TRUSTWORTHY MEDICAL APPLICATIONS ON THE BLOCKCHAIN

An Experiment Using Remote Attestation to Provide a Digital Twin Infrastructure

Lappeenranta–Lahti University of Technology LUT

Master's Programme in Industrial Engineering and Management, Master's thesis

2023

Kaisa Jatkola

Examiners: Professor Leonid Chechurin

Dr. Ian Oliver

ABSTRACT

Lappeenranta–Lahti University of Technology LUT

LUT School of Engineering Science

Industrial Engineering and Management

Kaisa Jatkola

TRUSTWORTHY MEDICAL APPLICATIONS ON THE BLOCKCHAIN

An Experiment Using Remote Attestation to Provide a Digital Twin Infrastructure

Master's thesis
2023
65 pages, 30 figures and 6 tables
Examiner(s): Professor Leonid Chechurin, Dr. Ian Oliver

Keywords: Blockchain, Non-fungible token, Digital twin, Remote Attestation

The verification of the integrity of data recorded on blockchains is a disregarded challenge. The limitations of blockchains to provide verification mechanisms suggest the necessity to extend the data provenance verification further back into the real-world infrastructure. The deployment of blockchain in critical areas handling sensitive data, such as healthcare machines, motivates the development of such measures.

The purpose of this thesis is to explore blockchains in real-world medical applications. The implementation introduces a mechanism to establish a link between real-world medical systems and blockchains by utilizing mechanisms such as Non-Fungible Tokens (NFT), Trusted Platform Module (TPM), and remote attestation.

This thesis provides practical insight into the design of blockchain applications with the requirement of digital twin-like properties. In conclusion, TPM and remote authentication mechanisms can be used to verify the integrity of devices and the data they generate. However, the overall architecture of blockchains and the required infrastructure are still lacking. Thus, more investigation is required to understand the actual utility of blockchains.

TIIVISTELMÄ

Lappeenrannan–Lahden teknillinen yliopisto LUT

LUT Teknis-luonnontieteellinen

Tuotantotalous

Kaisa Jatkola

LUOTETTAVAT LÄÄKETIETEELLISET SOVELLUKSET LOHKOKETJUSSA

Tutkimus etätodennuksen hyödyntämisestä Digital Twin-infrastruktuurissa

Tuotantotalouden diplomityö
2023
65 sivua, 30 kuvaa, ja 6 taulukkoa
Tarkastaja(t): Professor Leonid Chechurin, Dr. Ian Oliver

Avainsanat: Lohkoketju, Tokenit, Etätodennus

Lohkoketjuun tallennettujen tietojen eheyden todentaminen on huomiotta jätetty haaste. Lohkoketjujen rajoitukset todentamismekanismin tarjoamisessa viittaavat siihen, että tietojen alkuperän todentaminen on ulotettava kauemmas reaalimaailman infrastruktuuriin. Lohkoketjujen käyttöönotto arkaluonteisia tietoja käsittelevillä kriittisillä aloilla, kuten terveydenhuollon koneissa, motivoi tällaisten toimenpiteiden kehittämiseen.

Tämän diplomityön tavoitteena on tutkia lohkoketjuja reaalimaailman lääketieteellisissä sovelluksissa. Työn toteutuksessa esitellään mekanismi, jolla voidaan luodaan yhteys reaalimaailman lääketieteellisten järjestelmien ja lohkoketjujen välille hyödyntämällä mekanismeja kuten etätodennus, Non-Fungible Tokens (NFT) ja Trusted Platform Module (TPM).

Diplomityö tarjoaa käytännön näkemystä lohkoketjusovellusten suunnittelusta, joissa vaaditaan Digital Twin-konseptin kaltaisia ominaisuuksia. Johtopäätöksenä voidaan todeta, että TPM- ja etätodennusmekanismeja voidaan käyttää laitteiden ja niiden tuottamien tietojen eheyden todentamiseen. Lohkoketjujen kokonaisarkkitehtuuri ja tarvittava infrastruktuuri ovat kuitenkin vielä puutteellisia. Näin ollen, lohkoketjujen todellisen hyödyn ymmärtämiseksi tarvitaan vielä lisätutkimusta.

