applications. Main research interests are blockchain technology, bioinformatics, big data problems, and decision support systems.

Interview duration: 1 hour

Related safety critical domain software category: Health Software.

Application/Implementation Status: Presented in the following table. We have added brief explanations to the table for all situations where 'Fully Achieved' has not been specified in practices. We have also presented the implementation status of the processes.

Processes	**Base Practices**	**Process Implementation Status N/A, NI, PI, LI, FI**	**Practice Application Status N/A, NA, PA, LA, FA**
2. Blockchain dApp planning	2.4 Decide on the blockchain development life cycle model		LA (Waterfall development life cycle model is followed, but

			not all stages were implemented systematically.)
	2.5 Decide on the safety class of the product	LI	LA (The application developed is in the safety class A category. The standards have started to be reviewed.)
4. Blockchain dApp requirements elicitation	4.2 Elicit stakeholder requirements	LI	LA (Requirements are defined according to the health domain needs, but a systematic approach is not followed.)
5. Blockchain dApp requirements analysis	5.4 Specify blockchain dApp software requirements	FI	FA
	5.7 Specify blockchain dApp safety requirements		FA
	5.8 Validate the requirements, and update when necessary		FA
6. Blockchain dApp risk management	6.1 Identify the software that could contribute to a hazardous situation and potential causes	PI	LA (If incorrect results regarding patient health data are recorded in the developed application, hazardous situations may occur. The standards have started to be reviewed.)
	6.2 Define risks to the blockchain dApp product		PA (The standards have started to be reviewed, risks have been defied but a systematic approach has not yet been followed.)
	6.4 Analyze the process and product risks		PA (The standards have started to be reviewed, risks have been analyzed but a systematic approach has not yet been followed)
	6.6 Manage the process and product risks that may be raised by changes		FA

7. Blockchain dApp architectural design	7.1 Define and describe the blockchain dApp architecture		FA
	7.3 Decide platform use or network creation		FA
	7.4 Decide on storage method		FA
	7.7 Ensure the security of the system	LI	LA (The security have been stated to be covered by the blockchain platform (Hyperledger Fabric); stated that private blockchain was preferred and cryptology mechanisms were used.)
	7.8 Apply anonymity mechanism if needed		N/A (No anonymity mechanism have been applied in the developed application)
	7.9 Verify the architecture		FA
10. Blockchain dApp integration	10.2 Verify and test the integration	LI	LA (testing was provided, there is no traceability in record kept.)
11. Blockchain dApp verification	11.2 Verify the blockchain dApp product	LI	LA (product is verified, there is no traceability in record kept.)
12. Blockchain dApp validation	12.2 Validate the blockchain dApp product	LI	LA (Smart contracts are validated by review and analysis of their code logic, ensuring that they function as intended. HL7 FHIR, GDPR were reviewed, will be taken into account in the subsequent application development process.)

Overall Evaluation: Developer SC has developed a blockchain based application where health data of patients is kept on the private blockchain. SC is working on a new project, which is about application of blockchain technology in clinical research.

It can be said that SC develops blockchain dApps compatible with the health related practices in BDRM. Out of 23 questions (3 organization questions, 20 process questions), 22 have been directly or indirectly answered in the interview. Only question about anonymity mechanism application remains unanswered due to the absence of current necessity for utilization.

Considering the answers given by the organization BG, the research questions of the case study and the answers to the questions are presented below.

CSRQ1: Which BDRM processes and practices are applied in the organization? (Only for health related practices and the processes associated with them)

- The 8 practices in the model are "Fully Applied"
- The 2 practices are"Partially Applied".
- The 8 practices are "Largely Applied"
- The 1 practice that have not yet been implemented is marked as "Not Applicable."

Blockchain dApp requirements analysis process is "Fully Implemented", Blockchain dApp risk management process is "Partially Implemented", the remaining six processes are "Largely Implemented".

CSRQ2: Does the organization follow any specific processes or base practices when developing blockchain dApps that are not covered by the questions? (Only for health related practices)

The SC stated that the questions are highly comprehensive, and he/she does not have any additional suggestions to add.

5.3.2.5 Fifth Case Study: Organization BG

Organization BG is one of the leading companies in Turkey that carries out both research and product development activities in the field of blockchain technology and crypto assets. We selected Organization BG since they are experienced and we obtained following information in line with our questions in the "selection strategy" title.

Overview of Organization BG

Location: Ankara, Turkey

Expertise: Leading company in blockchain technology, completed seven blockchain products that have been delivered and started to be used.

Experience: 7 years of developing blockchain dApps

Personnel: 25 dedicated blockchain-focused professionals (project managers, system engineers, blockchain architects, blockchain developers, cryptologists, network infrastructure managers, software developers, quality experts, business analysts, test engineers, candidate engineers)

Methodologies: Agile, Scrum, Waterfall

Certifications: PMI certificate, CMMI5

Overview of Case

Project: Blockchain-based digital identity management system

Project Duration: 12 months

Project Personnel: 10 dedicated employees (project manager, system engineer, blockchain architect, two blockchain developers, cryptologist, two software developers, business analyst, test engineer)

Interview Participants:

- Project manager - 26 years of experience as developer, analyst, systems engineer and project manager in software development projects, 6 years of experience as project manager in blockchain projects

- Blockchain developer – 8 years of experience as software developer, 4 years of experience in developing blockchain applications. Strong knowledge and experience in smart contract development, distributed ledger technologies, and consensus algorithms.

- Business analyst - 10 years of experience in business analysis, 2 years of experience in blockchain projects. Expertise in identifying, analyzing, and documenting business requirements.

- Test engineer – 6 years of experience as test engineer, 3 years of experience in software testing in blockchain projects. Expertise in creating software test strategies and test plans.

Interview Duration: 3 hours

Application/Implementation Status: Presented in the following table. We have added brief explanations to the table for all situations where 'Fully Achieved' has not been specified in practices. We have also presented the implementation status of the processes.

Processes	Base Practices	Process Implementation Status N/A, NI, PI, LI, FI	Practice Application Status N/A, NA, PA, LA, FA
1. Blockchain dApp project initiation process	1.1 Identify objectives and key performance indicators	FI	FA
	1.2 Evaluate blockchain suitability		FA
	1.3 Evaluate the feasibility of the blockchain dApp project		FA

2. Blockchain dApp planning	2.1 Create blockchain dApp project scope, schedule, budget, and resources management plans		FA
	2.2 Create a communication plan		FA
	2.3 Create a change management plan	FI	FA
	2.4 Decide on the blockchain development life cycle model		FA
	2.5 Decide on the safety class of the product		NA (Safety Critical dApps have not yet been developed)
	2.6 Decide on the need for using digital assets		FA
3. Blockchain dApp monitoring and control	3.1 Monitor the blockchain dApp project against the plan		FA
	3.2 Control the blockchain dApp project	FI	FA
	3.3 Manage corrective actions to closure		FA
4. Blockchain dApp requirements elicitation	4.1 Identify stakeholders		FA
	4.2 Elicit stakeholder requirements		FA
	4.3 Review stakeholder requirements	FI	FA
	4.4 Agree on requirements		FA
	4.5 Manage changes made in the stakeholder requirements		FA
5. Blockchain dApp requirements analysis	5.1 Specify blockchain dApp system requirements		FA
	5.2 Identify the consensus mechanism		FA
	5.3 Include tokenomics in blockchain dApps including digital tokens		FA
	5.4 Specify blockchain dApp software requirements	FI	FA
	5.5 Specify blockchain dApp security requirements		FA
	5.6 Specify blockchain dApp privacy requirements		FA
	5.7 Specify blockchain dApp safety requirements		N/A (Safety Critical dApps have not yet been developed)
	5.8 Validate the requirements, and update when necessary		FA
	5.9 Develop approval criteria for testing		FA
6. Blockchain dApp risk management	6.1 Identify the software that could contribute to a hazardous situation and potential causes		FA
	6.2 Define risks to the blockchain dApp product		FA
	6.3 Apply risk mitigation plan and risk contingency plan	FI	FA

	6.4 Analyze the process and product risks		FA
	6.5 Resolve the process and product risks		FA
	6.6 Manage the process and product risks that may be raised by changes		FA
7. Blockchain dApp architectural design	7.1 Define and describe the blockchain dApp architecture		FA
	7.2 Decide on blockchain network type		FA
	7.3 Decide platform use or network creation		FA
	7.4 Decide on storage method		FA
	7.5 Decide where to deploy the modules of the system	FI	FA
	7.6 Decide on incentives if there is a need for digital assets		FA
	7.7 Ensure the security of the system		FA
	7.8 Apply anonymity mechanism if needed		FA
	7.9 Verify the architecture		FA
8. Blockchain dApp detailed design	8.1 Prepare for detailed design		FA
	8.2 Design the backend	FI	FA
	8.3 Design the frontend		FA
9. Blockchain dApp implementation	9.1 Develop unit verification procedures		FA
	9.2 Build APIs		FA
	9.3 Develop the backend	FI	FA
	9.4 Develop the frontend, user interface		FA
10. Blockchain dApp integration	10.1 Integrate the backend and frontend units	FI	FA
	10.2 Verify and test the integration		FA
11. Blockchain dApp verification	11.1 Prepare for verification		FA
	11.2 Verify the blockchain dApp product	FI	FA
	11.3 Manage verification results		FA
12. Blockchain dApp validation	12.1 Prepare for validation		FA
	12.2 Validate the blockchain dApp product	FI	FA
	12.3 Manage validation results		FA
13. Blockchain dApp quality assurance	13.1 Specify blockchain dApp product quality requirements		FA
	13.2 Assure blockchain dApp product quality	FI	FA
	14.1 Develop a transition strategy		FA

14. Blockchain dApp transition	14.2 Confirm the blockchain dApp product is ready	FI	FA
	14.3 Deploy the blockchain dApp product on the test network		FA
	14.4 Deploy the blockchain dApp product on the main network		FA
	14.5 Make the blockchain dApp product available to the users		FA
	14.6 Manage results of transition		FA
15. Blockchain dApp maintenance	15.1 Develop a maintenance plan	FI	FA
	15.2 Analyze, assess, and accept or reject change requests		FA
	15.3 Implement, test, and deploy modifications		FA
	15.4 Retire the blockchain dApp product		FA

Overall Evaluation: Organization BG is an R&D center operating in blockchain technology and crypto assets. It conducts both research and product development activities, engaging in activities related to both fields. The organization is developing privacy, security, and confidentiality-focused critical blockchain projects. Government institutions in Turkey frequently prefer this organization for their blockchain solution needs.

The organization develops blockchain dApps compatible with the BDRM. Out of 146 questions (7 organization questions, 139 process questions), 138 have been directly or indirectly answered in the interview. Only nine questions directly related to the safety critical domain remain unanswered as applications in this domain have not yet been developed. Questions, which are related to the safety critical domain but can also be applied when developing applications in other domains are answered in detail by the organization BG.

Considering the answers given by the organization BG, the research questions of the case study and the answers to the questions are presented below.

CSRQ1: Which BDRM processes and practices are applied in the organization?

- Two practices that have not yet been implemented are marked as “Not Applicable.” These practices “2.5 Decide on safety class of the product”, “5.7 Specify blockchain dApp safety requirements” are directly related to the safety critical domain.

- The remaining 66 practices are categorized as “Fully Achieved”. Seven of the practices “2.4 Decide on the blockchain development life cycle model, 4.2 Elicit stakeholder requirements, 5.8 Validate the requirements and update when necessary, 7.3 Decide platform use or network creation, 7.8 Ensure security of the system, 10.2 Verify and test the integration, 12.2 Validate the blockchain dApp product.” include questions, which are specifically related to the safety critical domain and left unanswered. All the remaining questions about these practices have been answered in detail and there is a complete and systematic approach. So, these practices are also marked as “Fully Achieved”.

All of the processes are “Fully Implemented” by the organization.

Notable strengths include thorough project planning, effective risk management, and adherence to quality assurance practices.

The case study findings at Organization BG demonstrate the applicability of the BDRM in blockchain projects. The company’s extensive experience, skilled personnel, and adherence to best practices contribute to their success in developing and deploying blockchain applications.

CSRQ2: Does the organization follow any specific processes or base practices when developing blockchain dApps that are not covered by the questions?

It was suggested by the organization that “governance of the dApp product” process could be added. However, as the BDRM is a model encompassing the development process, we decided that adding a process focused on the usage of the created dApp product was not in the scope of the model.

5.4. Discussion

The BDRM is intended to provide a standard development framework for blockchain dApps. Using the meta-model of ISO/IEC 12207 (2017), and taking into account the related safety critical domain requirements, it incorporates essential processes and practices. The BDRM consists of fifteen processes and sixty-eight associated practices. The model provides a comprehensive framework for guiding individuals and organizations in the development of blockchain-based dApps in the safety critical domain.

The literature review has revealed studies addressing various aspects of blockchain dApp development processes and practices. These studies offer valuable insights into the recommendations for developing blockchain dApps. However, to the best of our knowledge, there is no comprehensive process reference model study for the entire blockchain dApp development process, particularly in safety-critical domains.

The studies reviewed present a diverse range of practices and processes relevant to blockchain dApp development. Notably, Chakraborty *et al.* (2018b) highlighted essential practices such as code review, unit testing, and community discussion for eliciting requirements. Marchesi *et al.* (2020) proposed a Scrum-based method emphasizing the importance of defining goals, identifying actors, and reviewing user stories. Antal *et al.* (2021) provided guidelines for design and implementation, including risk identification and DLT-compliant application design. Similarly, Nousias *et al.* (2022) introduced development and deployment processes on the Ethereum blockchain. While the reviewed studies offer valuable recommendations, they primarily focus on suggesting practices rather than providing a comprehensive development model. Furthermore, the discussion largely revolves around specific phases of development, overlooking the general approach needed, especially in safety-critical domains. Studies by Porru *et al.* (2017), Vacca *et al.* (2021), and Lahami *et al.*

(2022) address testing, software quality, and testing techniques in blockchain-oriented software but do not consider safety-critical domain standards.

In contrast, the proposed BDRM not only outlines processes for blockchain dApp development but also addresses the challenges of safety-critical domains. By integrating health-focused, automotive-specific, and energy domain-related standards, the BDRM ensures regulatory compliance. This comprehensive approach distinguishes the BDRM from existing studies and underscores its significance in guiding the systematic development of blockchain dApps in safety-critical domains.

In BDRM, a substantial proportion of the practices, 47% (32 of 68), contain blockchain-specific information. In addition, 19 practices incorporate safety critical domain specific information. The model also includes information on the safety classifications for the practices, as defined by the IEC 62304 standard (2006), ISO 26262 standard (2018), and IEC 61508 standard (2010).

The initial version of the model included thirteen processes and forty-six practices. Following expert feedback, the model was expanded to encompass 15 processes and 68 practices. The model was subjected to eight reviews by blockchain technology and safety critical domain software specialists. We first conducted an interview with a blockchain solution developer engineer working for a company that operates in a safety critical domain to determine the model's suitability for the organization. The processes and practices of the BDRM were described, and two open-ended questions were posed. The company did not implement any additional processes or practices beyond those outlined in the BDRM. This result indicates that the model is sufficiently inclusive. In addition, the BDRM increased company awareness of processes and practices that were not implemented within blockchain dApp projects. The company intends to implement the missing processes and practices in future projects.

Our validation approach comprised conducting case studies to explore the applicability of the BDRM. This encompassed five case studies: three companies operating within the health, energy, and automotive sectors; one company specializing in privacy and security oriented blockchain software; and one developer focused on creating blockchain-based applications in the health domain. The case studies involved a total of 11.5 hours of meetings. Each case study highlighted unique insights into the application of BDRM practices. Table 11 contains summary information about the processes and practice implementation situations of the cases.

Table 11: Process and practice implementation situation

Case No-Organization	Experience	BDRM Implementation	Implementation Status of Processes	Application Status of Practices
1- OE	Newer Player	Not developes BDRM-compatible blockchain dApps	1 process LI 1 process PI 13 processes NI	20 practices FA 5 practices PA. 4 practices LA 29 practices NA. 10 practices N/A

2- AZ	Experienced	Develops BDRM-compatible blockchain dApps	15 processes FI	67 practices FA 1 practice N/A
3- ER	Experienced	Develops BDRM-compatible blockchain dApps	14 processes FI 1 process N/A	62 practices FA 6 practices N/A
4- SC	Newer Player	Develops blockchain dApps compatible with the health related practices in BDRM	1 process FI 6 processes LI 1 process PI	8 practices FA 2 practices PA 8 practices LA 1 practice N/A
5- BG	Experienced	Develops BDRM-compatible blockchain dApps	15 processes FI	66 practices FA 2 practices N/A

Organization BG, demonstrated a robust implementation of BDRM processes, emphasizing meticulous planning, effective risk management, and a commitment to quality assurance. This shows the organization develops blockchain dApps compatible with the BDRM successfully.

On the other hand, Organization OE, a newer player focusing on renewable energy blockchain solutions, revealed a mixed implementation of BDRM practices, exposing gaps in crucial areas such as risk identification and quality assurance. This emphasized the need for startup companies to prioritize aspects like risk mitigation and security to ensure project integrity.

Organization AZ, is an experienced company exporting its products, with expertise in logistics and supply chain blockchain applications in automotive domain, exhibited comprehensive BDRM adoption except for the retirement process. This highlighted their proficiency in blockchain based safety critical application development and adherence to industry standards.

Similarly, Organization ER, specializing in a wide range of health-related R&D products, demonstrated a substantial implementation of BDRM practices; however, it revealed gaps in certain aspects of their blockchain application development process. This indicated their expertise in implementing application development procedures while also signaling areas for potential improvement.

Meanwhile, Developer SC, focusing on healthcare-related blockchain applications, displayed a comprehensive understanding of health domain-specific BDRM practices.

These case studies collectively underscored the adaptability of BDRM across diverse safety critical domains while highlighting the critical importance of comprehensive implementation. They emphasized the necessity for careful attention to safety, security, and privacy requirements, risk management, and quality assurance to ensure the integrity of blockchain projects in safety-critical domains. Ultimately, the case studies presented the potential and versatility of BDRM while also revealing areas for companies where further attention and development might be required for optimal outcomes.

Three of the organizations are experienced and two of them are newer players. According to our observations, there is a consistency between experience and BDRM compliance. The organizations BG, AZ and ER are experienced and they have PMI and quality certifications. These organizations develop BDRM-compatible blockchain dApps. On the other hand, organization OE is an entrepreneurial company and does not yet follow a systematic approach. This organization do not have any certifications. OE does not develop BDRM-compatible blockchain dApps.

The case studies highlight the adaptability of BDRM across diverse safety-critical domains while also revealing areas for further attention and development. Leveraging organizational experience and adhering to systematic approaches and certifications can significantly enhance BDRM compliance, ensuring the integrity and safety of blockchain projects in safety-critical domains.