ABBREVIATIONS

DL	Distributed Ledger
DT	Digital Twins
IoT	Internet of Things
IPFS	Inter Planetary File System
NFT	Non-Fungible Token
PKI	Public Key Infrastructure
TPM	Trusted Platform Module
UI	User Interface

Table of Contents

1 Introduction 7
1.1 Background 7
1.2 Research Objective, Questions & Scope 8
1.3 Structure 9
2 Literature Review 10
2.1 Principles of Blockchain 10
2.2 Types of Blockchain & Consensus Methods 12
2.3 Smart Contracts 13
2.4 Non-Fungible Tokens 15
2.5 Blockchain in Healthcare 16
2.5.1 Data Management 17
2.5.2 Supply Chain 18
2.5.3 Internet of Medical Things 20
2.6 Limitations in the Implementation of Blockchain 21
2.7 Trusted Computing 22
2.7.1 Trusted Platform Module 22
2.7.1 Key Derivation Function & Measured Boot 23
2.7.2 Remote Attestation 24
2.7.3 Trusted Computing in Healthcare Systems 25
2.8 Summary 25
3 System Description 27
3.1 Case Study 27
3.2 Ventilator system 28
3.3 Data Models 31
3.3.1 Medical Device 32
3.3.2 Prescriptions 33
3.3.3 Physiological Data 34
3.4 Operations 35
3.4.1 Provisioning 36
3.4.2 Verification 38
3.4.3 Operations on Prescriptions 40

3.4.4 Medical Data Generation 41
3.4.5 Medical Data Transfer 43
3.5 Blockchain Architecture 44
4 Implementation 46
4.1 Trusted Infrastructure 46
4.2 Device Provisioning 48
4.3 Attestation 51
4.4 Prescription 52
4.5 Medical Data Generation 53
5 Result & Discussion 55
5.1 Results 55
5.2 Discussion 57
6 Conclusion 59
References 61

1 Introduction

1.1 Background

The concept of blockchain is evolving from a cryptocurrency transaction ledger to a programmable interactive environment on which distributed applications are established. Blockchain and the programs running on it, known as smart contracts, are increasingly emerging in domains where properties of trust and data integrity are required. (Entriken et al., 2018) In the medical industry, blockchain applications have been introduced to medical data management. In such scenarios, blockchain implementations facilitate the immutable storing of medical data as smart contracts, Non-Fungible Tokens (NFTs), and other similar data structures. Accordingly, these applications enable the establishment of tradeable entities. (Entriken et al., 2018 & Wang et al., 2021) When considering other implementations, blockchain applications are increasingly used to perform services that utilize data collected from real-world objects, users, and the surrounding environments by the underlying Internet of Things (IoT) devices. These applications are generally known as the concept of digital twins. (Maksymyuk et al., 2022)

The motivation for the thesis derives from the vague evidence of blockchain in real-life environments. Blockchains can guarantee untampered data – within certain byzantine failure constraints - and audit trails (Wang et al., 2022 & Zheng et al., 2017). However, the currently existing blockchain systems fail to provide mechanisms to verify the external integrity of the data on the chain. (Hardjono & Smith, 2019) Similarly, the mechanisms of reliably linking real-world devices with blockchain are not well understood. (Arcenegui et al., 2021) Simply because something is on a blockchain does not mean it is correct.

The lack of the ability to provide external integrity in scenarios where data is provided by a real-world device is a critical oversight in terms of security and trustworthiness. For example, in case external data source is compromised, it becomes possible to feed non-sensical and wrong data to the blockchain. According to Altamimi and Zriqat (2016), the aspects of security and trustworthiness of data are particularly important when working with critical data, such as medical data, where the possibility of counterfeited data may be a risk.