In addition to defining processes for blockchain dApp development, the BDRM contributes to addressing the challenges outlined in the SLR (Baysal et al., 2021) and MLR studies (Baysal et al., 2023). The model contributes to an increase in awareness because it contains information on how to avoid these challenges. The following is a summary of the challenges and solutions:

After being stored in a blockchain, data cannot be changed or removed. However, data privacy regulations mandate that data be rectified or deleted upon request. In addition, the size of safety critical domain data can be quite large. Due to the increase in data size, systems must also deal with storage issues and mining costs. To address data removal-on-demand and data volume challenges, the BDRM includes “7.4. Decide on storage method” in the architectural design process for Blockchain dApps. This method provides three storage options: on-chain, hybrid, and off-chain (i.e., storing health data in external storage and its hash in the blockchain). Off-chain storage has the potential to solve problems associated with data deletion, modification, and size. However, when data is stored off-chain, it poses a risk of deletion and should be replaced with the roll-up technology, which relocates computations off-chain while retaining certain information for each transaction, thereby resolving storage issues. This solution is also included in the BDRM. Organization BG and AZ indicated that they utilized this method as a solution in their applications.

The following difficulty stems from the nature of blockchain networks. As data is stored in each block of a blockchain, data loss is impossible. This may, however, result in redundant data in the chain. In the “7.1. Define and describe the blockchain dApp architecture” practice, the BDRM suggests the use of IPFS, which is a distributed peer-to-peer storage network that inherently supports deduplication, in conjunction with blockchain. Organization BG uses IPFS as a solution to redundant data in the chains.

Due to consensus mechanisms and ledger replication across all network participants, blockchains face a scalability problem. This also results in significant computational power and storage space demands on each node. This is a performance issue. To address these performance and scalability constraints, the BDRM includes the practices “7.2. Decide on blockchain network type, 7.3 Decide on framework, and 5.2. Identify a consensus mechanism”.

The BDRM comprises all phases of development and guides the creation of blockchain-based dApps. Therefore, it contributes to the difficulty of developing smart contracts properly, which has a significant impact on the efficiency of the blockchain.

The next obstacle is that once a smart contract has been added to a network, its code cannot be altered. To upgrade following a change request, a new contract must be deployed. BDRM contains information about blockchain-specific design practices to aid in the creation of high-quality smart contracts and addresses the challenge of smart contract code changes. While conducting a case study with organization OE, we observed that smart contract modification is a challenge for the organization.

In addition, the BDRM has a “11. Blockchain dApp verification” practice that includes testing type recommendations for safety critical domains. This practice also includes suggestions for managing the execution of smart code and transaction fees. Organizations in case studies in the safety critical domain stated that they carried out detailed tests.

We also observed the following challenges during the case studies in validation phase of BDRM. Organizations pay special attention to the issue of whether there really is any logic when customers want blockchain-based applications even though the technology is not needed because it is niche. BDRM includes the practice “1.2. Evaluate blockchain suitability” to determine whether blockchain is applicable to the specified domain and capable of solving the specified problem.

It was mentioned that difficulties can arise in calculating gas fees for blockchain transactions and executions. BDRM includes the practice “1.3 Evaluate the feasibility of the blockchain dApp project”, which includes information about example tools that could be used for gas fee estimation and example about fee schedule.

Due to its decentralized nature, the developer of the blockchain may not perform maintenance. The sustainability, expansion, and resolution of issues fall under the responsibility of the user community. The decision-making for adding new features is their own, and the governance process should be well-designed. A multi-stakeholder decision-making mechanism and a suitable design for updating the code must be in place. Organizations mentioned that it adds adding extra load during the development phase. BDRM contains “15.2 Analyze, assess, and accept or reject change requests” practice that presents an example mechanism, which could be used to approve change requests in communities.

The challenges provided above and the solution approaches included in the BDRM are summarized in Table 12.

Table 12: Overview of Challenges and Solutions in BDRM

Challenge	Blockchain Solution in BDRM	Related Practice	Organization’s Status
Customers want blockchain-based applications even though the technology is not needed	Determine whether blockchain is applicable to the specified domain and capable of solving the specified problem	1.2. Evaluate blockchain suitability	BG faces this challenge.
Gas fee calculation challenges in blockchain transactions	Information about example tools that could be used for gas fee estimation and example about fee schedule	1.3 Evaluate the feasibility of the blockchain dApp project	OE faced challenges in gas fee calculation
Data Immutability vs. Privacy	Off-chain storage with roll-up technology	"7.4. Decide on storage method"	BG and AZ utilized this method.
Redundant Data in Blockchain	Use of IPFS for deduplication	"7.1. Define and describe the blockchain dApp architecture"	BG used IPFS to address redundant data in chains.
Scalability Challenges	Selection of blockchain network type, framework, and consensus mechanism	"7.2. Decide on blockchain network type," "7.3 Decide on framework," and "5.2. Identify a consensus mechanism"	Not faced scalability challenges in their projects.
Developing smart contracts properly, Smart Contract Code Changes	Deployment of new contract for upgrades	15.3 Implement, test, and modify modifications	OE faced challenges in smart contract modification.
Blockchain dApp Verification	Testing type recommendations for safety-critical domains	"11. Blockchain dApp verification" procedure	Organizations in safety-critical domains conduct detailed tests.
The decision-making for adding new features in communities, and the governance process	Presents an example mechanism, which could be used to approve change requests in communities	15.2 Analyze, assess, and accept or reject change requests	AZ experienced this challenge.

CHAPTER 6

CONCLUSION

This thesis proposes the creation of the BDRM and its implications. Blockchain technology offers significant potential in safety-critical domains like health, automotive, and energy due to its transparency, security, and decentralization. It provides a trustworthy environment for stored data and is tamper-resistant. However, there is a lack of comprehensive studies on blockchain processes and development guidelines in these domains. This thesis study aims to develop a generic BDRM to address these needs and facilitate effective blockchain application development in safety critical domains.

In this comprehensive study, we have introduced a generic BDRM developed through a rigorous process of design science research (DSR). The BDRM encompasses a set of 15 processes and 68 essential practices that are indispensable for the development of blockchain-based applications in safety critical domains. The BDRM contains specific information about health, automotive, and energy domains in 19 practices. 32 of 68 practices in the model contain blockchain-specific information.

The BDRM was developed through an incremental and iterative process, based on the results of SLR and MLR studies. Experts reviewed various versions of the model to ensure its applicability, completeness, correctness, consistency, understandability, and usability.

The BDRM, using the meta-model of ISO/IEC 12207 (2017), successfully integrates the requirements of the health-focused standards (i.e. IEC 62304, IEC 82304, ISO 14971) automotive-specific standards (i.e. ASPICE, ISO 26262), and energy domain-related standards (i.e IEC 61508) with blockchain development processes and practices.

The BDRM represents a significant solution to the challenges encountered in the development of blockchain dApps within safety-critical domains. Safety-critical domains, such as health, automotive, and energy, demand rigorous standards for data integrity, security, and regulatory compliance due to the potential safety risks. Traditional software development processes often lack to address these unique requirements.

By introducing the BDRM, this thesis proposes a standardized framework tailored specifically for the development of blockchain dApps within safety-critical domains. The BDRM serves as a comprehensive guide, outlining fundamental processes and practices necessary for the development, deployment, and maintenance of blockchain-based applications. Its generic nature allows for adaptability across various domains, while its focus on safety-critical domains ensures alignment with specific regulatory standards and requirements.

One of the key contributions of the BDRM is its dual-purpose functionality. Not only does it provide guidance for development activities, but it also ensures compliance with regulatory software development standards. This addresses a significant challenge faced by developers in safety-critical domains, where adherence to regulatory requirements often necessitates a substantial investment of time and effort. The BDRM streamlines this process by offering information for regulatory compliance, thereby reducing development time and minimizing the risk of non-compliance.

Moreover, the BDRM addresses the potential benefits of blockchain technology in mitigating the inherent challenges of safety-critical domains. By leveraging blockchain's attributes of transparency, security, and immutability, the BDRM enhances data integrity, reliability, and auditability within these domains. For example, in the health domain, blockchain technology can facilitate secure and transparent sharing of patient data, while ensuring compliance with privacy regulations such as HIPAA. Similarly, in the automotive industry, blockchain-based solutions can streamline supply chain management processes, improve vehicle security, and enhance traceability of vehicle histories, thereby reducing the risk of counterfeit parts and fraudulent activities.

In conclusion, the BDRM is a pioneering architecture that addresses the specific challenges of developing blockchain-based dApps in safety-critical domains. Its comprehensive framework, dual-purpose functionality, and focus on regulatory compliance make it a valuable resource for developers, researchers, and practitioners interested in using the strength of blockchain technology to ensure safety, reliability, and compliance in safety-critical domains.

We present information including implications and future studies under three subheadings. In Section 6.1, we provide information on the implications for theory, including guidance for blockchain application development, significant potential for standardization efforts, and serving as a valuable reference for domain-specific model development. In Section 6.2, the focus is on the implications for practice, highlighting the multifaceted role of BDRM as a comprehensive guide for development activities, ensuring regulatory compliance, and addressing challenges in safety-critical domains. Section 6.3 includes future work recommendations.

6.1 Implications for Theory

As the blockchain environment is still in its early stages of standardization, it is important to establish a systematic method to guide the development of blockchain applications. To the best of our knowledge our research is the first to meet the need for a process model in this particular area.

BDRM also has the potential to contribute to the development of blockchain technology's standardization. Technical Committee 307 of the International Organization for Standardization (ISO/TC 307 Participation, n.d.) and the FDA (2019) are currently developing standards for blockchain and distributed ledger technologies. Their efforts demonstrate their dedication to the advancement of the field. Such standardization initiatives would benefit greatly from a process reference model such as the one presented in this study.

In addition, the BDRM can serve as a valuable example for researchers who wish to develop domain-specific models using design science research approach.

6.2 Implications for Practice

This study aims to contribute to existing literature and practitioners by highlighting the dual purpose service of BDRM. It serves as a guide for development activities and ensures compliance with regulatory software development standards. The practical implications of the BDRM are significant, addressing the application of theoretical insights in real-world scenarios. It also addresses challenges in safety-critical domains, addressing potential benefits of blockchain technology.

The study asserts that BDRM is a pioneering model that encompasses necessary processes and practices for developing blockchain-based decentralized applications in safety-critical domains. The model can be used independent of any particular life cycle development model. By adhering to the BDRM, developers can ensure regulatory compliance when creating blockchain-based safety critical applications, a process that would ordinarily require substantial time and effort to adapt.

The adoption of BDRM offers organizations various opportunities, including improved quality assurance, more effective risk management, and overall project success.

6.3 Future Work

Despite the fact that this thesis has a significant contribution to the industry by presenting the BDRM and its use in the context of related applications, there are a number of directions that future study and development could take into account:

Case Studies: More case studies could be conducted with companies with different size from health, energy and automative domains.

Capability Assessment: The model emphasizes the process dimension, and the objective of the model does not entail capability assessment. BDRM could be used in conjunction with the ISO/IEC TS 33061:2021 standard (2021) to evaluate the maturity and capability of software processes within organizations.

Awareness Review: Since blockchain technology is a relatively new field, efforts could be made to measure organizations' awareness in this area.

BDRM Enhancement: Regularly updating the BDRM to keep up-to-date with regulatory modifications and guaranteeing that the BDRM continues to adhere to the most recent guidelines.

Process Guidance Tool: Developing a software tool aligned with BDRM processes to help the development of safety-critical blockchain applications.

Innovation with Technology Integration: Examining how blockchain technology can be integrated with cutting-edge innovations in the safety critical domain, like artificial intelligence, the Internet of Things (IoT), and decentralized identification, can lead to new avenues for innovation.

Open Source Blockchain Solutions: There are popular blockchain platforms developed as open source and continuously improved by communities in the finance domain. Creating such an open source blockchain solution for safety-critical domains could be thoroughly examined, and precautions could be identified.

To sum up, there are a lot of opportunities for future work in this field, ranging from improving the model itself to investigating new technologies and how they might be used in the safety critical domain. The success of dApps will be aided by continued research and development in these fields.

REFERENCES

25010, I. (2011). *ISO/IEC 25010:2011 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models*. https://www.iso.org/standard/35733.html

Abdeen, M. A. R., Ali, T., Khan, Y., & Yagoub, M. C. E. (2019). Fusing identity management, HL7 and blockchain into a global healthcare record sharing architecture. *International Journal of Advanced Computer Science and Applications*, *10*(6), 630–636. https://doi.org/10.14569/ijacsa.2019.0100681

Adams, R. J., Smart, P., & Huff, A. S. (2017). Shades of Grey: Guidelines for Working with the Grey Literature in Systematic Reviews for Management and Organizational Studies. *International Journal of Management Reviews*, *19*(4), 432–454. https://doi.org/10.1111/ijmr.12102

Agbo, C., Mahmoud, Q., & Eklund, J. (2019). Blockchain Technology in Healthcare: A Systematic Review. *Healthcare*, *7*(2), 56. https://doi.org/10.3390/healthcare7020056

Akmeemana, C. (2021). *How Australia's National Blockchain Roadmap sets an example for the world*. https://forkast.news/australia-national-blockchain-roadmap-example/

Alhajjaj, Y., Qatawneh, M., Abualghanam, O., & Almaiah, M. A. (2023). Using of Blockchain in the Context of Automotive Industry: A Survey. *2023 International Conference on Information Technology: Cybersecurity Challenges for Sustainable Cities, ICIT 2023 - Proceeding*, 519–523. https://doi.org/10.1109/ICIT58056.2023.10225958

Alketbi, A., Nasir, Q., & Abu Talib, M. (2020). Novel blockchain reference model for government services: Dubai government case study. *International Journal of System Assurance Engineering and Management*, *11*(6), 1170–1191. https://doi.org/10.1007/s13198-020-00971-2

AMSYS. (n.d.). *AMCHART Patient driven Electronic Health Record on the blockchain*. https://www.youtube.com/watch?v=KpmRnPc1eIk

Anas, H., Ilyas, M., Tariq, Q., & Hummayun, M. (2016). Requirements Validation Techniques: An Empirical Study. *International Journal of Computer Applications*, *148*(14), 5–10. https://doi.org/10.5120/ijca2016910911

Antal, C., Cioara, T., Anghel, I., Antal, M., & Salomie, I. (2021). Distributed ledger technology review and decentralized applications development guidelines. *Future Internet*, *13*(3), 1–32. https://doi.org/10.3390/fi13030062

Antwi, M., Adnane, A., Ahmad, F., Hussain, R., Habib ur Rehman, M., & Kerrache, C. A. (2021). The Case of HyperLedger Fabric as a Blockchain Solution for Healthcare Applications. *Blockchain: Research and Applications*, *2*(1), 100012. https://doi.org/10.1016/j.bcra.2021.100012

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. *Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016*, 25–30. https://doi.org/10.1109/OBD.2016.11

Bada, A. O., Damianou, A., Angelopoulos, C. M., & Katos, V. (2021). Towards a Green Blockchain: A Review of Consensus Mechanisms and their Energy Consumption. *Proceedings - 17th Annual International Conference on Distributed Computing in Sensor Systems, DCOS 2021*, 503–511. https://doi.org/10.1109/DCOSS52077.2021.00083

Baysal, M. V., Özcan-Top, Ö., & Betin-Can, A. (2023). Blockchain technology applications in the health domain: a multivocal literature review. *The Journal of Supercomputing*, 1–45. https://doi.org/10.1007/s11227-022-04772-1

Baysal, M. V., Özcan-Top, Ö., & Can, A. B. (2021). Implications of Blockchain Technology in the Health Domain. *Advances in Software Engineering, Education, and e-Learning*, 641–656. https://doi.org/10.1007/978-3-030-70873-3_45

Baysal, M. V., “Blockchain dApp Process Reference Model (BDRM) Technical Report METU/II-TR-2024-249,” 2024.

Belchior, R., Vasconcelos, A., Guerreiro, S., & Correia, M. (2022). A Survey on Blockchain Interoperability: Past, Present, and Future Trends. *ACM Computing Surveys*, *54*(8). https://doi.org/10.1145/3471140

Bhawiyuga, A., Wardhana, A., Amron, K., & Kirana, A. P. (2019). *Platform for Integrating Internet of Things Based Smart Healthcare System and Blockchain Network*. 55–60.

Bitcoin. (n.d.). *Bitcoin*. Retrieved October 19, 2022, from https://bitcoin.org

Blockchain, I. (n.d.). *How blockchain can streamline healthcare*. https://www.youtube.com/watch?v=h3aZ8mrlR-0

BlocksEDU. (n.d.). *Blockchain for Electronic Health Records?* https://www.youtube.com/watch?v=fVQOOF5GCFs

Cai, W., Wang, Z., Ernst, J. B., Hong, Z., Feng, C., & Leung, V. C. M. (2018). Decentralized Applications: The Blockchain-Empowered Software System. *IEEE Access*, *6*, 53019–53033. https://doi.org/10.1109/ACCESS.2018.2870644

Castaldo, Luigi and Cinque, V. (2018). Blockchain-Based Logging for the Cross-Border Exchange of eHealth Data in Europe. In *Security in Computer and*

Information Sciences (Vol. 821). Springer International Publishing. https://doi.org/10.1007/978-3-319-95189-8

Cernian, A., Tiganoaia, B., Sacala, I. S., Pavel, A., & Iftemi, A. (2020). Patientdatachain: A blockchain-based approach to integrate personal health records. *Sensors (Switzerland)*, *20*(22), 1–24. https://doi.org/10.3390/s20226538

Chakraborty, P., Shahriyar, R., Iqbal, A., & Bosu, A. (2018a). Understanding the software development practices of blockchain projects: A survey. *International Symposium on Empirical Software Engineering and Measurement*. https://doi.org/10.1145/3239235.3240298

Chakraborty, P., Shahriyar, R., Iqbal, A., & Bosu, A. (2018b). Understanding the software development practices of blockchain projects: A survey. *International Symposium on Empirical Software Engineering and Measurement*, 1–10. https://doi.org/10.1145/3239235.3240298

Chattu, V. K., Nanda, A., Chattu, S. K., Kadri, S. M., & Knight, A. W. (2019). The emerging role of blockchain technology applications in routine disease surveillance systems to strengthen global health security. *Big Data and Cognitive Computing*, *3*(2), 1–10. https://doi.org/10.3390/bdcc3020025

Chen, Y., Ding, S., Xu, Z., Zheng, H., Yang, S., & Chen, Y. (2019). *Blockchain-Based Medical Records Secure Storage and Medical Service Framework. June 2017.*

Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2020). A Novel Blockchain Based Smart Contract System for eReferral in Healthcare: HealthChain. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 12435 LNCS*. Springer International Publishing. https://doi.org/10.1007/978-3-030-61951-0_9

Chenthara, S., Ahmed, K., Wang, H., Whittaker, F., & Chen, Z. (2020). Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. In *PLoS ONE* (Vol. 15, Issue 12 December). https://doi.org/10.1371/journal.pone.0243043

Choudhury, O., Fairoza, N., Sylla, I., & Das, A. (2019). *A Blockchain Framework for Managing and Monitoring Data in Multi-Site Clinical Trials*. 1–13. http://arxiv.org/abs/1902.03975

Cichosz, S. L., Stausholm, M. N., Kronborg, T., Vestergaard, P., & Hejlesen, O. (2019). How to Use Blockchain for Diabetes Health Care Data and Access Management: An Operational Concept. *Journal of Diabetes Science and Technology*, *13*(2), 248–253. https://doi.org/10.1177/1932296818790281

Coelho, F. C. (2018). *Optimizing Disease Surveillance by Reporting on the Blockchain*. 1–10. http://dx.doi.org/10.1101/278473

Coinsider. (n.d.). *Can Blockchain " Fix " Healthcare ? (Solve . Care Deep Dive)*. https://www.youtube.com/watch?v=sJDSFI8M_5g

COMPARE Tracking Switched Outcomes in Cinical Trials. (n.d.). Retrieved January 2, 2020, from https://compare-trials.org/results

Crypto, T. (n.d.). *Solve Care - Healthcare on Blockchain*. https://www.youtube.com/watch?v=IYGJ9q5cMcc

Cyran, M. A. (2018). Blockchain as a Foundation for Sharing Healthcare Data. *Blockchain in Healthcare Today*. https://doi.org/10.30953/bhty.v1.13

Davidson, J. (2022). *Coinbase Vault (Complete 2022 Guidei,* Retrieved Jun 18, 2023, from https://www.walletwhys.com/co?nbase-vault/

Deloitte. (2017). Blockchain risk management Risk functions need to play an active role in shaping blockchain strategy. In *Deloitte*. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-blockchain-risk-management.pdf

Dentacoin ecosystem. (n.d.). Retrieved April 10, 2020, from https://dentacoin.com

Destefanis, G., Marchesi, M., Ortu, M., Tonelli, R., Bracciali, A., & Hierons, R. (2018). Smart contracts vulnerabilities: A call for blockchain software engineering? *International Workshop on Blockchain Oriented Software Engineering*, 19–25. https://doi.org/10.1109/IWBOSE.2018.8327567

Dey, T., Jaiswal, S., Sunderkrishnan, S., & Katre, N. (2018). HealthSense: A medical use case of Internet of Things and blockchain. *Proceedings of the International Conference on Intelligent Sustainable Systems, ICISS 2017*, *Iciss*, 486–491. https://doi.org/10.1109/ISS1.2017.8389459

Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2017). Secure and Trustable Electronic Medical Records Sharing using Blockchain. *Annual Symposium Proceedings. AMIA Symposium*, *2017*, 650–659.

e-estonia. (n.d.). *An Overview of e-Health Services in Estonia [Video]*. https://www.youtube.com/watch?v=H4QLzQGMI3k

ECC. (2023). *Deploying American Blockchains Act of 2023 Draft Bill*. https://doi.org/10.1016/s0140-6736(02)85846-9

Einaste, T. (n.d.). *Blockchain and healthcare: the Estonian experience*. https://e-estonia.com/blockchain-healthcare-estonian-experience/

Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016). A Case Study for Blockchain in Healthcare. *Proceedings of IEEE Open & Big Data Conference*, *13*, 13. https://www.healthit.gov/sites/default/files/5-56-onc_blockchainchallenge_mitwhitepaper.pdf

Ellervee, A., Matulevicius, R., & Mayer, N. (2017). A comprehensive reference model for blockchain-based distributed ledger technology. *CEUR Workshop Proceedings*, *1979*, 320–333.

Erturk, E., Lopez, D., & Yu, W. Y. (2019). Benefits and risks of using blockchain in smart energy: A literature review. *Contemporary Management Research*, *15*(3), 205–225. https://doi.org/10.7903/cmr.19650

Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R. (2018). Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Computing*, *5*(1), 31–37. https://doi.org/10.1109/MCC.2018.011791712

Ethereum. (n.d.). *Ethereum*. Retrieved January 15, 2023, from https://ethereum.org/en/what-is-ethereum/

Ethereum Tester. (2022). Retrieved January 16, 2023, from https://github.com/ethereum/eth-tester

Fan, K., Wang, S., Ren, Y., Li, H., & Yang, Y. (2018). MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. *Journal of Medical Systems*, *42*(8), 1–11. https://doi.org/10.1007/s10916-018-0993-7

FBI. (n.d.). *Insurance Fraud*. Retrieved January 19, 2023, from https://www.fbi.gov/stats-services/publications/insurance-fraud

FDA. (2019). *FDA's Technology Modernization Action Plan (TMAP)*. https://www.fda.gov/media/130883/download

FDA. (2023). *Food and Drug Administration (FDA)*. Retrieved March 3, 2022, from https://www.fda.gov/home

Finck, M. (2018). Blockchains and Data Protection in the European Union. *European Data Protection Law Review*, *4*(1), 17–35. https://doi.org/10.21552/edpl/2018/1/6

Flowdevelopers. (2022). *Dapp Deployment Guide*. https://developers.flow.com/flow/dapp-development/deployment

Foundation, H. (n.d.). *ACTION-EHR : Patient-Centric Blockchain-Based Healthcare Data Management for ... Alevtina Dubovitskaya*. https://www.youtube.com/watch?v=mH5jUNaiejs

Fraga-Lamas, P., & Fernández-Caramés, T. M. (2019). A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry. *IEEE Access*, *7*, 17578–17598. https://doi.org/10.1109/ACCESS.2019.2895302

Garousi, V., Felderer, M., & Mäntylä, M. V. (2019). Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Information and Software Technology*, *106*(May 2018), 101–121. https://doi.org/10.1016/j.infsof.2018.09.006

Gharat, A., Aher, P., Chaudhari, P., & Alte, B. (2021). A Framework for Secure Storage and Sharing of Electronic Health Records using Blockchain Technology.

ITM Web of Conferences, *40*, 03037. https://doi.org/10.1051/itmconf/20214003037

Giustini, D. (2012). *Finding the Hard to Finds*. https://studylib.net/doc/7663974/finding-the-hard-to-finds---hlwiki-canada

Gong, J., & Zhao, L. (2020). Blockchain application in healthcare service mode based on Health Data Bank. *Frontiers of Engineering Management*, *7*(4), 605–614. https://doi.org/10.1007/s42524-020-0138-9

Gong, Y., van Engelenburg, S., & Janssen, M. (2021). A reference architecture for blockchain-based crowdsourcing platforms. *Journal of Theoretical and Applied Electronic Commerce Research*, *16*(4), 937–958. https://doi.org/10.3390/jtaer16040053

Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. *Journal of Medical Systems*, *42*(7), 1–7. https://doi.org/10.1007/s10916-018-0982-x

Guti, O., Romero, G., Luis, P., Salazar, A., Charris, M., & Wightman, P. (n.d.). *HealthyBlock : Blockchain-Based IT Architecture for Electronic Medical Records Resilient to Connectivity Failures*.

Hafid, A., Hafid, A. S., & Samih, M. (2020). Scaling Blockchains: A Comprehensive Survey. *IEEE Access*, *8*, 125244–125262. https://doi.org/10.1109/ACCESS.2020.3007251

Haq, I., & Muselemu, O. (2018). Blockchain Technology in Pharmaceutical Industry to Prevent Counterfeit Drugs. *International Journal of Computer Applications*, *180*(25), 8–12. https://doi.org/10.5120/ijca2018916579

Hashim, F., Shuaib, K., & Sallabi, F. (2021). Medshard: Electronic health record sharing using blockchain sharding. *Sustainability (Switzerland)*, *13*(11), 1–21. https://doi.org/10.3390/su13115889

Hathaliya, J., Sharma, P., Tanwar, S., & Gupta, R. (2019). Blockchain-Based Remote Patient Monitoring in Healthcare 4.0. *Proceedings of the 2019 IEEE 9th International Conference on Advanced Computing, IACC 2019*, 87–91. https://doi.org/10.1109/IACC48062.2019.8971593

Healthcare IT News Staff. (2021). *The biggest healthcare data breaches of 2021*. Healthcare IT News. https://www.healthcareitnews.com/news/biggest-healthcare-data-breaches-2021

Healthureum. (n.d.). *Healthureum HHEM - Introducing blockchain into healthcare*. https://www.youtube.com/watch?v=pX0uWV1utbg

Healthverity. (n.d.). Retrieved January 5, 2023, from https://healthverity.com/

Heidenreich, G. (2014). Scope of IEC Health Software Standards. *TOPRA Annual Medical Devices Symposium*.

Heilman, E., Baldimtsi, F., & Goldberg, S. (2016). Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain Bitcoin Transactions. *Financial Cryptography and Data Security*, pp 43–60. https://doi.org/10.1007/978-3-662-53357-4

Hevner, A., & Chatterjee, S. (2010). *Design Science Research in Information Systems*. 9–22. https://doi.org/10.1007/978-1-4419-5653-8_2

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems. *MIS Quarterly*, *28*(1), 75–105.

Hohenheim, G. (2018). *AIDOC, blog on a blockchain company in AI & Healthcare*. https://medium.com/@grhohenheim/aidoc-blog-on-a-blockchain-company-in-ai-healthcare-b6020488ccc4

Hölbl, M., Kompara, M., Kamišalić, A., & Zlatolas, L. N. (2018). A systematic review of the use of blockchain in healthcare. *Symmetry*, *10*(10). https://doi.org/10.3390/sym10100470

Hyperledger. (n.d.). *hy.pdf*. https://www.hyperledger.org/blog/2019/12/02/hyperledger-for-healthcare-how-fabric-drives-the-next-generation-pharma-supply-chain

Hyperledger Composer. (2018). *Hyperledger Composer*. https://github.com/hyperledger/composer/releases

IBM. (n.d.). *Using Blockchain to Prevent Counterfeit Drugs in Kenya*. https://www.youtube.com/watch?v=11Z4-XYoZAE

IEC. (2010). *IEC 61508-3:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*. https://webstore.iec.ch/publication/5517

IEC 61508-2. (2010). *IEC 61508-2 Functional safety of electrical/electronic/programmable electronic safety-related systems - Requirements for electrical/electronic/programmable electronic safety- related systems*.

IEC 61508-3. (2010). *IEC 61508-3 Functional safety of electrical/electronic/programmable electronic safety-related systems - Software requirements: Vol. Partie 1:*

IEC 61508-5. (2010). *IEC 61508-5 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Examples of methods for the determination of safety integrity levels*. https://nobelcert.com/DataFiles/FreeUpload/IEC 61508-5-2010.pdf

IEC 61508-6. (2010). *IEC 61508-6 Functional safety of electrical/electronic/programmable electronic safety-related systems - Guidelines on the application of IEC 61508-2 and IEC 61508-3*.

IEC 62304. (2006). *IEC 62304:2006 Medical device software — Software life cycle processes*. https://www.iso.org/standard/38421.html

IEC 82304. (2016). *IEC 82304-1:2016 Health software — Part 1: General requirements for product safety*. https://www.iso.org/standard/59543.html

Interbit. (n.d.). *' Blockchain in Healthcare ' from BTL CTO Hugh Halford Thompson*. https://www.youtube.com/watch?v=yT0aM6D-TTk

Investopedia. (2022). *51% Attack: Definition, Who Is At Risk, Example, and Cost*. Investopedia. https://www.investopedia.com/terms/1/51-attack.asp#:~:text=our editorial policies-,What Is a 51%25 Attack%3F,power to alter the blockchain.

ISO/IEC/IEEE 12207. (2017). *ISO/IEC/IEEE 12207:2017 Systems and software engineering — Software life cycle processes*. https://www.iso.org/standard/63712.html

ISO/IEC. (2019). *ISO/IEC 25030, Software Engineering — Software product quality requirements and evaluation (SQuaRE) - Quality requirements*.

ISO/IEC 15504. (2012). *INTERNATIONAL STANDARD ISO / IEC 15504-5 An exemplar Process Assessment Model* (Vol. 2012).

ISO/IEC 33061. (2021). *ISO/IEC TS 33061:2021 Information technology — Process assessment — Process assessment model for software life cycle processes*. https://www.iso.org/standard/80362.html

ISO/TC 307 Participation. (n.d.). *ISO/TC 307 Blockchain and distributed ledger technologies Participation*. https://www.iso.org/committee/6266604.html?view=participation

ISO 14971. (2019). *ISO 14971 Medical devices — Application of risk management to medical devices*.

ISO 26262-2. (2018). *ISO 26262 Road vehicles — Functional safety —Management of functional safety*.

ISO 26262-6. (2018). *ISO 26262 Road vehicles — Functional safety —Product development at the software level*.

ISO 26262-7. (2018). *ISO 26262 Road vehicles-Functional safety-Part 7: Production, operation, service and decommissioning* (Vol. 2018). https://www.kekaoxing.com

ISO 26262-9. (2018). *ISO 26262-9 Road vehicles — Functional safety —Automotive safety integrity level (ASIL)-oriented and safety-oriented analyses*.

ISO 26262. (2018). *ISO 26262:2018 Road vehicles — Functional safety*. https://www.iso.org/standard/68383.html

Ivan, D. (2016). Moving Toward a Blockchain-based Method for the Secure Storage of Patient Records. *NIST Workshop on Blockchain & Healthcare*, *August*, 11. https://www.healthit.gov/sites/default/files/9-16-drew_ivan_20160804_blockchain_for_healthcare_final.pdf

Jha, S. (2023). *The Complete Guide for Types of Blockchain!* Simplilearn. https://www.simplilearn.com/tutorials/blockchain-tutorial/types-of-blockchain

Jita, H., & Pieterse, V. (2018). A framework to apply the internet of things for medical care in a home environment. *ACM International Conference Proceeding Series*, 45–54. https://doi.org/10.1145/3291064.3291065

Juneja, A., & Marefat, M. (2018). Leveraging blockchain for retraining deep learning architecture in patient-specific arrhythmia classification. *2018 IEEE EMBS International Conference on Biomedical and Health Informatics, BHI 2018*, *2018-Janua*(March), 393–397. https://doi.org/10.1109/BHI.2018.8333451

Jung, H. H., & Pfister, F. M. J. (2020). Blockchain-enabled Clinical Study Consent Management. *Technology Innovation Management Review*, *10*(2), 14–24. https://doi.org/10.22215/timreview/1325

Kaur, H., Alam, M. A., Jameel, R., Mourya, A. K., & Chang, V. (2018). A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment. *Journal of Medical Systems*, *42*(8), 1–14. https://doi.org/10.1007/s10916-018-1007-5

Khalil, I. (2019). *A Novel Architecture for Tamper Proof Electronic Health Record Management System using Blockchain Wrapper*. 97–105.

Khan, K. M., Arshad, J., & Khan, M. M. (2018). Secure digital voting system based on blockchain technology. *International Journal of Electronic Government Research*, *14*(1), 53–62. https://doi.org/10.4018/IJEGR.2018010103

Khan, S., Amin, M. B., Azar, A. T., & Aslam, S. (2021). Towards Interoperable Blockchains: A Survey on the Role of Smart Contracts in Blockchain Interoperability. *IEEE Access*, *9*. https://doi.org/10.1109/ACCESS.2021.3106384

Kim, H. J., Kim, H. H., Ku, H., Yoo, K. D., Lee, S., Park, J. I., Kim, H. J., Kim, K., Chung, M. K., Lee, K. H., & Kim, J. H. (2021). Smart decentralization of personal health records with physician apps and helper agents on blockchain: Platform design and implementation study. *JMIR Medical Informatics*, *9*(6), 1–14. https://doi.org/10.2196/26230

Kim, T. M., Lee, S. J., Chang, D. J., Koo, J., Kim, T., Yoon, K. H., & Choi, I. Y. (2021). Dynamichain: Development of medical blockchain ecosystem based on dynamic consent system. *Applied Sciences (Switzerland)*, *11*(4), 1–20.

https://doi.org/10.3390/app11041612

Kirli, D., Couraud, B., Robu, V., Salgado-Bravo, M., Norbu, S., Andoni, M., Antonopoulos, I., Negrete-Pincetic, M., Flynn, D., & Kiprakis, A. (2022). Smart contracts in energy systems: A systematic review of fundamental approaches and implementations. *Renewable and Sustainable Energy Reviews*, *158*(November 2021), 112013. https://doi.org/10.1016/j.rser.2021.112013

Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering - A systematic literature review. *Information and Software Technology*, *51*(1), 7–15. https://doi.org/10.1016/j.infsof.2008.09.009

Koul, R. (2018a). Blockchain Oriented Software Testing - Challenges and Approaches. *2018 3rd International Conference for Convergence in Technology, I2CT 2018*, 1–6. https://doi.org/10.1109/I2CT.2018.8529728

Koul, R. (2018b). Blockchain Oriented Software Testing - Challenges and Approaches. *3rd International Conference for Convergence in Technology*, 1–6. https://doi.org/10.1109/I2CT.2018.8529728

Kshetri, N. (2018). Blockchain and Electronic Healthcare Records. *IEEE Computer*, *51*(12), 59–63.

Kumar, Adarsh, Krishnamurthi, R., Nayyar, A., Sharma, K., Grover, V., & Hossain, E. (2020). *A Novel Smart Healthcare Design , Simulation , and Implementation Using*. 118433–118471. https://doi.org/10.1109/ACCESS.2020.3004790

Kumar, Akhil, Liu, R., & Shan, Z. (2020). Is Blockchain a Silver Bullet for Supply Chain Management? Technical Challenges and Research Opportunities. *Decision Sciences*, *51*(1), 8–37. https://doi.org/10.1111/deci.12396

Kumar, R., Marchang, N., & Tripathi, R. (2020). Distributed Off-Chain Storage of Patient Diagnostic Reports in Healthcare System Using IPFS and Blockchain. *2020 International Conference on COMmunication Systems and NETworkS, COMSNETS 2020*, 1–5. https://doi.org/10.1109/COMSNETS48256.2020.9027313

Lahami, M., Maalej, A. J., Krichen, M., & Hammami, M. A. (2022). A Comprehensive Review of Testing Blockchain Oriented Software. *International Conference on Evaluation of Novel Approaches to Software Engineering, ENASE - Proceedings*, *May*, 355–362. https://doi.org/10.5220/0011042800003176

Landi, H. (2020). *IBM rolls out blockchain network to address supply-chain issues caused by COVID-19*. https://www.fiercehealthcare.com/tech/ibm-rolls-out-blockchain-network-to-match-healthcare-organizations-non-traditional-suppliers

Lawson, T. (2018). Accelerating technology disruption in the automotive market - Blockchain in the automotive industry. *Deloitte*.

https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/consumer-business/deloitte-cn-consumer-blockchain-in-the-automotive-industry-en-180809.pdf

Lee, H. A., Kung, H. H., Udayasankaran, J. G., Kijsanayotin, B. M. M. P., Marcelo, A. B., Chao, L. R., & Hsu, C. Y. (2020). An architecture and management platform for blockchain-based personal health record exchange: Development and usability study. *Journal of Medical Internet Research*, *22*(6), 1–15. https://doi.org/10.2196/16748

Lee, H., Kung, H., & Udayasankaran, J. G. (2020). *An Architecture and Management Platform for Blockchain-Based Personal Health Record Exchange : Development and Usability Study Corresponding Author : 22*, 1–15. https://doi.org/10.2196/16748

Lee, S. H., & Yang, C. S. (2018). Fingernail analysis management system using microscopy sensor and blockchain technology. *International Journal of Distributed Sensor Networks*, *14*(3). https://doi.org/10.1177/1550147718767044

Leeming, G., Cunningham, J., & Ainsworth, J. (2019). A Ledger of Me: Personalizing Healthcare Using Blockchain Technology. *Frontiers in Medicine*, *6*(July), 1–10. https://doi.org/10.3389/fmed.2019.00171

Leeway Hertz. (2022). *What is Zero Knowledge Proof and its role in blockchain?* https://www.leewayhertz.com/zero-knowledge-proof-and-blockchain/#What-are-the-advantages-of-Zero-Knowledge-Proof

Li, S., Zhou, T., Yang, H., & Wang, P. (2023). *Blockchain-Based Secure Storage and Access Control Scheme for Supply Chain Ecological Business Data : A Case Study of the*.

Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2018). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*, *2017-Octob*, 1–5. https://doi.org/10.1109/PIMRC.2017.8292361

Lindman, J., Berryhill, J., Benjamin, W., & Barbieri-Piccinin, M. (2020). *The Uncertain Promise of Blockchain for Government*. OECD Observatory of Public Sector Innovation (OPSI)'s Blog. https://medium.com/digital-states/the-uncertain-promise-of-blockchain-for-government-e99fd69141fd

Lu, Q., & Xu, X. (2017). Adaptable Blockchain- Based Systems: A case study for product traceability. *IEEE Software*, *34(6)*, 21–27.

M.Höst, & P.Runeson. (2007). Checklists for Software Engineering Case Study Research. *Proceedings - 1st International Symposium on Empirical Software Engineering and Measurement, ESEM 2007*, 482–484. https://doi.org/10.1109/ESEM.2007.46

Mamo, N., Martin, G. M., Desira, M., Ellul, B., & Ebejer, J. P. (2020). Dwarna: a blockchain solution for dynamic consent in biobanking. *European Journal of Human Genetics*, *28*(5), 609–626. https://doi.org/10.1038/s41431-019-0560-9

Marchesi, L., Marchesi, M., & Tonelli, R. (2020). ABCDE—agile block chain DApp engineering. *Blockchain: Research and Applications*, *1*(1–2), 100002. https://doi.org/10.1016/j.bcra.2020.100002

Marchesi, M., Marchesi, L., & Tonelli, R. (2018). An Agile Software Engineering Method to Design Blockchain Applications. *Proceedings of the 14th Central and Eastern European Software Engineering Conference Russia*, 1–8. https://doi.org/10.1145/3290621.3290627

MarketsandMarket. (2022). *Blockchain.News - Growth of Blockchain Market.*

Mauri, R. (2017). *Blockchain for fraud prevention: Industry use cases*. IBM Blockchain Blog. https://www.ibm.com/blogs/blockchain/2017/07/blockchain-for-fraud-prevention-industry-use-cases/

Mccarthy, M. (n.d.). *Harvard Blockchain Health Care Use Cases MIT ' s Shada AlSalama PhD*. https://www.youtube.com/watch?v=lc0SIx1zvP0

McGhin, T., Choo, K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications*, *135*(1), 62–75. https://doi.org/.1037//0033-2909.I26.1.78

MDD. (2023). *The Medical Device Directives*. European Comission. https://ec.europa.eu/growth/sectors/medical-devices/current-directives_en

MDR. (2017). *European Commission - Medical Device Regulations*. https://health.ec.europa.eu/medical-devices-sector/directives_en

MediBloc. (n.d.). Retrieved April 11, 2020, from https://medibloc.org/en

Medicalchain. (n.d.). *Medicalchain Explainer Video - Blockchain Technology for Electronic Health Records*. https://www.youtube.com/watch?v=CsxjlsBYmrI

Medicalchain. (2018). *Medicalchain Whitepaper*. https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf

Medicalchain. (2020). Retrieved April 11, 2020, from https://medicalchain.com/en/

MediShare (MDS). (n.d.). Retrieved April 11, 2020, from https://www.medishare.com/

Miraz, M. H., & Ali, M. (2020a). Blockchain Enabled Smart Contract Based Applications: Deficiencies with the Software Development Life Cycle Models. *Baltica Journal*, *33*(1), 101–116.

Miraz, M. H., & Ali, M. (2020b). *Blockchain Enabled Smart Contract Based*

Applications: Deficiencies with the Software Development Life Cycle Models (Vol. 33, Issue 1). http://arxiv.org/abs/2001.10589

Muniat, A., Ullah, P. R., & Mushsharat, S. (2021). *An Automated Approach towards Smart Healthcare with Blockchain and Smart Contracts*. 250–255.

Musamih, A., Salah, K., Jayaraman, R., Arshad, J., Debe, M., Al-Hammadi, Y., & Ellahham, S. (2021). A blockchain-based approach for drug traceability in healthcare supply chain. *IEEE Access*, *9*, 9728–9743. https://doi.org/10.1109/ACCESS.2021.3049920

Naheed, S., Faiza, K., Elhadj, C. G., & Anoud, B. (2021). *Blockchain smart contracts : Applications , challenges , and future trends*. 2901–2925.

Nakagawa, E. Y., Oliveira Antonino, P., & Becker, M. (2011). Reference architecture and product line architecture: A subtle but critical difference. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6903 LNCS*(October 2016), 207–211. https://doi.org/10.1007/978-3-642-23798-0_22

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://doi.org/10.1007/s10838-008-9062-0

Norwich University Online. (2018). *The 5 Pillars of Information Assurance*. https://online.norwich.edu/academic-programs/resources/the-5-pillars-of-information-assurance

Nour, M., Chaves-Avila, J. P., & Sanchez-Miralles, A. (2022). Review of Blockchain Potential Applications in the Electricity Sector and Challenges for Large Scale Adoption. *IEEE Access*, *10*, 47384–47418. https://doi.org/10.1109/ACCESS.2022.3171227

Nousias, N., Tsakalidis, G., Petridou, S., & Vergidis, K. (2022). Modelling the Development and Deployment of Decentralized Applications in Ethereum Blockchain: A BPMN-Based Approach. In *Lecture Notes in Business Information Processing: Vol. 447 LNBIP*. Springer International Publishing. https://doi.org/10.1007/978-3-031-06530-9_5

Nugent, T., Upton, D., & Cimpoesu, M. (2016). Improving data transparency in clinical trials using blockchain smart contracts. *F1000Research*, *5*, 1–9. https://doi.org/10.12688/f1000research.9756.1

OECD. (2022). *Recommendation of the Council on blockchain and other distributed ledger technologies*. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0470

Oliveira, M. T. de, H.Reis, L., Carrano, R. C., Seixas, F. L., Saade, D. C., Albuquerque, C. V., Fernandes, N. C., Olabarriaga, S. . D., Medeiros, D. S., & Mattos., D. M. (2019). Towards a Blockchain-Based Secure Electronic Medical Record for Healthcare Applications. *IEEE International Conference on Communications*, *2019-May*. https://doi.org/10.1109/ICC.2019.8761307

Omar, I. A., Jayaraman, R., Debe, M. S., Salah, K., Yaqoob, I., & Omar, M. (2021). Automating Procurement Contracts in the Healthcare Supply Chain Using Blockchain Smart Contracts. *IEEE Access*, *9*, 37397–37409. https://doi.org/10.1109/ACCESS.2021.3062471

Omar, I. A., Jayaraman, R., Salah, K., Simsekler, M. C. E., Yaqoob, I., & Ellahham, S. (2020). Ensuring protocol compliance and data transparency in clinical trials using Blockchain smart contracts. *BMC Medical Research Methodology*, *20*(1), 1–17. https://doi.org/10.1186/s12874-020-01109-5

Panda, S. S., Jena, D., & Das, P. (2021). A Blockchain-Based Distributed Authentication System for Healthcare. *International Journal of Healthcare Information Systems and Informatics*, *16*(4), 1–14. https://doi.org/10.4018/ijhisi.20211001.oa12

Pandey, P., & Litoriya, R. (2020a). Implementing healthcare services on a large scale: Challenges and remedies based on blockchain technology. *Health Policy and Technology*, *9*(1), 69–78. https://doi.org/10.1016/j.hlpt.2020.01.004

Pandey, P., & Litoriya, R. (2020b). Securing and authenticating healthcare records through blockchain technology. *Cryptologia*, *44*(4), 341–356. https://doi.org/10.1080/01611194.2019.1706060

Patel, V. (2019). A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Informatics Journal*, *25*(4), 1398–1411. https://doi.org/10.1177/1460458218769699

Patientory. (n.d.). Retrieved April 17, 2021, from https://patientory.com/

Pawar, P., Parolia, N., Shinde, S., Edoh, T. O., & Singh, M. (2021). eHealthChain—a blockchain-based personal health information management system. *Annales Des Telecommunications/Annals of Telecommunications*. https://doi.org/10.1007/s12243-021-00868-6

Pham, H. L., Tran, T. H., & Nakashima, Y. (2019). A Secure Remote Healthcare System for Hospital Using Blockchain Smart Contract. *2018 IEEE Globecom Workshops, GC Wkshps 2018 - Proceedings*, 1–6. https://doi.org/10.1109/GLOCOMW.2018.8644164

Porru, S., Pinna, A., Marchesi, M., & Tonelli, R. (2017). Blockchain-oriented software engineering: Challenges and new directions. *Proceedings - 2017 IEEE/ACM 39th International Conference on Software Engineering Companion, ICSE-C 2017*, 169–171. https://doi.org/10.1109/ICSE-C.2017.142

Prusty, N. (2017). *Building Blockchain Projects*. Packt Publishing Ltd.

Raryelcostasouza. (2020). *pyTranscriber Application*. https://github.com/raryelcostasouza/pyTranscriber/releases

Rathee, G., & Sharma, A. (2020). *A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology*. 9711–9733.

Runeson, P., Engström, E., & Storey, M.-A. (2020). The Design Science Paradigm as a Frame for Empirical Software Engineering. *Contemporary Empirical Methods in Software Engineering*, 127–147. https://doi.org/10.1007/978-3-030-32489-6_5

Runeson, P., & Höst, M. (2009). Guidelines for conducting and reporting case study research in software engineering. *Empirical Software Engineering*, *14*(2), 131–164. https://doi.org/10.1007/s10664-008-9102-8

Saravanan, M., Shubha, R., Marks, A. M., & Iyer, V. (2018). SMEAD: A secured mobile enabled assisting device for diabetics monitoring. *11th IEEE International Conference on Advanced Networks and Telecommunications Systems, ANTS 2017*, 1–6. https://doi.org/10.1109/ANTS.2017.8384099

Schäffer, M., di Angelo, M., & Salzer, G. (2019). Performance and Scalability of Private Ethereum Blockchains. *Lecture Notes in Business Information Processing*, *361*(August), 103–118. https://doi.org/10.1007/978-3-030-30429-4_8

Schär, F. (2021). Decentralized finance: on blockchain-and smart contract-based financial markets. *Federal Reserve Bank of St. Louis Review, 103*(2), 153–174. https://doi.org/10.20955/r.103.153-74

Schneier. (2021). *Smart Contract Bug Results in $31 Million Loss*. https://doi.org/10.1108/03684920910991603

Sean Au, T. P. (2018). *Tokenomics: The Crypto Shift of Blockchains, ICOs, and Tokens*. https://books.google.com.tr/books?hl=tr&lr=&id=hCdyDwAAQBAJ&oi=fnd&pg=PP1&dq=Study+on+tokenomics+in+blockchain+dApps+including+digital+tokens.&ots=jZP7KrFzep&sig=y2jEepla2yZMiCX_FJq5QFRvQWw&redir_esc=y#v=onepage&q&f=false

Sedgwick, K. (2023). *Bitcoin History Part 10: The 184 Billion BTC Bug – Featured Bitcoin News*. https://news.bitcoin.com/bitcoin-history-part-10-the-184-billion-btc-bug/

Shae, Z., & Tsai, J. J. P. (2017). On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine. *Proceedings - International Conference on Distributed Computing Systems*, 1972–1980. https://doi.org/10.1109/ICDCS.2017.61

Shammer, A. (1979). How to share a secret. *Communications of the ACM*, *22*(11). https://doi.org/10.1007/978-3-642-15328-0_17

Sharma, S. (2019). PubHeal-A Decentralized Platform on Health Surveillance of People. *2019 IEEE Pune Section International Conference, PuneCon 2019*, 1–6.

https://doi.org/10.1109/PuneCon46936.2019.9105834

Shi, S., He, D., Li, L., Kumar, N., & Khurram, M. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers & Security*, *97*(January), 101966.

Sillaber, C., & Waltl, B. (2017). Life Cycle of Smart Contracts in Blockchain Ecosystems. *Datenschutz Und Datensicherheit - DuD*, *41*(8), 497–500. https://doi.org/10.1007/s11623-017-0819-7

Singh Chouhan, A., Sanaullah Qaseem, M., Mohammed Abdul Basheer, Q., & Asma Mehdia, M. (2021). Blockchain based EHR system architecture and the need of blockchain inhealthcare. *Materials Today: Proceedings*, *xxxx*. https://doi.org/10.1016/j.matpr.2021.06.114

SRcoin. (n.d.). Retrieved April 11, 2020, from https://www.srcoin.info

Stackoverflow. (2017). Retrieved April 11, 2020, from *Permissions within a blockchain ?*

State of the DApps. (2022). *DApp Statistics*. Retrieved May 21, 2023, from https://www.stateofthedapps.com/stats

Sultana, M., Hossain, A., Laila, F., Taher, K. A., & Islam, M. N. (2020). *Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology*. 1–10.

Sun, B., Lv, Z., & Li, Q. (2021). Obstetrics Nursing and Medical Health System Based on Blockchain Technology. *Journal of Healthcare Engineering*, *2021*. https://doi.org/10.1155/2021/6631457

Sylim, P., Liu, F., Marcelo, A., & Fontelo, P. (2018). Blockchain technology for detecting falsified and substandard drugs in distribution: Pharmaceutical supply chain intervention. *Journal of Medical Internet Research*, *20*(9), 1–12. https://doi.org/10.2196/10163

Synaptic Health Alliance. (2021). *Our pilot project*. https://www.synaptichealthalliance.com/project

Takyar, A. (2021). *BLOCKCHAIN IN PHARMA SUPPLY CHAIN-REDUCING COUNTERFEIT DRUGS*. https://www.leewayhertz.com/blockchain-in-pharma-supply-chain/

Taralunga, D. D., & Florea, B. C. (2021). A blockchain-enabled framework for mhealth systems. *Sensors*, *21*(8), 1–24. https://doi.org/10.3390/s21082828

Taylor, T. (2021). *Hackers , Breaches , and the Value of Healthcare Data*. https://www.securelink.com/blog/healthcare-data-new-prize-hackers/

TBV. (2022a). *Enerji sektöründe blokzinciri gelişmeleri*.

TBV. (2022b). *Ülke genelinde uygulanabilir enerji sektörü blockchain kullanim alanlari, avantajlar ve riskler*.

TechTarget. (2022). *blockchain dApp*. https://www.techtarget.com/iotagenda/definition/blockchain-dApp

Telusko. (n.d.). *Blockchain in Healthcare | Use Case*. https://www.youtube.com/watch?v=dvFOMm6mBao

The Health Insurance Portability and Accountability Act (HIPAA). (n.d.). Retrieved January 2, 2020, from https://www.hipaajournal.com/hipaa-privacy-laws/

Thompson, B. B. (2022). *Blockchain Testing Tutorial What is Blockchain ? Features of Blockchain includes Type of Blockchain Public Blockchain :* https://www.guru99.com/blockchain-testing.html

Tith, D., Lee, J. S., Suzuki, H., Wijesundara, W. M. A. B., Taira, N., Obi, T., & Ohyama, N. (2020). Patient consent management by a purpose-based consent model for electronic health record based on blockchain technology. *Healthcare Informatics Research*, *26*(4), 265–273. https://doi.org/10.4258/hir.2020.26.4.265

Tripathi, G., Ahad, M. A., & Paiva, S. (2020). S2HS- A blockchain based approach for smart healthcare system. *Healthcare*, *8*(1), 100391. https://doi.org/10.1016/j.hjdsi.2019.100391

Trufflesuite. (2021). *Ganache: A Tool for Creating a Local Blockchain for Fast Ethereum Development.* https://github.com/trufflesuite/ganache

Trustradius. (2023). *Automotive Software Solutions*. https://www.trustradius.com/automotive?f=75

Tseng, J. H., Liao, Y. C., Chong, B., & Liao, S. W. (2018). Governance on the drug supply chain via gcoin blockchain. *International Journal of Environmental Research and Public Health*, *15*(6). https://doi.org/10.3390/ijerph15061055

Uddin, M. (2021). Blockchain Medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry. *International Journal of Pharmaceutics*, *597*(November 2020), 120235. https://doi.org/10.1016/j.ijpharm.2021.120235

Uddin, M. A., Stranieri, A., Gondal, I., & Balasubramanian, V. (2018). Continuous Patient Monitoring with a Patient Centric Agent: A Block Architecture. *IEEE Access*, *6*, 32700–32726. https://doi.org/10.1109/ACCESS.2018.2846779

Upadhyay, N. (2020). Demystifying blockchain: A critical analysis of challenges, applications and opportunities. *International Journal of Information Management*, *54*(October). https://doi.org/10.1016/j.ijinfomgt.2020.102120

Usman, M., & Qamar, U. (2020). Secure Electronic Medical Records Storage and Sharing Using Blockchain Technology. *Procedia Computer Science*, *174*, 321–

327. https://doi.org/10.1016/j.procs.2020.06.093

Usmani, F. (2022). *Stakeholders in Project Management : Definition , Types & Examples Stakeholders in Project Management*. https://pmstudycircle.com/stakeholders-in-project-management-definition-and-types

Vacca, A., Di Sorbo, A., Visaggio, C. A., & Canfora, G. (2021). A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges. *Journal of Systems and Software*, *174*, 110891. https://doi.org/10.1016/j.jss.2020.110891

VDA QMC Working Group. (2023). *Automotive SPICE*. https://vda-qmc.de/wp-content/uploads/2023/12/Automotive-SPICE-PAM-v40.pdf

Villarreal, E. R. D., Garcia-Alonso, J., Moguel, E., & Alegria, J. A. H. (2023). Blockchain for Healthcare Management Systems: A Survey on Interoperability and Security. *IEEE Access*, *11*(January), 5629–5652. https://doi.org/10.1109/ACCESS.2023.3236505

Vitalik. (2021). *An Incomplete Guide to SEO*. https://vitalik.ca/general/2021/01/05/rollup.html

Vora, J., Nayyar, A., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., & Rodrigues, J. J. P. C. (2019). BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records. *2018 IEEE Globecom Workshops, GC Wkshps 2018 - Proceedings*, 1–6. https://doi.org/10.1109/GLOCOMW.2018.8644088

Vota, W. (2019). *10 Blockchain Implementation Risks in International Development*. https://www.ictworks.org/blockchain-implementation-risks/#.Y6oG13ZBxPY

Vu, T. X., Chatzinotas, S., & Ottersten, B. (2019). Blockchain-based Content Delivery Networks: Content Transparency Meets User Privacy. *IEEE Wireless Communications and Networking Conference, WCNC*, *2019-April*. https://doi.org/10.1109/WCNC.2019.8885904

Wang, H., & Song, Y. (2018). *Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain*.

Webmedy. (n.d.). *Advantages of Blockchain Technology for Healthcare*. https://www.youtube.com/watch?v=r5Eqdm9v2_E

Wong, D. R., Bhattacharya, S., & Butte, A. J. (2019). Prototype of running clinical trials in an untrustworthy environment using blockchain. *Nature Communications*, *10*(1), 1–8. https://doi.org/10.1038/s41467-019-08874-y

World Health Organisation (WHO). (2017). *1 in 10 Medical Products in Developing Countries Is Substandard or Falsified*. https://www.who.int/news/item/28-11-2017-1-in-10-medical-products-in-developing-countries-is-substandard-or-falsified

Wu, H., & Wang, L. (2019). *A Patient-Centric Interoperable Framework for Health Information Exchange via Blockchain*. 0–4.