Given these challenges, the unexplored integration of trusted computing mechanisms and blockchain technology presents an interesting area for exploration. In the real world, technologies such as Trusted Platform Module (TPM) are designed to provide trust by establishing the identity and integrity of systems. By extending this approach through the integration of remote attestation procedures, the ability to monitor and detect state changes within a device's systems becomes feasible. Moreover, the combination of these technologies establishes trust in real-world systems. (Trusted Computing Group, 2019) Whereas technologies, such as blockchain and NFTs, enable the representation of real-world entities within the blockchain environment. The inherent integrity and provenance properties establish trust. (Entriken et al., 2018 & Wang et al., 2021)

1.2 Research Objective, Questions & Scope

The objective of the research is to study blockchain in real-world applications. The main interest of the thesis is to explore the constitution of blockchain applications with TPM and remote attestation mechanisms. In this thesis, the given technologies are experimented to better understand the implementation of blockchain applications. The research objective can be divided into the following research questions.

1. How can blockchains be applied in a real-world environment?
2. What technologies can be used to verify the provenance of the data in the blockchain?

There are a few limitations in this research. Essentially, the research emphasizes the existing applications of blockchain technologies and trusted computing concepts rather than the technologies themselves. Therefore, examining the technological properties and implementation of blockchains in detail is outside the scope of this study. Thus, an overview of the technological properties of blockchain and trusted computing concepts is presented to understand the main concepts.

In order to form a base for the research topic, a literature review is conducted. Given the novelty of the research topic in this thesis, the literature review approach is a narrative review. According to Saunders et al. (2019), in contrast to more systematic reviews, narrative

reviews are more flexible in nature and suitable for understanding an unexplored and emerging topic, such as in this thesis.

The literature review consists of reviewing peer-reviewed academic articles related to the topic of this thesis. Due to the novelty of the research area, further information sources, such as conference papers and industry projects, are utilized to obtain the most recent research and viewpoints in the area.

1.3 Structure

The thesis is organized into six main Chapters. Chapter 1 introduces the background and objectives of the research. Chapter 2 focuses on the literature, considering distributed ledgers' general frameworks and operations mechanisms, their typical application scenarios in the medical domain, and the current limitations. In order to establish a comprehensive overview of the technical capabilities of blockchain, the concepts of smart contracts and NFT are discussed. In addition, the Chapter discusses the concept of trusted computing and related technologies. After the literature review, Chapter 3 represents the system design of the medical case study. Chapter 4 discusses the implementation and design choices of the case study. Finally, conclusions of the research and future research recommendations are provided in Chapter 5.

2 Literature Review

This chapter outlines the current literature on blockchain technologies and the area of trusted computing and remote attestation. In order to establish a comprehensive overview of blockchain technologies and their properties, the main principles are discussed in section 2.1. The following sections, 2.2 and 2.3, introduces the main principles of smart contracts and NFTs.

Once the technical properties of blockchain are discussed, section 2.4 outlines the current literature on the application of blockchain technologies, smart contracts, and related data structures in medical data systems. Due to the novelty of the technology and the limited evidence of real-world implementation, the current limitations of blockchain are reviewed in section 2.5. Lastly, section 2.6 discusses the concepts of trusted computing and its application in medical data systems.

2.1 Principles of Blockchain

A distributed ledger (DL) is a transaction ledger shared across various network participants. The DLs are intended to provide a decentralized and transparent approach to data recording, verification, and storage. (Bashir, 2018) In typical centralized ledgers, all records are stored in one central location. A central authority exclusively maintains and determines the true state of the ledger. In contrast to traditional centralized ledgers, DL systems typically possess only one ledger duplicated by every network participant, resulting in each participant holding an identical copy of the entire ledger. Without a central authority, the participants mutually agree on transactions and the ledger's true state. (Zheng et al., 2017 & Yaga et al., 2018)

One of the key implementations of DL is blockchain, a distributed ledger that organizes data structures into blocks and utilizes cryptographic methods to link these blocks together. (Wang et al., 2022 & Zheng et al., 2017). Wang et al. (2022) present a generic process for a blockchain system. The process can be divided into five steps: transaction initiation, transaction validation, new block generation, block validation, and ledger update. The generic workflow is presented in Figure 1.