Wu, Z., Zhang, J., Gao, J., Li, Y., Li, Q., Guan, Z., & Chen, Z. (2020). Kaya: A Testing Framework for Blockchain-based Decentralized Applications. *Proceedings - 2020 IEEE International Conference on Software Maintenance and Evolution, ICSME 2020*, 826–829. https://doi.org/10.1109/ICSME46990.2020.00103

Wust, K., & Gervais, A. (2018). Do you need a blockchain? *Proceedings - 2018 Crypto Valley Conference on Blockchain Technology, CVCBT 2018*, *i*, 45–54. https://doi.org/10.1109/CVCBT.2018.00011

Xia, Q. I., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare : Trust-less Medical Data Sharing Among. *IEEE Access*, *5*, 1–10. https://doi.org/10.1109/ACCESS.2017.2730843

Xia, Q., Sifah, E. B., Smahi, A., Amofa, S., & Zhang, X. (2017). BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. *Information (Switzerland)*, *8*(2). https://doi.org/10.3390/info8020044

Xiao, Y., Xu, B., Jiang, W., & Wu, Y. (2021a). *The HealthChain Blockchain for Electronic Health Records : Development Study Corresponding Author : 23*, 1–13. https://doi.org/10.2196/13556

Xiao, Y., Xu, B., Jiang, W., & Wu, Y. (2021b). The healthchain blockchain for electronic health records: Development study. *Journal of Medical Internet Research*, *23*(1), 1–13. https://doi.org/10.2196/13556

Xilinx. (n.d.). *The Developer ' s Guide to Understanding*. https://www.xilinx.com/products/design-tools/resources/the-developers-guide-to-blockchain-development.html

Xu, X., Weber, I., Staples, M., Xu, X., Weber, I., & Staples, M. (2019). Design Process for Applications on Blockchain. *Architecture for Blockchain Applications*, 93–111. https://doi.org/10.1007/978-3-030-03035-3_6

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., & Rimba, P. (2017). A Taxonomy of Blockchain-Based Systems for Architecture Design. *IEEE International Conference on Software Architecture*, 243–252. https://doi.org/10.1109/ICSA.2017.33

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain Technology Overview - National Institute of Standards and Technology Internal Report 8202. In *NIST Interagency/Internal Report*. https://doi.org/10.6028/NIST.IR.8202

Yaqoob, S., Khan, M. M., Talib, R., Butt, A. D., Saleem, S., Arif, F., & Nadeem, A. (2019). Use of blockchain in healthcare: A systematic literature review. *International Journal of Advanced Computer Science and Applications*, *10*(5), 644–653. https://doi.org/10.14569/ijacsa.2019.0100581

Zheng, Q., Li, Y., Chen, P., & Dong, X. (2019). An Innovative IPFS-Based Storage Model for Blockchain. *Proceedings - 2018 IEEE/WIC/ACM International Conference on Web Intelligence, WI 2018*, 704–708. https://doi.org/10.1109/WI.2018.000-8

Zhuang, Y., Chen, Y., Shae, Z., Shyu, C., & Hall, P. N. (2020). *Generalizable Layered Blockchain Architecture for Health Care Applications : Development , Case Studies , and Evaluation Corresponding Author : 22*, 1–13. https://doi.org/10.2196/19029

Zhuang, Y., Sheets, L., Gao, X., Shen, Y., Shae, Z., Tsai, J. J. P., & Shyu, C. (2020). *Development of A Blockchain Framework for Virtual Clinical Trials*. 1412–1420.

Zhuang, Y., Sheets, L. R., Chen, Y. W., Shae, Z. Y., Tsai, J. J. P., & Shyu, C. R. (2020). A patient-centric health information exchange framework using blockchain technology. *IEEE Journal of Biomedical and Health Informatics*, *24*(8), 2169–2176. https://doi.org/10.1109/JBHI.2020.2993072

Zolfaghari, A. H., Nasiri, M., & Sharifian, R. (2019). Comment on: DMMS: A Decentralized Blockchain Ledger for the Management of Medication Histories. *Blockchain in Healthcare Today*, 1–15. https://doi.org/10.30953/bhty.v2.98

APPENDICES

APPENDIX A

PROCESS
REFERENCE
MODEL

BLOCKCHAIN DAPP PROCESS REFERENCE MODEL (BDRM)

Merve Vildan Baysal[1, 2], Özden Özcan-Top[1], Aysu Betin Can[1]

[1]Dept. of Information Systems, Grad. Sch. of Informatics, Middle East Technical University
[2]The Scientific and Technological Research Council of Türkiye

Version
2023-03

Table of Contents

(*) This content is available at METU/II-TR-2024-249 (Baysal, 2024)

A. INTRODUCTION

Blockchain technology has garnered significant attention in a variety of domains in recent years. Despite the enormous potential for using blockchain technology, there are a number of risks and challenges that may occur in technological and domain-specific situations. These challenges needs to be recognized and resolved. Blockchain decentralized applications (dApps) cannot be developed without the establishment of decentralized systems that allow multiple parties to access and validate the data. However, this presents its own set of challenges, such as ensuring interoperability across different blockchain platforms and testing decentralized systems. In safety-critical systems, the problem of identifying responsible authority also becomes a significant challenge. In safety critical domains, any failure or malfunction of a system or technology could potentially result in significant harm, injury, or damage to the environment. Therefore, ensuring the safety, reliability, and correctness of operations within these domains is crucial and often subject to stringent regulations, standards, and rigorous testing procedures. Blockchain systems may be exploited or subject to security breaches due to smart contract vulnerabilities, which are weaknesses or flaws in the code of smart contracts. It is important to adhere to the best practices for smart contract development and verification in order to mitigate such risks. Moreover, when transaction volumes rise, scalability and performance issues could appear, which reduce the effectiveness and responsiveness of the system.

Optimizing the system architecture, choosing appropriate consensus mechanisms, and implementing solutions like sharding could help to address these issues. Additionally, in order to ensure the privacy, security, and integrity of sensitive data, blockchain applications may be subject to specific regulations.

A process reference model that is consistent with the relevant domain standards would offer valuable guidance to address these difficulties and risks that could arise during the development process, as well as assisting to achieve regulatory compliance. The Blockchain DApp Process Reference Model (BDRM) document offers valuable guidance for development organizations or individuals involved in blockchain dApp development in safety critical domains.

This document proposes a generic BDRM encompassing blockchain dApp development processes. It also provides insights into tailoring this framework specifically for health, energy, and automotive domains by incorporating domain-specific information in E, F, and G parts of the document for ensuring compliance with related regulations in these domains.

B. NORMATIVE REFERENCES

The following referenced documents are recommended for the application of this document.

Health Domain:

- IEC 62304 Medical device software – Software life cycle processes for the health domain (IEC 62304, 2006)
- IEC 82304-1:2016 Health software - General requirements for product safety (IEC 82304, 2016)
- ISO 14971:2019 Medical devices – Application of risk management to medical devices (ISO 14971, 2019)

Automotive Domain:

- Automotive SPICE Process Reference Model version 4.0 (VDA QMC Working Group, 2023)
- ISO 26262-2:2018 Road vehicles - Functional safety – Management of Functional Safety (ISO 26262-2, 2018)
- ISO 26262-6:2018 Road vehicles - Functional safety – Product development at the software level (ISO 26262-6, 2018)
- ISO 26262-7:2018 Road vehicles - Functional safety – Production, operation, service and decommissioning (ISO 26262-7, 2018)
- ISO 26262-9:2018 Road vehicles - Functional safety –Automotive safety integrity level (ASIL)-oriented and safety-oriented analyses (ISO 26262-9, 2018)

Energy Domain:

- IEC 61508-2:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Requirements for electrical/electronic/programmable electronic safety-related systems. (IEC 61508-2, 2010)
- IEC 61508-3:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Software requirements (IEC 61508-3, 2010)
- IEC 61508-5:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Examples of methods for the determination of safety integrity levels (IEC 61508-5, 2010)
- IEC 61508-6:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Guidelines on the application of IEC 61508-2 and IEC 61508-3 (IEC 61508-6, 2010)

General:

- ISO/IEC 25030:2019 Software Engineering — Software product quality requirements and evaluation (SQuaRE) - Quality requirements framework (ISO/IEC, 2019)

C. DEFINITIONS

- **APIs**: External API's retrieve data or perform other tasks that are not directly related to the blockchain.
- **Backend:** Backend is responsible for the technical infrastructure that makes blockchain work. Backend is the blockchain system which includes node software, consensus mechanism, smart contracts, data storage component that stores all the transactions and blocks.
- **Blocks:** The records that comprise blockchain networks.
- **Consensus mechanism:** They guarantee the trustworthiness and authenticity of blocks without the need for a central authority, enabling agreement between untrusted parties. Through consensus models, users of the network agree that a transaction is valid (Yaga et al., 2018).
- **Decentralized application (dApp):** is a type of distributed open source software application that runs on a blockchain or peer-to-peer networks (TechTarget, 2022).
- **Frontend:** Frontend is responsible for providing a user-friendly and intuitive interface that allows users to interact with the blockchain. Consists of user interface, data visualization components that display the blockchain data, transaction management component that allows users to create, sign, and broadcast transactions on the blockchain, a wallet component that allows users to manage their funds.
- **On-chain storage**: The data is stored on the blockchain network
- **Off chain storage**: The data is stored in an external storage and its hash in the blockchain
- **Permissionless blockchain networks**: They are decentralized ledger platforms where anyone can publish blocks.
- **Permissioned blockchain networks**: This networks only allow a selected group of users to publish blocks. Blocks of data in permissioned blockchain networks need to be approved by authorized network nodes.
- **Smart Contracts/Chaincodes**: is a piece of code on the blockchain network that emerges to minimize the need for trusted intermediaries. If a series of pre-defined conditions are fulfilled, a smart contract executes itself, and the execution results are recorded in the blockchain (Yaga et al., 2018).
- **Stakeholder**: According to the PMBOK Guide, "A stakeholder is an individual, group, or organization who may affect, be affected by or perceive itself to be affected by a decision, activity, or outcome of a project" (Usmani, 2022). It include customers, users, project team members, project sponsors, etc.
- **Reference Architecture**: A model that can support system development by addressing all applicable business principles, architectural styles, best practices for software development, and software components (Nakagawa et al., 2011).
- **Tokenomics**: It is a term formed by pairing up the two words "token" and "economics". It explains the factors that affect a token's value and use, including when it is created and distributed, incentive mechanisms, supply and demand, and token burn schedules.

D. KEY CONCEPTS

Blockchain System Components

Blockchain consists of blocks, nodes, transactions, smart contracts, and consensus models. They use mining, public/private key cryptography, and hashing functions.

- Blocks are the data structures in a blockchain that permanently record valid transactions.
- Cryptographic Hashing is a method employed to transform data of any size into a string of a fixed length. Each block within a blockchain has a unique hash. Blocks include the hash value of the preceding block, so forming a chain structure. Manipulating data within a block would result in an alteration of its hash value, so breaking the link with the subsequent blocks. Hashing is essential for ensuring data integrity in blockchain networks.
- Transaction is the recording of an event, like the creation of new assets or the transfer of assets between parties. The source and destination addresses, the amount of assets being transferred, and other data (such as transaction fees) are all included in each transaction.
- Nodes are the computers/servers that participate in storing and validating transactions in a blockchain network. They also collaborate to ensure a blockchain's stability, security, and accuracy by confirming new transactions and blocks and engaging in consensus mechanisms.
- Consensus mechanism is a method for reaching an agreement within a blockchain system. They create a shared understanding across nodes about the current state of the network.
- Mining involves solving complex puzzles within a Proof of Work (PoW) consensus mechanism to add new blocks to the blockchain.
- A smart contract is a piece of code and associated data that is implemented on a blockchain network through transactions that are cryptographically signed. Smart contracts are automatically executed at the nodes after a set of predetermined conditions are fulfilled.
- Public-private key cryptography, often known as asymmetric cryptography, is employed to ensure the security of communication and the verification of parties involved. Public keys are utilized to encrypt messages, while private keys are employed to decrypt them. Private keys are employed in blockchain networks to authenticate transactions and validate ownership of assets.

Blockchain networks can be characterized as *permissionless, permissioned*, or both. Permissionless blockchain networks are decentralized platforms that allow anyone to publish blocks on the ledger. A network that restricts block publishing to a particular set of users is referred to as a permissioned network. Below are the most common types of blockchain:

- Public blockchains enable individuals to actively participate in the network by submitting transactions and assuming the role of a validator. These blockchains are usually decentralized, meaning that there is no central authority that governs the network.

- Private Blockchains are limited to a defined set of participants, such as a company or a consortium of businesses. Participation in the private network is limited to the nodes that have been specifically chosen. Consortium Blockchains are a combination of public and private blockchains, where a network is formed by a collective of organizations who have joint control and governance.

- Consortium blockchains are commonly employed in situations when numerous entities require cooperation and the exchange of data.
- Hybrid blockchains include features from both public and private blockchains, enabling the advantages of public blockchains like decentralization and transparency, while preserving the privacy and control offered by private blockchains.

Process Concepts

BDRM was developed based on the meta-model of the ISO/IEC 12207 Software Life Cycle Processes standard (ISO/IEC/IEEE 12207, 2017). The BDRM includes processes and base practices:

- The model's processes provide a comprehensive framework for effectively managing the entire software life cycle, from acquisition to maintenance, and ensuring the delivery of software systems of high-quality.
- The base principles included in the processes focus on actions aimed at developing dApp products that meet to the requirements of consumers and end-users.

The format for defining each process is as follows.

Process ID	Each process has a unique ID.
Process Name	Each process has a name.
Purpose of the Process	The purpose outlines the goals of executing the process.
Outcomes	The outcomes refer to the observable results that are expected to be achieved via the successful implementation of the process.
Base Practices and Special Notes	Each practice is defined with a unique ID. The practices are sets of cohesive tasks of a process. The model integrates the requirements of the ISO/IEC 12207 alongside health-focused standards (i.e. IEC 62304, IEC 82304, ISO 14971) automotive-specific standards (i.e. ASPICE, ISO 26262), and energy domain-related standards (i.e IEC 61508). Information specific to blockchain development are highlighted in blue in the BDRM. The notes are recommendations to support the achievement of blockchain dApp outcomes, and to ensure Safety Classification (given in brackets, [Class A, B, C] for health domain, [ASIL A, B, C, D] for automotive domain, [SIL 1, 2, 3, 4] for energy domain if applicable) The model includes specific information related to the health, energy, and automotive domains as additional documents. Information related to

	the health, automotive, and energy domains are highlighted in gray, orange, and green respectively.
Inputs and Outputs	There are inputs necessary to execute each process and outputs generated as a result of conducting the process activities.

The processes and base practices of the BDRM are given in Table 1. The first-level headings in the model in this table are processes, while the second-level headings are base practices. In total, the model covers 15 processes and 68 base practices. In Table 1, practices that include information that is specific to blockchain development is highlighted in blue, and practices that are related to the safety-critical domain are indicated in purple.

Tablo 1: The BDRM processes and practices

Processes	**Base Practices**
1. Blockchain dApp project initiation process	1.1 Identify objectives and key performance indicators 1.2 Evaluate blockchain suitability 1.3 Evaluate the feasibility of the blockchain dApp project
2. Blockchain dApp planning	2.1 Create blockchain dApp project scope, schedule, budget, and resources management plans 2.2 Create a communication plan 2.3 Create a change management plan 2.4 Decide on the blockchain development life cycle model 2.5 Decide on the safety class of the product 2.6 Decide on the need for using digital assets
3. Blockchain dApp monitoring and control	3.1 Monitor the blockchain dApp project against the plan 3.2 Control the blockchain dApp project 3.3 Manage corrective actions to closure
4. Blockchain dApp requirements elicitation	4.1 Identify stakeholders 4.2 Elicit stakeholder requirements 4.3 Review stakeholder requirements 4.4 Agree on requirements 4.5 Manage changes made in the stakeholder requirements
5. Blockchain dApp requirements analysis	5.1 Specify blockchain dApp system requirements 5.2 Identify the consensus mechanism 5.3 Include tokenomics in blockchain dApps including digital tokens 5.4 Specify blockchain dApp software requirements 5.5 Specify blockchain dApp security requirements 5.6 Specify blockchain dApp privacy requirements 5.7 Specify blockchain dApp safety requirements 5.8 Validate the requirements, and update when necessary 5.9 Develop approval criteria for testing
6. Blockchain dApp risk management	6.1 Identify the software that could contribute to a hazardous situation and potential causes 6.2 Define risks to the blockchain dApp product 6.3 Apply risk mitigation plan and risk contingency plan 6.4 Analyze the process and product risks

	6.5 Resolve the process and product risks 6.6 Manage the process and product risks that may be raised by changes
7. Blockchain dApp architectural design	7.1 Define and describe the blockchain dApp architecture 7.2 Decide on blockchain network type 7.3 Decide on framework 7.4 Decide on storage method 7.5 Decide where to deploy the modules of the system 7.6 Decide on incentives if there is a need for digital assets 7.7 Ensure the security of the system 7.8 Apply anonymity mechanism if needed 7.9 Verify the architecture
8. Blockchain dApp detailed design	8.1 Prepare for detailed design 8.2 Design the backend 8.3 Design the frontend
9. Blockchain dApp implementation	9.1 Develop unit verification procedures 9.2 Build APIs 9.3 Develop the backend 9.4 Develop the frontend, user interface
10. Blockchain dApp integration	10.1 Integrate the backend and frontend units 10.2 Verify and test the integration
11. Blockchain dApp verification	11.1 Prepare for verification 11.2 Verify the blockchain dApp product 11.3 Manage verification results
12. Blockchain dApp validation	12.1 Prepare for validation 12.2 Validate the blockchain dApp product 12.3 Manage validation results
13. Blockchain dApp quality assurance	13.1 Specify blockchain dApp product quality requirements 13.2 Assure blockchain dApp product quality
14. Blockchain dApp transition	14.1 Develop a transition strategy 14.2 Confirm the blockchain dApp product is ready 14.3 Deploy the blockchain dApp product on the test network 14.4 Deploy the blockchain dApp product on the main network 14.5 Make the blockchain dApp product available to the users 14.6 Manage results of transition
15. Blockchain dApp maintenance	15.1 Develop a maintenance plan 15.2 Analyze, assess, and accept or reject change requests 15.3 Implement, test, and deploy modifications 15.4 Retire the blockchain dApp product

E. PROCESSES

ID of the Process	1
Process Name	Blockchain dApp project initiation process
Purpose of the Process	The purpose is to identify objectives, to define the project at a high level in order to demonstrate its business value and evaluate the blockchain suitability.
Outcomes	As a result of successful implementation of Blockchain dApp project initiation process: a) objectives of the blockchain dApp development project are identified b) key performance indicators (KPIs) are identified c) blockchain suitability is evaluated for the specified problem d) the feasibility of the blockchain dApp project is evaluated
Base Practices and Special Notes	**1.1 Identify objectives and key performance indicators.** Identify the main goals of the blockchain dApp development project. Define the key performance indicators (KPIs) that will be used to assess the blockchain dApp's success and effectiveness [Class A, B, C][ASIL A, B, C, D][SIL 1, 2, 3, 4]. NOTE: The metrics may include transaction throughput, response time, system uptime, number of active users, gas fees, or any other relevant performance indicators specific to the dApp. **1.2. Evaluate blockchain suitability**. Determine whether blockchain is applicable to the specified domain and capable of solving the specified problem [Class A, B, C][ASIL A, B, C, D][SIL 1, 2, 3, 4]. NOTE: When determining eligibility, we recommend leveraging the findings of supporting studies. (Yaga et al., 2018; Wust & Gervais, 2018). Which type of blockchain might be appropriate is also identified in (Wust & Gervais, 2018). **1.3 Evaluate the feasibility of the blockchain dApp project**. Assess the feasibility of achieving project objectives with the current resources and constraints [Class A, B, C][ASIL A, B, C, D][SIL 1, 2, 3, 4]. NOTE: Perform a detailed financial analysis to determine the project's financial viability. This includes calculating costs, forecasting income, and determining profitability. Estimated costs range between developing a blockchain system from scratch and utilizing existing platforms. Some

	platforms charge transaction and execution fees, while others charge procurement fees. If creation of a new blockchain is to be preferred: ● This option is the most costly option. Depending on the needs of a given project, such as the number and complexity of features that must be incorporated into the product the overall cost of developing a blockchain will vary. It is recommended to make a cost estimation of developers (Core Blockchain Developers and Blockchain Software Developers) or outsource the blockchain Project to offshore software companies in order to reduce development cost. Depending on particular business needs, creating a blockchain system from scratch, testing it, and deploying it could take months or even longer. Based on the time, the total cost might be approximated. As handling user data is required for a blockchain solution, the cost of data management should be assessed. Other costs such as legal expenses, and maintenance should be considered (TP&P Technology, 2020). Generally, this option could be preferred if the system being developed has its own digital asset. If a blockchain with gas fee is to be preferred: ● It is recommended to make a transaction and execution cost estimate. Gas is the way in which computing resources (CPU, storage) are priced in some of the blockhain platforms. Tools (ETH Gas Station, Blocknative, Gwei Gas Calculator, AWT Gas Calculator, SnowTrace, etc) could be used for gas fee estimation (REES, 2022). The cost of sending data to the blockchain determines transaction costs. Execution costs are determined by the cost of computing processes performed as a result of the transaction (StackExchange, 2022). As an example about fee schedule, Appendix G of Ethereum's Yellow Paper could be reviewed (Wood, 2022). If enterprise blockchains is to be preferred: ● There is no need to make an estimation of transaction and execution costs. There is no notion of gas. ● "Blockchain as a Service" (BaaS) accounts should be purchased. For example IBM Blockchain platform; Hyperledger Fabric on SAP cloud platform; Hyperledger Fabric on Azure from Microsoft; Hyperledger Fabric (HVM) from AWS; Corda on AWS (Davies, 2022) It is recommended to make a procurement estimate. Proof of Concept (POC) could be used to validate and demonstrate the feasibility of a proposal. A proof of concept is a theoretical demonstration of the production and use of an idea. It enables the testing

	of a DApp with minimal resources before investing significant time and money to the development process.