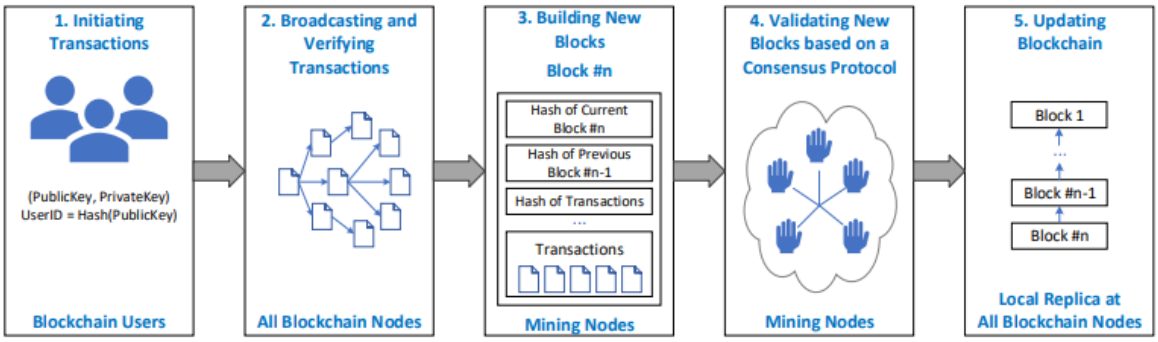

Figure 1 Generic workflow of a blockchain system (Wang et al., 2022)

Depending on the blockchain, a block typically consists of valid transaction proposals received over a certain period. The transactions are initiated and proposed by the blockchain network participants, typically called nodes. (Yaga et al., 2018) A transaction is considered valid when the validation requirements are fulfilled. (Buterin, 2014).

In order to prove the authenticity of the node, the nodes use cryptographic encryption methods, such as public key infrastructure (PKI). According to Yaga et al. (2018), the essence of PKI is that it provides pseudonymity to some extent, which allows nodes to be identified by their public addresses instead of their real identities (Yaga et al., 2018). PKI provides a pair of public and private keys for each user. The user's private key is used to cryptographically sign a transaction when the transaction is subsequently proposed to the blockchain network. The public key acts as the user's public address in the transaction verification operations. (Zheng et al., 2017)

Figure 2 illustrates a simplified example of a block data structure. For example, each block comprises a block identifying hash, a creation time, a hash of the preceding block, transaction data, and other relevant information depending on the protocol. (Zheng et al., 2017)

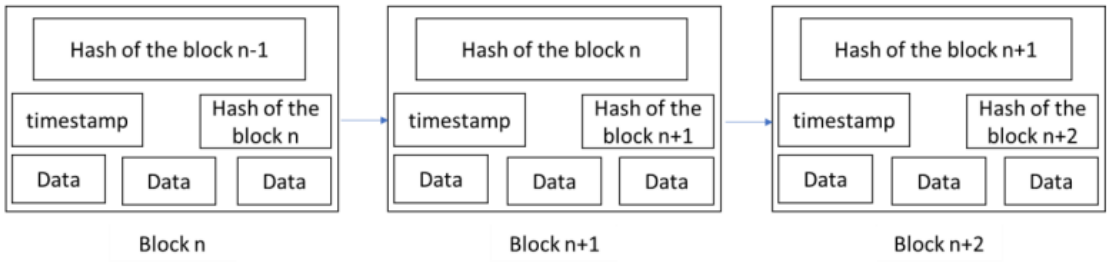

Figure 2 An example of a blockchain structure (Zheng et al., 2017)