Inputs	**Outputs**
Stakeholder expectations, business requirements [Practice 1.1].	Clearly articulated and well-defined objectives for the blockchain dApp development project [Practice 1.1].
	Defined KPIs for measuring success [Practice 1.1]
Problem statement, domain information, supportive studies [Practice 1.2].	The evaluation of blockchain suitability for the specified problem [Practice 1.2].
Project goals, available resources, constraints financial analysis data [Practice 1.3].	The evaluation of the feasibility of the blockchain dApp project, considering available resources and constraints, and the decision on which type of blockchain approach is preferred [Practice 1.3].
	If a POC was conducted, the results and findings from the POC [Practice 1.3].

Only informative sections of BDRM and one example process are presented in this thesis study. The rest of the BDRM including full content is reserved as a technical report: METU/II-TR-2024-249 (Baysal, 2024)

The rest of BDRM includes the following processes and related base practices:

2. Blockchain dApp planning - The purpose is to create and coordinate effective plans to carry out development process activities in accordance with the scope, magnitude, and safety classifications of the system to be developed.

3. Blockchain dApp monitoring and control. The purpose is to determine the status of the project, monitor and control project activities throughout the application’s life to ensure that the progress is according to plans and schedules.

4. Blockchain dApp requirements elicitation. The purpose is to gather, process, and monitor changing needs and requirements throughout the application’s life.

5. Blockchain dApp requirements analysis. The purpose is to transform the defined stakeholder requirements into technical requirements that will guide the design of the system.

6. Blockchain dApp risk management. The purpose is to identify, analyze, and treat the risks continuously.

7. Blockchain dApp architectural design. The purpose is to convert the set of requirements into a written architecture that outlines the structure and determine which system requirements should be assigned to which system components.

8. Blockchain dApp detailed design. The purpose is to provide a design that implements and can be verified against the requirements.

9. Blockchain dApp implementation. The purpose of the Blockchain dApp implementation process is to produce executable software units that properly reflect the design.

10. Blockchain dApp integration. The purpose is to combine the software units to integrated software items that are compatible with the software design.

11. Blockchain dApp verification. The purpose is to confirm that the dApp meets its defined requirements.

12. Blockchain dApp validation. The purpose is to validate the dApp to acquire confidence that it can accomplish its intended objective or use under specific operational conditions.

13. Blockchain dApp quality assurance. The purpose ist o achieve stakeholder satisfaction by monitoring the quality of the dApp product to ensure it satisfies stakeholder requirements.

14. Blockchain dApp transition. The purpose is to move the blockchain dApp product into the operational status.

15. Blockchain dApp maintenance. The purpose ist o change, modify, and update software to keep up with stakeholder needs, to correct faults and to improve performance.

APPENDIX B

QUESTIONS TO BE ASKED KEY STAKEHOLDERS WITHIN THE ORGANIZATIONS

Questions for Process 1 - Blockchain dApp project initiation process

Intended interview participant: Project Managers

Base Practices	Questions
1.1 Identify objectives and key performance indicators	Eng: How long does the project initiation process typically take? Tr: Proje başlatma süreci genellikle ne kadar sürer? Eng: What are the primary objectives of your blockchain dApp development project? Tr: Blokzincir dApp geliştirme projenizin temel amaçları nelerdir?
1.2. Evaluate blockchain suitability	Eng: How do you determine if blockchain is a suitable technology for the specified problem? Tr: Blokzincirin belirli bir problem için uygun bir teknoloji olup olmadığını nasıl belirlersiniz? Eng: Have you used any supportive studies to determine blockchain suitability? Tr: Blockzincirin uygunluğunu belirlemek için herhangi bir çalışmadan yararlandınız mı?
1.3 Evaluate the feasibility of the blockchain dApp project	Eng: Can you provide insights into the financial analysis conducted to assess the project’s financial feasibility? Tr: Projeye yönelik finansal uygulanabilirliği değerlendirmek için yapılan mali analizlere dair bilgi verebilir misiniz? Eng: What factors do you consider when selecting a specific blockchain platform?

	Tr: Blokzincir platformu seçerken hangi faktörleri göz önünde bulunduruyorsunuz?
	Eng: How do you estimate the gas fees for the blockchain transactions and executions?
	Tr: Blokzincir işlemlerinde gaz ücretlerini nasıl öngörüyorsunuz?
	Eng: Do you use any specific tools or references for gas fee estimation? (if applicable)
	Tr: Gaz ücreti tahmini için belirli araçlar veya referanslar kullanıyor musunuz? (şayet uygulanıyorsa)
	Eng: Do you consider using “Blockchain as a Service” (BaaS) accounts for the project?
	Tr: Proje için “Blockchain as a Service” (BaaS) hesaplarını kullanmayı düşünüyor musunuz?
	Eng: Have you conducted a Proof of Concept (POC) to validate the feasibility of the blockchain dApp?
	Tr: Blokzincir dApp’in uygulanabilirliğini doğrulamak için kavram kanıtı (POC) gerçekleştirdiniz mi?

Questions for Process 2 - Blockchain dApp planning

Intended interview participant: Project Managers

Base Practices	Questions
2.1 Create blockchain dApp scope, schedule, budget, and resources management plans	Eng: How are roles, responsibilities, and authorities defined within your team for a specific project?
	Tr: Projede, takımınız içinde roller, sorumluluklar ve yetkiler belirlenirken nasıl bir yaklaşım izlersiniz?
	Eng: How do you create blockchain dApp scope, schedule, budget, and resources management plans for a new project?

	Tr: Yeni bir blokzincir dapp projesi için kapsam, zaman çizelgesi, bütçe ve kaynak yönetimi planını nasıl oluşturursunuz? Eng: How do you assess the experience, knowledge, and skills required for a project, and how do you select individuals and teams accordingly? Tr: Projede gereken deneyim, bilgi ve becerileri nasıl değerlendiriyorsunuz ve bireyleri ve ekipleri nasıl seçiyorsunuz?
2.2 Create communication plan	Eng: How do you ensure clear communication among all project participants, and what elements are included in your communication plan? Tr: Ekip üyeleri arasında verimli iletişimi nasıl sağlıyorsunuz ve iletişim planınızda hangi unsurlar yer alıyor?
2.3 Create change management plan	Eng: How your company creates and coordinates effective change management plan? Tr: Şirketiniz etkili bir değişim yönetimi planını nasıl oluşturur ve koordine eder? Eng: How do you handle change requests, approvals, and their impact on the project's schedule, budget, and resources? Tr: Değişiklik taleplerini, onayları ve bunların projenin zaman çizelgesi, bütçesi ve kaynakları üzerindeki etkilerini nasıl yönetiyorsunuz?
2.4 Decide on a blockchain development life cycle model	Eng: How do you decide on the appropriate blockchain development life cycle model for project? Which methodologies you follow in safety critical domain? Tr: Proje için hangi blokzincir geliştirme yaşam döngüsü modelinin uygun olduğuna nasıl karar veriyorsunuz? Güvenlik kritik alanlarda hangi metodolojileri uyguluyorsunuz?
2.5 Decide on safety class of the product	Eng: Can you elaborate on your process of classifying safety classification based on the relevant safety critical domain standard for each project?

	Tr: Projelerinizde güvenlik kritik alan standardına dayalı olarak güvenlik sınıflandırmasını sınıflandırma sürecinizi açabilir misiniz?
2.6 Decide on the need for using digital assets	Eng: How do you determine the need for using digital assets in a blockchain dApp, and what factors influence the decision between utility and security tokens? (if applicable) Tr: Blokzincir dApp projesinde dijital varlık kullanımının gerekliliğini nasıl belirliyorsunuz, karar üzerinde etkili olan faktörler nelerdir? (şayet uygulanıyorsa)

Questions for Process 3 - Blockchain dApp monitoring and control

Intended interview participant: Project Managers

Base Practices	Questions
3.1 Monitor the blockchain dApp project against the plan	Eng: How do you monitor and control project activities to ensure that they are progressing according to plans and schedules? Tr: Projedeki faaliyetleri nasıl izliyor ve kontrol ediyor ve zaman çizelgelerine göre ilerlediğinden emin oluyorsunuz? Eng: How do you manage project risks and ensure data management during the monitoring phase? Tr: Proje risklerini nasıl yönetiyor ve izleme aşamasında veri yönetimini nasıl sağlıyorsunuz? Eng: Can you describe the process of conducting progress reviews and milestone reviews for a Blockchain dApp project? Tr: Bir Blokzincir dApp projesi için ilerleme incelemeleri ve kilometre taşı incelemeleri yürütme sürecini açıklayabilir misiniz?
3.2 Control the blockchain dApp project	Eng: What methods do you use to analyze and resolve issues that arise during the development of a Blockchain dApp? Tr: Blokzincir dApp geliştirme sırasında ortaya çıkan sorunları analiz etmek ve çözmek için hangi yöntemleri kullanıyorsunuz?

	Eng: How do you handle contractual changes in cost, time, or quality due to stakeholder requests during project execution? Tr: Proje yürütme sırasında paydaş talepleri nedeniyle maliyet, zaman veya kalite konusundaki sözleşmesel değişiklikleri nasıl ele alıyorsunuz?
3.3 Manage corrective actions to closure	Eng: Can you describe a situation where project replanning was necessary, and how it was executed to ensure project success? Tr: Projenin yeniden planlanmasının gerekli olduğu bir durumu ve proje başarısını garantilemek için bunun nasıl yürütüldüğünü açıklayabilir misiniz?

Questions for Process 4 - Blockchain dApp requirements elicitation

Intended interview participant: Business Analysts or Requirements Elicitation Team Members

Base Practices	Questions
4.1 Identify stakeholders	Eng: How do you perform requirements elicitation process? Tr: Gereksinim ortaya çıkarma sürecini nasıl gerçekleştiriyorsunuz? Eng: Can you explain the process you follow to identify stakeholders who may have an interest or influence in the dApp project? Tr: dApp projesine ilgisi veya etkisi olabilecek paydaşları belirlemek için izlediğiniz süreci açıklayabilir misiniz?
4.2 Elicit stakeholder requirements	Eng: How do you establish communication with the identified stakeholders to ensure effective requirements elicitation?

	Tr: Gereksinimlerin etkili bir şekilde ortaya çıkarılmasını sağlamak için belirlenen paydaşlarla iletişimi nasıl kuruyorsunuz? Eng: How do you elicit stakeholder needs and transform them into requirements for a Blockchain dApp project? Tr: Paydaşların ihtiyaçlarını nasıl ortaya çıkarır ve bunları bir blokzincir dApp projesi için gereksinimlere nasıl dönüştürürsünüz? Eng: Are the requirements defined considering the safety classifications? Tr: Gereksinimler güvenlik sınıfları dikkate alınarak mı tanımlanıyor? Eng: How do you handle community discussions to collect requirements? How do you ensure that the requirements gathered from community discussions are aligned with the overall project objectives? (if applicable) Tr: Gereksinimleri toplamak için topluluk tartışmaları yapıyor musunuz? Topluluk tartışmalarından elde edilen gereksinimlerin genel proje hedefleriyle uyumlu olmasını nasıl sağlıyorsunuz? (şayet uygulanıyorsa)
4.3 Review stakeholder requirements	Eng: How do you maintain traceability between stakeholder needs and the defined requirements? Tr: Paydaş ihtiyaçları ile tanımlanan gereksinimler arasındaki izlenebilirliği nasıl sağlıyorsunuz? Eng: Could you provide examples of how you review stakeholder requirements and requests to better understand their needs and expectations? Tr: Paydaşların ihtiyaçlarını ve beklentilerini daha iyi anlamak için onların gereksinimlerini ve isteklerini nasıl incelediğinize dair örnekler verebilir misiniz?
4.4 Agree on requirements	Eng: How do you ensure agreement across teams on the stakeholder requirements for a dApp project?

	Tr: Bir dApp projesi için paydaş gereksinimleri konusunda ekipler arasında anlaşmayı nasıl sağlarsınız?
4.5 Manage changes made in the stakeholder requirements	Eng: Can you explain your approach to managing changes made in stakeholder requirements throughout the project? Tr: Proje boyunca paydaş gereksinimlerinde yapılan değişiklikleri yönetme yaklaşımınızı açıklayabilir misiniz? Eng: What query mechanisms do you provide to stakeholders to keep them aware of the status and disposition of their requirements changes? Tr: Paydaşlara, gereksinimlerindeki değişikliklerin durumu ve düzeni hakkında bilgi sahibi olmalarını sağlamak için hangi sorgulama mekanizmalarını sağlıyorsunuz?

Questions for Process 5 - Blockchain dApp requirements analysis

Intended interview participant: Business Analysts or Requirements Analysis Team Members

Base Practices	Questions
5.1 Specify blockchain dApp system requirements	Eng: How do you perform requirements analysis process? Tr: İhtiyaç analizi sürecini nasıl gerçekleştiriyorsunuz? Eng: Can you explain the process of specifying system requirements, considering factors like consensus mechanism, cost, scalability, developer requirements, and expected timeline? Tr: Uzlaşma mekanizması, maliyet, ölçeklenebilirlik, geliştirici gereksinimleri ve beklenen zaman çizelgesi gibi faktörleri göz önünde bulundurarak sistem gereksinimlerini belirleme sürecini açıklayabilir misiniz?

5.2 Identify a consensus mechanism	Eng: How do you choose the most suitable consensus mechanism for a Blockchain dApp project? Tr: Blokzincir dApp projesi için en uygun uzlaşma mekanizmasını nasıl seçersiniz? Eng: Do you consider green computing and energy efficiency while selecting a consensus mechanism? Tr: Uzlaşma mekanizması seçerken yeşil bilişim ve enerji verimliliğini göz önünde bulunduruyor musunuz?
5.3 Include tokenomics in blockchain dApps including digital tokens	Eng: Do you include tokenomics in Blockchain dApps and utilize digital tokens to reward and incentivize network participants, customers, and stakeholders? Can you explain the process of investigating tokenomics and its implementation in your Blockchain dApp projects? (if applicable) Tr: Blokzincir dApp'lerine token ekonomisi ekliyor musunuz ve ağ katılımcılarını, müşterilerini ve paydaşlarını ödüllendirmek ve teşvik etmek için dijital tokenleri kullanıyor musunuz? Token ekonomisi araştırma sürecini ve bunun Blokzincir dApp projelerinizde uygulanmasını açıklayabilir misiniz?
5.4 Specify blockchain dApp software requirements	Eng: How do you specify software requirements for Blockchain dApps, considering actors, user stories? Could smart contracts or chaincodes be specified to regulate data access rights and permission policies? Tr: Blockchain DApp'ler için yazılım gereksinimlerini belirlerken, aktörleri ve kullanıcı hikayelerini nasıl dikkate alırsınız? Veri erişim haklarını ve izin politikalarını düzenlemek için akıllı sözleşmeler veya zincir kodları kullanılabilir mi?
5.5 Specify blockchain dApp security requirements	Eng: How do you define security requirements to ensure data confidentiality, authorization, authentication, audit trail, system security, communication integrity, and anonymity in your Blockchain dApp projects? Tr: Blokzincir dApp projelerinizde veri gizliliğini, yetkilendirmeyi, kimlik doğrulamayı, denetim takibini, sistem güvenliğini, iletişim bütünlüğünü

	ve anonimliği sağlamak için güvenlik gereksinimlerini nasıl tanımlarsınız? Eng: Do you take into account the principles of information security (confidentiality, integrity, non-repudiation, accountability, and authenticity) while defining security requirements? Tr: Güvenlik gereksinimlerini tanımlarken bilgi güvenliği ilkelerini (gizlilik, bütünlük, inkar edilemezlik, hesap verebilirlik ve özgünlük) göz önünde bulunduruyor musunuz?
5.6 Specify blockchain dApp privacy requirements	Eng: How do you define privacy requirements for Blockchain dApps, considering the sensitivity of information, privacy laws, policies, and regulations? Tr: Bilginin hassasiyeti, gizlilik yasaları, politikaları ve düzenlemelerini göz önünde bulundurarak Blokzincir dApp'leri için gizlilik gereksinimlerini nasıl tanımlarsınız? Eng: Can you provide examples of how you have ensured data privacy in previous Blockchain dApp projects? Tr: Blokzincir dApp projelerinde veri gizliliğini nasıl sağladığınıza ilişkin örnekler verebilir misiniz?
5.7 Specify blockchain dApp safety requirements	Eng: How do you define safety requirements for Blockchain dApps? Tr: Blokzincir dApp'leri için güvenlik gereksinimlerini nasıl tanımlarsınız?
5.8 Validate the requirements and update when necessary	Eng: How do you validate the requirements to ensure their validity, consistency, completeness, realism, and verifiability? Are the requirements updated considering the safety classification? Tr: Gereksinimleri geçerlilik, tutarlılık, eksiksizlik, gerçekçilik ve doğrulanabilirlik açısından doğrulamak için nasıl bir yaklaşım izliyorsunuz? Gereksinimler güvenlik sınıfları dikkate akınarak mı güncelleniyor? Eng: How do you maintain traceability between the system and software requirements and the stakeholder requirements?

	Tr: Sistem ve yazılım gereksinimleri ile paydaş gereksinimleri arasında izlenebilirliği nasıl sağlıyorsunuz?
5.9 Develop approval criteria for testing	Eng: How do you handle changes and new requirements during the validation phase, and how do you update the requirements baseline accordingly? Tr: Doğrulama aşamasında ortaya çıkan değişiklikleri ve yeni gereksinimleri nasıl yönetiyorsunuz ve buna göre gereksinimleri nasıl güncelliyorsunuz? Eng: Can you explain how you define the approval criteria for dApp product tests using the specified requirements? Tr: Belirlenen gereksinimleri kullanarak dApp ürünü testlerinin onay kriterlerini nasıl tanımladığınızı açıklayabilir misiniz?

Questions for Process 6 - Blockchain dApp risk management

Intended interview participant: Risk Managers or Project Managers

Base Practices	Questions
6.1 Identify software that could contribute to a hazardous situation and potential causes	Eng: How do you perform risk management process? Tr: Risk yönetimi sürecini nasıl gerçekleştiriyorsunuz? Eng: How do you define and record risk control measures in compliance with relevant standards for your Blockchain dApp projects? Tr: Blokzincir dApp projeleriniz için ilgili standartlar ile uyumlu şekilde risk kontrol önlemlerini nasıl tanımlar ve kaydını tutarsınız? Eng: Can you explain how the company documents potential causes of hazardous situations in the safety critical dApp product, considering both direct software failures and failures of risk control measures? Tr: Hem doğrudan yazılım arızalarını hem de risk kontrol önlemlerindeki başarısızlıkları göz

	önünde bulundurarak şirketin güvenlik kritik dApp ürünündeki tehlikeli durumların potansiyel nedenlerini nasıl dokümante ettiğini açıklayabilir misiniz?
6.2 Define risks to the blockchain dApp product	Eng: Do you take into account blockchain-specific risk items like lack of standards, energy requirements, lack of centralized authority, legal and regulatory framework risks, malicious users and risk of aquiring 51% of hashing power, and risks related to smart contracts security and management and oracles (non-blockchain entities that provide data to the network potentially causing the execution of smart contracts on the network)? Tr: Standart eksikliği, enerji gereksinimleri, merkezi otorite eksikliği, yasal ve düzenleyici çerçeve riskleri, kötü niyetli kullanıcılar ve hash gücünün %51'ini ele geçirme gibi blokzincire özgü risk öğelerini ve ulak (ağa veri sağlayan, potansiyel olarak ağda akıllı sözleşmelerin yürütülmesine neden olan blokzincir dışı varlıklar) ve akıllı sözleşmelerin güvenliği ve yönetimiyle ilgili riskleri hesaba katıyor musunuz?
6.3 Apply risk mitigation plan and risk contingency	Eng: How does your company develop and apply a risk mitigation plan for identified risks in a Blockchain dApp project? Tr: Şirketiniz, bir blokzincir dApp projesinde tanımlanan riskler için nasıl bir risk azaltma planı geliştirir ve uygular?
6.4 Analyze the project and product risks	Eng: Can you explain the process of documenting potential causes and classifying risks based on their severity? Tr: Potansiyel nedenleri belgeleme ve riskleri şiddetlerine göre sınıflandırma sürecini açıklayabilir misiniz? Eng: How do you analyze project and product risks to determine their priority and allocate resources to monitor risks effectively? Tr: Projeyi ve ürünü etkileyebilecek riskleri analiz etme ve önceliklendirmek, riskleri etkili bir şekilde izlemek için kaynakları nasıl tahsis ettiğinizi açıklayabilir misiniz?

	Eng: Can you provide insights into how the company assesses risk control measures to identify the potential for generating new hazardous situations during the development dApps? Tr: Şirketiniz, dApp’lerin geliştirilmesi sırasında yeni tehlikeli durumlar oluşturma potansiyelini belirlemek için risk kontrol önlemlerini nasıl değerlendiriyor?
6.5 Resolve the project and product risks	Eng: How do you implement risk response plans in addressing identified risks and reducing their impact? Tr: Tanımlanan risklerle başa çıkmak ve etkilerini azaltmak için risk yanıt planlarını nasıl uygularsınız?
6.6 Manage the project and product risks that may be arised of changes	Eng: Can you explain the process of continuously reviewing and updating risk response plans as necessary? Tr: İhtiyaca bağlı olarak risk yanıt planlarını gözden geçirme ve güncelleme sürecini açıklayabilir misiniz? Eng: Do you consider if any new potential causes are being introduced that could lead to a hazardous situation? Tr: Herhangi yeni potansiyel nedenlerin ortaya çıkarak tehlikeli durumlara yol açabileceği göz önünde bulunduruluyor mu?

Questions for Process 7 - Blockchain dApp architectural design

Intended interview participant: Blockchain Architects or Technical Leads

Base Practices	Questions
7.1 Define and describe the blockchain dApp architecture	Eng: How do you perform architectural design process? Tr: Mimari tasarım sürecini nasıl gerçekleştiriyorsunuz?

	Eng: Do you ensure that the design adheres to the principles of privacy, security, data integrity, and availability? Tr: Tasarımın gizlilik, güvenlik, veri bütünlüğü ve erişilebilirlik ilkelerine uygun olmasını sağlıyor musunuz? Eng: Does your company describes the architecture considering the scalability, fault tolerance, cost-efficiency, performance and privacy requirements. Tr: Şirketiniz mimariyi ölçeklenebilirlik, hata toleransı, maliyet verimliliği, performans ve gizlilik gereksinimlerini dikkate alarak tanımlıyor mu? Eng: Does your company benefit from reference architectures? (if available) Tr: Şirketiniz referans mimarilerden faydalanıyor mu? (şayet uygulanıyorsa)
7.2 Decide on blockchain network type	Eng: How do you decide between public, consortium, or hybrid blockchain types and the permission status based on the properties of use case actors in a dApp project? Tr: Bir dApp projesinde açık, konsorsiyum veya hibrit blockchain türleri arasında nasıl karar veriyorsunuz ve izin durumu konusundaki kararları kullanım durumu aktörlerinin özelliklerine göre nasıl belirliyorsunuz? Eng: Can you provide examples of when permissioned blockchain networks with trusted nodes were preferred and how they contributed to performance in your projects? (if applicable) Tr: Güvenilir düğümlere sahip izinli blokzincir ağları tercih edildiği durumlarda nelerin göz önünde bulundurulduğunu ve bu tercihlerin projelerinizde performansa nasıl katkı sağladığını örneklerle açıklayabilir misiniz? (şayet uygulanıyorsa)
7.3 Decide platform use or network creation	Eng: How do you decide whether to use a dApp development platform or to create a new blockchain framework for your Blockchain dApp projects?

	Tr: dApp geliştirme platformu kullanma veya yeni bir blokzincir çerçevesi oluşturmaya neye göre karar veriyorsunuz?
	Eng: How do you determine the block size and target time span between blocks, and how do these choices impact the throughput and latency in your projects?
	Tr: Blok boyutunu ve bloklar arasındaki süreyi nasıl belirlersiniz ve bu seçimler projelerinizdeki verimi ve gecikmeyi nasıl etkiler?
	Eng: Can you explain how you ensure compliance with existing regulatory requirements in the health/energy/automotive domain when deciding blockchain frameworks?
	Tr: Blokzincir çerçevelerine karar verirken sağlık/enerji/otomotiv alanındaki mevcut düzenleyici gerekliliklere uyumu nasıl sağladığınızı açıklayabilir misiniz?
	Eng: Can you provide information about if the company has leveraged blockchain platforms like Hyperledger Fabric to ensure compliance with regulations such as HIPAA, GDPR, KVKK? (if applicable)
	Tr: Şirketin HIPAA, GDPR, KVKK gibi düzenlemelere uyumu sağlamak için Hyperledger Fabric gibi blockchain platformlarından yararlanıp yararlanmadığı hakkında bilgi verebilir misiniz? (şayet uygulanıyorsa)
7.4 Decide on storage method	Eng: How do you decide on the storage method (on-chain, off-chain, or hybrid) in a Blockchain dApp project?
	Tr: Blokzincir dApp projesinde depolama yöntemine (zincir içi, zincir dışı veya hibrit) nasıl karar verirsiniz?
	Eng: Can you provide examples of how you have addressed performance and scalability issues when dealing with huge safety critical domain data in your projects?
	Tr: Projelerinizde güvenlik kritik alandaki büyük hacimli verileriyle uğraşırken performans ve ölçeklenebilirlik sorunlarını nasıl ele aldığınıza dair örnekler verebilir misiniz?

7.5 Decide where to deploy the modules of the system	Eng: How do you decide where to deploy (cloud, IPFS, or blockchain-as-a-service model) the Blockchain dApp project? Tr: Blokzincir dApp projesini nereye dağıtacağınıza (bulut, IPFS veya hizmet olarak blockchain modeli) nasıl karar verirsiniz?
7.6 Decide on incentives if there is a need for digital asset	Eng: How do you decide on incentives such as rewards and transaction fees to encourage participants to cooperate and create value in a Blockchain dApp project? (if applicable) Tr: Katılımcıları Blokzincir dApp projesinde işbirliği yapmaya ve değer yaratmaya teşvik etmek için ödüller ve işlem ücretleri gibi teşviklere nasıl karar veriyorsunuz? (şayet uygulanıyorsa) Eng: Can you explain how you apply incentives (rewards and transaction fees to encourage participants to cooperate and create value) when there is a need for digital assets in the project? (if applicable) Tr: Projede dijital varlıklara ihtiyaç duyulduğunda teşvikleri (katılımcıları işbirliği yapmaya ve değer yaratmaya teşvik etmek için ödüller ve işlem ücretleri) nasıl uyguladığınızı açıklayabilir misiniz? (şayet uygulanıyorsa)
7.7 Ensure security of the system aligned with the requirements	Eng: How do you ensure security of the system aligned with the security requirements (e.g data integrity, confidentiality, secure connection, encription, zero trust policies)? Do you consider safety critical domain regulations? Tr: Sistemin güvenliğini, güvenlik gereksinimlerine (örn. veri bütünlüğü, gizlilik, güvenli bağlantı, şifreleme, sıfır güven politikaları) uygun olarak nasıl sağlıyorsunuz? Güvenlik kritik alan düzenlemelerini dikkate alıyor musunuz? Eng: Do you conduct a thorough threat modeling exercise to identify potential security threats and vulnerabilities in a Blockchain dApp project? Tr: Blokzincir dApp projesinde potansiyel güvenlik tehditlerini ve güvenlik açıklarını belirlemek için kapsamlı bir tehdit modelleme çalışması yapıyor musunuz?

7.8 Apply anonymity mechanism if needed	Eng: Can you provide examples of how you have implemented anonymity mechanisms to preserve anonymity in blockchain applications with sensitive safety critical data? (if applicable) Tr: Hassas verilerine sahip blokzincir uygulamalarında anonimliği korumak için anonimlik mekanizmalarını nasıl uyguladığınıza dair örnekler verebilir misiniz?
7.9 Verify the architecture	Eng: How do you verify that the architecture meets security, privacy, and quality requirements in your Blockchain dApp projects? Tr: Blockchain dApp projelerinizde mimarinin güvenlik, gizlilik ve kalite gereksinimlerini karşıladığını nasıl doğrularsınız? Eng: How do you maintain traceability of architecture elements to stakeholder and system/software requirements? Tr: Mimari öğelerin paydaşlara ve sistem/yazılım gereksinimlerine göre izlenebilirliğini nasıl sağlıyorsunuz?

Questions for Process 8 - Blockchain dApp detailed design

Intended interview participant: Software Designers

Base Practices	Questions
8.1 Prepare for the detailed design	Eng: How do you perform detailed design process? Tr: Detaylı tasarım sürecini nasıl gerçekleştiriyorsunuz? Eng: How does your company review the software requirements gathered during the requirements elicitation phase before moving into the detailed design phase? Tr: Detaylı tasarım aşamasına geçmeden önce, gereksinimlerin belirlenmesi sırasında şirketiniz yazılım gereksinimlerini nasıl inceliyor?

	Eng: Can you explain how you identify design components? Tr: Tasarım bileşenlerini nasıl tanımladığınızı açıklar mısınız?
8.2. Design the backend	Eng: How do you design backend elements of your Blockchain dApp? Tr: Blokzincir dApp'inizin arka uç unsurlarını nasıl tasarlarsınız? Eng: How do you design Smart Contracts/Chaincodes for your Blockchain dApp projects, and what factors do you consider in their design? Tr: Blokzincir dApp projeleriniz için Akıllı Sözleşmeleri / Zincir Kodlarını nasıl tasarlıyorsunuz ve tasarımlarında hangi faktörleri göz önünde bulunduruyorsunuz? Eng: How do you design and implement cryptographic algorithms like ring signature, group signature, and multi-signature to ensure security and privacy in the backend? Tr: Arka uçta güvenliği ve gizliliği sağlamak için halka imzası, grup imzası ve çoklu imza gibi şifreleme algoritmalarını nasıl tasarlıyor ve uyguluyorsunuz? Eng: How do you design and implement blockchain oracles in your Blockchain dApp projects? Can you provide examples of how blockchain oracles have been utilized in previous projects to enhance the functionality of the dApp? (if applicable) Tr: Blokzincir dApp projelerinizde ulak'ları nasıl tasarlar ve uygularsınız? dApp'in işlevselliğini geliştirmek için önceki projelerde ulak'ların nasıl kullanıldığına dair örnekler verebilir misiniz? (şayet uygulanıyorsa) Eng: How does your company design the structure of the Blockchain dApp to address the challenges of patient mobility and adhere to data privacy and protection standards across different countries? (şayet uygulanıyorsa) Tr: Şirketiniz, hasta hareketliliğinin getirdiği zorlukların üstesinden gelmek ve farklı

ülkelerdeki veri gizliliği ve koruma standartlarına uymak için Blokzincir dApp'in yapısını nasıl tasarlıyor? (şayet uygulanıyorsa)

8.3. Design the frontend

Eng: How do you design frontend elements of your Blockchain dApp?

Tr: Blokzincir dApp'inizin ön uç unsurlarını nasıl tasarlıyorsunuz?

Eng: How do you approach the design of the User Interface for your Blockchain dApp projects, and what factors do you consider to create an intuitive and user-friendly interface?

Tr: Blokzincir dApp projeleriniz için Kullanıcı Arayüzü tasarımına nasıl yaklaşıyorsunuz? Sezgisel ve kullanıcı dostu bir arayüz oluşturmak için hangi faktörleri göz önünde bulunduruyorsunuz?

Questions for Process 9 - Blockchain dApp implementation

Intended interview participant: Software Developers

Base Practices

Questions

9.1 Develop unit verification procedures

Eng: How do you perform implementation process?

Tr: Geliştirme sürecini nasıl gerçekleştiriyorsunuz?

Eng: How does your company develop and record unit verification procedures to evaluate whether each dApp software unit complies with its design requirements?

Tr: Şirketiniz, her dApp yazılım biriminin tasarım gereksinimlerine uyup uymadığını denetlemek için birim doğrulama prosedürlerini nasıl geliştiriyor ve kaydını tutuyor?

Eng: Can you explain the methods and standards you use for unit testing, including unit test cases, unit test data, static code analysis, and code review?

Tr: Birim test senaryoları, birim test verileri, statik kod analizi ve kod incelemesi dahil olmak üzere

	birim testi için kullandığınız yöntemleri ve standartları açıklayabilir misiniz?
9.2 Build APIs	Eng: How do you build APIs in your Blockchain dApp projects (serve diverse purposes, such as generating key pairs and addresses, smart contracts, data authentication through hashes and digital signatures, storage and retrieval of data, audit functions, and smart asset lifecycle management)? Tr: Blokzincir dApp projelerinizde API’leri nasıl oluşturursunuz? (anahtar çiftleri ve adresler oluşturmak, akıllı sözleşmeler, karmalar ve dijital imzalar aracılığıyla veri kimlik doğrulaması, verilerin depolanması ve alınması, denetim işlevleri ve akıllı varlık yaşam döngüsü yönetimi gibi çeşitli amaçlar için)
9.3 Develop the backend, have a running blockchain	Eng: How do you develop the backend and create a running blockchain system in your projects? Tr: Projelerinizde, çalışan bir blokzincir sistemi oluşturmak için arka ucu nasıl geliştirirsiniz? Eng: What programming languages do you typically use to write smart contracts/chaincodes, and how do you ensure they are suitable for the chosen blockchain platform? Tr: Akıllı sözleşmeler / zincir kodları yazmak için genellikle hangi programlama dillerini kullanıyorsunuz ve bunların seçilen blokzincir platformuna uygun olduğundan nasıl emin oluyorsunuz? Eng: Can you explain the process of implementing the required logic, functions, and data structures within the smart contracts and how you perform testing to ensure their proper functioning? Tr: Akıllı sözleşmelerde gerekli olan mantığı, işlevleri ve veri yapılarını uygulama sürecini ve bunların düzgün işleyişinden emin olmak için testleri nasıl yaptığınızı açıklayabilir misiniz?
9.4 Develop the frontend, user interface	Eng: Can you describe the process of building a client-side application that interacts with smart contracts and how you ensure traceability between the implemented frontend elements, the architecture, the design, and the requirements?

Tr: Akıllı sözleşmelerle etkileşime giren istemci tarafı bir uygulama oluşturma sürecini tarif eder misiniz? Uygulanan ön uç öğeler, mimari, tasarım ve gereksinimler arasında izlenebilirliği nasıl sağladığınızı anlatabilir misiniz?

Questions for Process 10 - Blockchain dApp integration

Intended interview participant: Software Developers

Base Practices	Questions
10.1 Integrate the backend and frontend units	Eng: How do you perform integration process? Tr: Entegrasyon sürecini nasıl gerçekleştiriyorsunuz? Eng: How do you approach the integration of backend and frontend units in your Blockchain dApp projects? Tr: Blokzincir dApp projelerinizde arka uç ve ön uç birimlerinin entegrasyonunu nasıl gerçekleştiriyorsunuz? Eng: Can you explain how you maintain traceability between the integrated system elements, the architecture, the design, and the requirements throughout the integration process? Tr: Entegrasyon süreci boyunca entegre sistem elemanları, mimari, tasarım ve gereksinimler arasında izlenebilirliği nasıl sağladığınızı anlatabilir misiniz? Eng: Do you conduct internal audits during the integration phase to review if all requirements and specifications are met? If yes, could you provide some examples of how this audit is conducted and what aspects are examined? Tr: Entegrasyon aşamasında tüm gereksinimlerin ve spesifikasyonların karşılanıp karşılanmadığını gözden geçirmek için iç denetimler gerçekleştiriyor musunuz? Cevabınız evet ise bu denetimin nasıl yapıldığına ve hangi hususların incelendiğine dair örnekler verebilir misiniz?