The chaining of blocks is achieved through cryptographic hash functions. In hash functions, the same hash output cannot result from different messages, which makes it collision resistant. Accordingly, extracting the original input data from the output data is impossible. (Yaga et al., 2018) In order to chain a new block, a hash of the previous block is placed in the new block. As a result, the latest block in the chain continuously inherits a hash output of all the transactions that occurred in its predecessor until the first genesis block. Similarly, the subsequent blocks follow a similar procedure to continue the chain. (Zheng et al., 2017) Once a block is constituted, the blockchain network participants mutually validate the block through a consensus mechanism and record it on the blockchain. (Yaga et al., 2018)

By design, blockchains are considered to inherit advantageous properties, such as transparency and integrity (Agbo et al., 2019). In the blockchain network, all participants have access to the same information on the chain and are able verify the data (Pane et al., 2020). The process of chaining blocks guarantees that each transaction is hashed and time-stamped, resulting in a transaction audit trail. If any transaction recorded in a block is altered, the related hash outputs change, which causes the entire chain structure to be compromised. This approach makes the ledger more resistant to potential failures and tampering. (Yaga et al., 2018)

2.2 Types of Blockchain & Consensus Methods

Blockchains can be classified into different types according to the network's behavior. In essence, the approach to constructing governance models for adding nodes and reading and writing information on the blockchain network alternates among the blockchain systems.

(Marchesi et al., 2022) In certain blockchain implementations, all nodes can join the network and conduct different operations. Any node can join and read the blockchain without authorization or prior access permission. (Buterin, 2014 & Zheng et al., 2017) This type of blockchain is typically referred to as permissionless or public blockchain.

In contrast, some blockchains are restrained from external parties. In these blockchains, participating nodes must obtain access permission from a consortium or similar authority in order to join the blockchain. In addition, it is typical that nodes are granted specific permissions to conduct read and write operations and to participate in data management and validation operations. (Marchesi et al., 2022) This type of blockchain is typically referred to as permissioned blockchain. In further implementations of permissioned blockchains, the characteristics of closeness or openness can vary regarding the intended use of the blockchain. According to Buterin (2014), both permissionless and permissioned variations provide advantages and disadvantages. The suitability of a particular blockchain generally depends on the nature of the use case and its business means.

As previously mentioned, blockchains use different approaches to validate blocks and establish consensus between the ledgers in the distributed nodes. A consensus mechanism is a procedure that determines that all participants reach an agreement on the sequence in which the validated blocks are appended to the blockchain ledger. (Yaga et al., 2018) Consistency in the ordering of the blocks is important since typically there are multiple miners in the network that receive transaction proposals in varying sequences. Consequently, the miners may produce blocks, in which the sequencing of the transactions differs from other blocks. (Zheng et al., 2017) Various protocols are proposed for the consensus mechanism. For example, commonly known protocols are proof-of-work and proof-of-state. (Buterin, 2014) A further examination of these protocols is beyond the scope of this thesis.

2.3 Smart Contracts

According to Szabo (1994), smart contracts are essentially “computerized transaction protocol that executes terms of a contract” (Szabo, 1994). The common definition of smart contracts refers to a computer program deployed, stored, and executed on a blockchain network. Smart contracts operate autonomously on the blockchain, eliminating the necessity for intermediaries to verify and execute them. (Wang et al., 2018 & Entriken et al., 2018)

Although smart contracts are commonly associated with blockchain platforms such as Ethereum (Entriken et al., 2018), other blockchain networks and DLs implement similar programs.

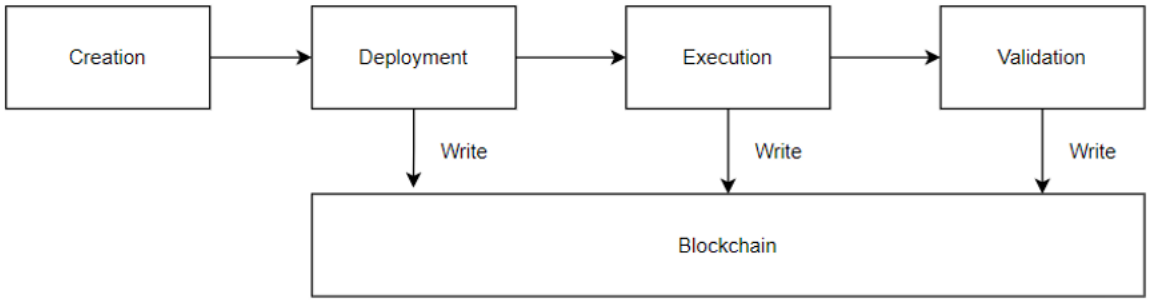

Figure 4 Simplified illustration of the smart contract process (adapted from Wang et al., 2018)