10.2 Verify and test the integration	Eng: How do you verify that the software units have been integrated into the software system in line with the integration plan in your projects? Tr: Projelerinizdeki entegrasyon planı doğrultusunda yazılım birimlerinin yazılım sistemine entegre edildiğini nasıl doğruluyorsunuz? Eng: How do you ensure that enough records are kept to allow the test to be repeated, and how are these records managed for future reference and traceability? Tr: Testin tekrarlanmasına izin verecek kadar yeterli kaydın tutulduğundan nasıl emin oluyorsunuz ve bu kayıtlar gelecekte referans ve izlenebilirlik açısından nasıl yönetiliyor? Eng: Do you consider testing contents in the safety critical domain standards (specified functioning of internal and external interfaces, testing under abnormal conditions including foreseeable misuse, implemented risk control measures defined in 6.2.)? Tr: Güvenlik kritik alanlardaki standartlardaki içerikleri (iç ve dış arayüzlerin belirtilen işleyişi, öngörülebilir yanlış kullanım dahil anormal koşullar altında test etme, 6.2.'de tanımlı uygulanan risk kontrol önlemleri) test etmeyi düşünüyor musunuz?

Questions for Process 11 - Blockchain dApp verification

Intended interview participant: Test Engineers

Base Practices	Questions
11.1 Prepare for verification	Eng: How do you perform verification, what kind of practices does it include? (various artifacts, including the actual system, models, prototypes, code, and sets of instructions.) Tr: Doğrulamayı nasıl gerçekleştiriyorsunuz, ne tür uygulamaları içeriyor? (gerçek sistem, modeller, prototipler, kod ve talimat setleri dahil olmak üzere çeşitli yapılar)

	Eng: How do you define the verification strategy for your Blockchain dApp projects? Tr: Blokzincir dApp projeleriniz için doğrulama stratejisini nasıl tanımlarsınız?
11.2 Verify the blockchain dApp product	Eng: How do you create test cases? Which specific types of testing do you perform on blockchain applications, such as functional testing, smart contract testing, security testing, performance testing, node testing, and regression testing? Are there specific testing approaches followed for the healthcare/automotive/energy domain? Tr: Test senaryolarını nasıl oluşturursunuz? Blokzincir uygulamalarında, İşlevsel test, akıllı sözleşme testi, güvenlik testi, performans testi, düğüm testi ve regresyon testi gibi hangi spesifik test türlerini gerçekleştiriyorsunuz? Sağlık/otomotiv/enerji alanine özel test yaklaşımları izleniyor mu? Eng: Can you elaborate on how you ensure the traceability between requirements and tests or other types of verification throughout the verification process? Tr: Doğrulama süreci boyunca, gereksinimler ile testler veya diğer doğrulama türleri arasındaki izlenebilirliği nasıl sağladığınızı detaylandırabilir misiniz? Eng: Do you perform testing in a live environment? Do you use a dedicated blockchain platform for testing? Tr: Testi canlı bir ortamda mı gerçekleştiriyorsunuz? Test için ayrılmış bir blokzincir platformu kullanıyor musunuz? Eng: Can you provide examples of notable blockchain testing tools you have utilized in your projects, such as Ethereum Tester, Ganache, and Hyperledger Composer? (if applicable) Tr: Projelerinizde kullandığınız Ethereum Tester, Ganache ve Hyperledger Composer gibi önemli blokzincir test araçlarına örnekler verebilir misiniz? (şayet uygulanıyorsa)
11.3 Manage verification results	Eng: How do you review verification results? What actions do you take based on the verification results, and how do you prioritize and manage

	subsequent actions to address any identified issues? Tr: Doğrulama sonuçlarını nasıl incelersiniz? Doğrulama sonuçlarına göre hangi eylemleri gerçekleştiriyorsunuz ve belirlenen sorunları çözmek için sonraki eylemleri nasıl önceliklendiriyor ve yönetiyorsunuz?

Questions for Process 12 - Blockchain dApp validation

Intended interview participant: Quality Assurance Specialists

Base Practices	Questions
12.1 Prepare for validation	Eng: How do you perform validation process? Tr: Doğrulama işlemini nasıl gerçekleştiriyorsunuz? Eng: How do you define the validation strategy for your Blockchain dApp projects, and what are the key considerations in determining the scope, priorities, and constraints? Tr: Blokzincir dApp projeleriniz için doğrulama stratejisini nasıl tanımlarsınız? Kapsamın, önceliklerin ve kısıtlamaların belirlenmesinde dikkate alınması gereken önemli noktalar nelerdir?
12.2 Validate the blockchain dApp product	Eng: How do you validate smart contracts in your Blockchain dApp projects, ensuring their code logic functions as intended? Tr: Blokzincir dApp projelerinizdeki kod mantığı işlevlerinin amaçlandığı gibi olmasını sağlamak için akıllı sözleşmeleri nasıl doğrularsınız? Eng: What methods do you use to test and evaluate the chosen consensus mechanism, and how do you assess the resilience, security, and performance characteristics of the consensus mechanism? Tr: Seçilen uzlaşı mekanizmasını test etmek ve değerlendirmek için hangi yöntemleri kullanıyorsunuz? Uzlaşı mekanizmasının dayanıklılığını, güvenliğini ve performans özelliklerini nasıl ölçüyorsunuz?

	Eng: In what ways do you ensure that your Blockchain dApp complies with relevant regulations and standards, such as data privacy regulations or specific safety critical domain standards? Are there specific validation approaches followed for the healthcare/automotive/energy domain? Tr: Blokzincir dApp’inizin veri gizliliği düzenlemeleri veya belirli güvenlik kritik alan standartları gibi düzenleme ve standartlara uygun olmasını hangi yollarla sağlıyorsunuz? Sağlık/otomotiv/enerji alanine özel doğrulama yaklaşımları izleniyor mu?
12.3 Manage validation results	Eng: How do you review the validation results? What actions do you take based on the validation results, and how do you prioritize and manage subsequent actions to address any identified issues? Tr: Doğrulama sonuçlarını nasıl incelersiniz? Doğrulama sonuçlarına göre hangi eylemleri gerçekleştiriyorsunuz ve belirlenen sorunları çözmek için sonraki eylemleri nasıl önceliklendiriyor ve yönetiyorsunuz?

Questions for Process 13 - Blockchain dApp quality assurance

Intended interview participant: Quality Assurance Specialists

Base Practices	Questions
13.1 Specify blockchain dApp product quality requirements	Eng: How do you perform quality assurance process? Tr: Kalite güvencesi sürecini nasıl gerçekleştiriyorsunuz? Eng: How do you specify the quality requirements for your Blockchain dApp projects? Do you refer to ISO/IEC 25030 for software product quality requirements and evaluation? Tr: Blokzincir dApp projeleriniz için kalite gereksinimlerini nasıl belirlersiniz? Yazılım ürünü kalite gereksinimleri ve değerlendirmesi için ISO/IEC 25030’a başvuruyor musunuz?

	Eng: Considering the unique characteristics of blockchain-based applications, in terms of scalability, interoperability, and energy efficiency, how do you address these specific quality characteristics in your quality requirements? Tr: Ölçeklenebilirlik, birlikte çalışabilirlik ve enerji verimliliği açısından blokzincir tabanlı uygulamaların benzersiz özelliklerini göz önünde bulundurarak, kalite gereksinimlerinizde bu kalite özelliklerini nasıl ele alıyorsunuz?
13.2 Assure the blockchain dApp product quality	Eng: How do you identify and address anomalies related to the accomplishment of critical quality characteristics in your Blockchain dApp projects? Tr: Blokzincir dApp projelerinizde kritik kalite özelliklerinin başarılmasına engel teşkil eden anormallikleri nasıl tespit edip giderirsiniz? Eng: Can you explain how you assure the achievement of the quality characteristics, and how do you determine and record the results of this assurance process? Tr: Kalite hedeflerine ulaşmayı nasıl güvence altına aldığınızı ve bu güvence sürecinin sonuçlarını nasıl belirleyip kayıt altına aldığınızı açıklayabilir misiniz?

Questions for Process 14 - Blockchain dApp transition

Intended interview participant: Project Manager

Base Practices	Questions
14.1. Develop a transition strategy	Eng: How do you develop a transition strategy for your Blockchain dApp products? Do you create a transition plan in agreement with the stakeholders? Tr: Blokzincir dApp ürünleriniz için uygulamaya geçiş stratejisini nasıl geliştirirsiniz? Paydaşlarla anlaşarak bir geçiş planı oluşturuyor musunuz?
14.2 Confirm the blockchain dApp product is ready for deployment	Eng: How do you ensure that the Blockchain dApp product is ready for deployment?

	Tr: Blokzincir dApp ürününün dağıtıma hazır olduğundan nasıl emin olursunuz?
14.3 Deploy the blockchain dApp on test network	Eng: Before the main network deployment, how do you ensure that the Blockchain dApp is fully functional and operating as intended? Do you deploy it on a test network and perform verification? Tr: Ana ağ dağıtımından önce Blokzincir dApp'inin tamamen işlevsel olduğundan ve amaçlandığı gibi çalıştığından nasıl emin olursunuz? Bunun bir test ağında doğrulamasını gerçekleştiriyor musunuz?
14.4 Deploy the blockchain dApp on main network	Eng: How do you carry out the deployment of the Blockchain dApp on the main network? Do you document the deployment procedure? Tr: Blokzincir dApp'in ana ağ üzerinde dağıtımını nasıl gerçekleştiriyorsunuz? Dağıtım prosedürünü belgeliyor musunuz?
14.5. Make the blockchain dApp product available to the users.	Eng: Once the Blockchain dApp is deployed, how do you make it accessible to the users in accordance with the transition strategy? Tr: Blokzincir dApp devreye alındıktan sonra geçiş stratejisine uygun olarak onu kullanıcılar için nasıl erişilebilir hale getirirsiniz?
14.6 Manage results of transition. Record transition results and anomalies encountered. Document the conditions	Eng: How do you record the results of the transition process? Do you document any anomalies encountered during the transition? Tr: Geçiş sürecinin sonuçlarını nasıl kaydediyorsunuz? Geçiş sırasında karşılaşılan herhangi bir anomaliyi belgeliyor musunuz? Eng: How do you ensure traceability between the transitioned system and its elements and the approved and controlled versions of the software system? Tr: Geçiş yapılan sistem ve unsurları ile yazılım sisteminin onaylı ve kontrollü versiyonları arasındaki izlenebilirliği nasıl sağlıyorsunuz?

Questions for Process 15 - Blockchain dApp maintenance

Intended interview participant: Project Manager

Base Practices	Questions
15.1 Develop a maintenance plan	Eng: How do you perform maintenance process? Tr: Bakım sürecini nasıl gerçekleştiriyorsunuz? Eng: How do you create a maintenance plan for your Blockchain dApp products? Do you record and assess user and internal organization feedback on the released applications? Tr: Blokzincir dApp ürünleriniz için bakım planını nasıl oluşturursunuz? Yayınlanan uygulamalara ilişkin kullanıcı ve kurum içi geri bildirimlerini kaydediyor ve değerlendiriyor musunuz?
15.2 Analyze, assess, and accept or reject change requests	Eng: How do you analyze, assess, and prioritize change requests for your Blockchain dApp products? Do you inform users and stakeholders about the issues and available changes? Tr: Blokzincir dApp ürünleriniz için değişiklik taleplerini nasıl analiz eder, değerlendirir ve önceliklendirirsiniz? Kullanıcıları ve paydaşları sorunlar ve mevcut değişiklikler hakkında bilgilendiriyor musunuz?
15.3 Implement, test, and modify modifications	Eng: After delivery, how do you implement modifications to fix bugs, enhance performance, or add new features to your Blockchain dApp products? Tr: Teslimattan sonra hataları düzeltmek, performansı artırmak veya Blokzincir dApp ürünlerinize yeni özellikler eklemek için değişiklikleri nasıl uygularsınız? Eng: How do you ensure the modifications are compatible with the existing blockchain network? Tr: Değişikliklerin mevcut blokzincir ağıyla uyumlu olmasını nasıl sağlıyorsunuz? Eng: Do you consider the challenges of blockchain modification (update challenges) ? Tr: Blokzincir modifikasyonunun zorluklarını (güncelleme zorlukları) dikkate alıyor musunuz?

15.4 Retire the blockchain dApp product	Eng: How do you handle the retirement of Blockchain dApp products once they are no longer in use or replaced? Do you have plans and activities to notify stakeholders about the retirement? Tr: Artık kullanılmadığında veya başkasıyla değiştirilmediğinde Blokzincir dApp ürünlerinin kullanımdan kaldırılmasını nasıl ele alacaksınız? Paydaşları kullanımdan kaldırma konusunda bilgilendirmeye yönelik planlarınız ve faaliyetleriniz var mı?

General Questions

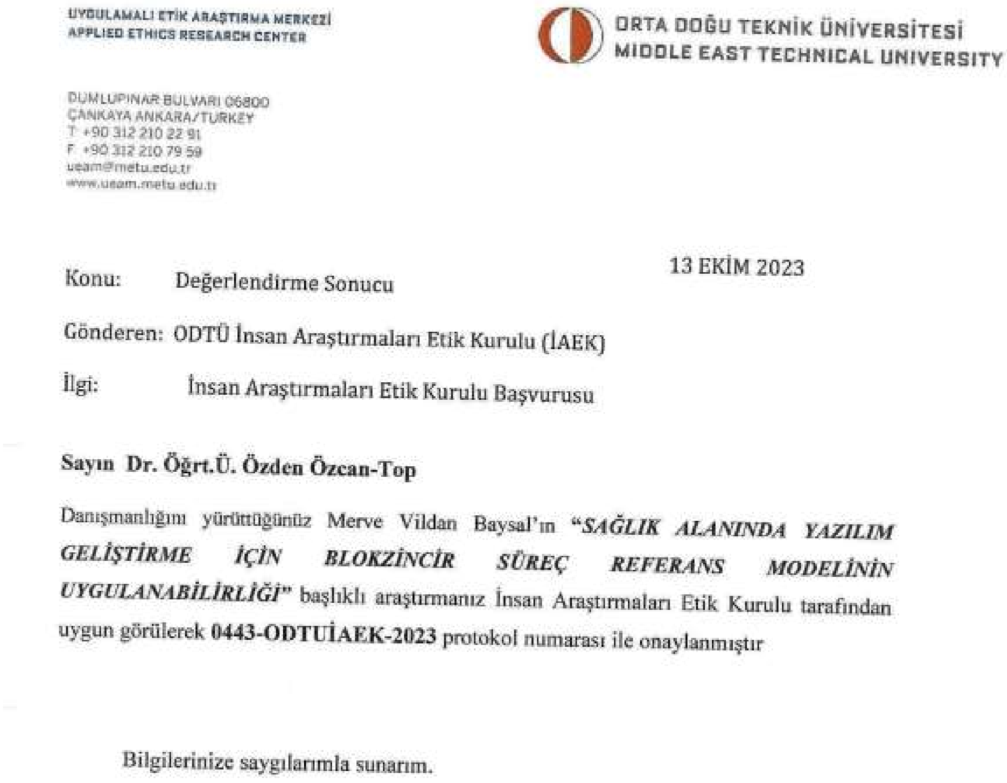
Intended interview participant: Project Manager

Eng: Do you follow any specific processes or base practices when developing blockchain health dApps that are not covered by the questions?

Tr: Blokzincir sağlık dApp'lerini geliştirirken soruların kapsamadığı herhangi bir spesifik süreci veya temel uygulamayı takip ediyor musunuz?

APPENDIX C

Ethics Committee Approval



UYGULAMALI ETİK ARAŞTIRMA MERKEZİ
APPLIED ETHICS RESEARCH CENTER

ORTA DOĞU TEKNİK ÜNİVERSİTESİ
MIDDLE EAST TECHNICAL UNIVERSITY

DUMLUPINAR BULVARI 06800
ÇANKAYA ANKARA/TURKEY
T: +90 312 210 22 91
F: +90 312 210 79 59
ueam@metu.edu.tr
www.ueam.metu.edu.tr

13 EKİM 2023

Konu: Değerlendirme Sonucu

Gönderen: ODTÜ İnsan Araştırmaları Etik Kurulu (İAEK)

İlgi: İnsan Araştırmaları Etik Kurulu Başvurusu

Sayın Dr. Öğrt.Ü. Özden Özcan-Top

Danışmanlığını yürüttüğünüz Merve Vildan Baysal'ın ***"SAĞLIK ALANINDA YAZILIM GELİŞTİRME İÇİN BLOKZİNCİR SÜREÇ REFERANS MODELİNİN UYGULANABİLİRLİĞİ"*** başlıklı araştırmanız İnsan Araştırmaları Etik Kurulu tarafından uygun görülerek **0443-ODTUİAEK-2023** protokol numarası ile onaylanmıştır

Bilgilerinize saygılarımla sunarım.

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: Baysal, Merve Vildan

EDUCATION

Degree	Institution	Year of Graduation
MS	Middle East Technical University Information Systems	2016
BS	Çankaya University Computer Engineering	2012
High School	Erzurum Anatolian High School	2006

WORK EXPERIENCE

Year	Place	Duty
09. 2012-Present	TÜBİTAK Technology and Innovation Support Programs Directorate (TEYDEB)	Expert (2012-2020) Coordinator (2020-Present)

Coordination of all studies carried out within the ÖNDEG Group regarding Frontier R&D Laboratories Support Program, SAYEM calls, Order Based R&D calls and HAMLE program, managing the Group Executive Board meetings.

Coordination of TEYDEB's transition process to PARDUS.

Analysis of needs regarding business application software used by TEYDEB, follow-up of development and tests, coordination between IT team and TEYDEB.

07.2011-08.2011	ASELSAN Radar and Electronic Warfare Systems (REHİS)	Engineering Intern
08.2010-09.2010	Turkish Radio and Television Corporation (TRT)	Engineering Intern

BLOCKCHAIN CERTIFICATES

Attended the blockchain technologies and applications certificate program organized by Ankara University between 23 May - 13 June 2022.

Informed about cryptographic fundamentals, bitcoin structure, consensus protocols, privacy in blockchain, blockchain platforms, enterprise blockchain solutions, blockchain application areas, wallets and cryptocurrency exchanges, metaverse and NFT.

PUBLICATIONS

Merve Vildan Şimşek, Aysu Betin Can, Barboros Can (2016) A Software Quality Model for Android Applications. 10. National Software Engineering Symposium. UYMS'16 - Çanakkale.

Merve Vildan Baysal, Barboros Can (2017) Priority Area Recommendations for Cloud Computing. 5. National High Performance Computing Conference. BAŞARIM'17 - Yıldız Teknik Üniversitesi, İstanbul

Öncü Şen, Numan Durakbasa, Merve Vildan Baysal, Gizem Şen (2019) Smart Factories: A Review of Situation, and Recommendations to Accelerate the Evolution Process. In book: Proceedings of the International Symposium for Production Research (pp.464-479)

Merve Vildan Baysal, Özden Özcan-Top, Aysu Betin-Can (2021) Implications of Blockchain Technology in the Health Domain. In book: Advances in Software Engineering, Education, and e-Learning (pp.641-656)

Merve Vildan Baysal, Özden Özcan-Top, Aysu Betin-Can (2023). Blockchain technology applications in the health domain: a multivocal literature review. The Journal of supercomputing, 79(3), 3112-3156.

Merve Vildan Baysal, Özden Özcan-Top, Aysu Betin-Can (2023). A Process Reference Model for Blockchain dApp Development for the Health Domain (Preprint), DOI: https://doi.org/10.21203/rs.3.rs-3449851/v1