Figure 4 above aims to summarize a simplified smart contract process. At the beginning of the process, the rules and conditions that govern the functionality of the contracts are defined, converted to executable computer programs, and deployed on a blockchain network. (Wang et al., 2018 & Zheng et al., 2020). Smart contracts are executed based on a set of pre-defined conditions and rules. The conditions can refer, for instance, to a particular external factor, such as a specific input, or an internal condition within the blockchain environment. When a condition in a smart contract is met, the smart contract automatically executes the transaction. (Wang et al., 2018) The participating nodes of the blockchain network validate the execution of the smart contract based on a consensus mechanism, which purpose is to ensure a collective agreement on the outcome of the contract's execution among the nodes. At last, the latest states of each involved participant are updated accordingly, and the transaction is recorded on the blockchain. (Zheng et al., 2020)

In traditional systems, smart contracts establish standard behavior between other contracts and participants in the blockchain environment. For that reason, the contracts are typically employed for specific operations, such as transferring digital values or assets, updating a state of variables, or interacting with other smart contracts. (Buterin, 2014) From a broader perspective, the contracts are considered the foundation for deploying blockchain applications. In some instances, these applications are identified as decentralized

applications, which are self-driven, autonomous applications interacting with the blockchain. (Wang et al., 2018) In addition, smart contracts can establish token generation, distribution, access control, and other rule enforcement (Entriken et al., 2018 & Wang et al., 2018).

2.4 Non-Fungible Tokens

Several approaches to implementing cryptographic tokens have been developed. For example, blockchain native tokens (e.g., Buterin, 2014) and on-chain tokens (e.g., Entriken et al., 2018) that are implemented on the blockchain and leverage the smart contract logic. Technically, the on-chain tokens comply with the main principle: the underlying smart contract manages the governance and functionality of a token (Entriken et al., 2018). Moreover, tokens can be further classified based on the obtained behavior.

Table 1 Token protocols proposed by Ethereum (Entriken et al., 2018).

Standard	**Name**
ERC-721	Non-fungible token
ERC-20	Fungible token
ERC-1155	Semi-fungible token

Table 1 above show some standard protocols proposed for implementing tokens in the Ethereum ecosystem. The ERC-721 standard specifies a set of smart contract variables that constitute a data structure known as a non-fungible token (NFT). Each NFT is typically associated with information, such as a unique token identity and owner identity, which are recorded in the token's metadata on the blockchain at the time the token is created. (Entriken et al., 2018)

The uniqueness, minting, and ownership properties differentiate NFTs from other typical cryptographic tokens, such as fungible tokens (ERC-20). These properties make NFTs suitable for representing, for example, ownership of unique digital or physical objects in a blockchain environment (Entriken et al., 2018 & Valenonti et al., 2021). The notion of ownership alters at different use scenarios of NFT. According to Entriken et al. (2018) and

Musamih et al. (2022) the ownership property can enforce the right to perform activities over the token, including transferring the token to other entities. In typical scenarios, the owner attribute can refer to, for example, a blockchain account address of an entity.

The NFTs are applications on blockchain that derive their properties and advantages from the underlying chain. The identity, metadata, and provenance information associated with the NFTs are permanently recorded on the chain once the token is minted. (Wang et al., 2021) Once the token is minted, the record cannot be altered without compromising the integrity of the chain (Wang et al., 2021). In this work, the process of minting refers to an activity in which a smart contract's state is permanently fixed with the information it holds at that point in time. Figure 5 summarizes the process of creating an NFT.

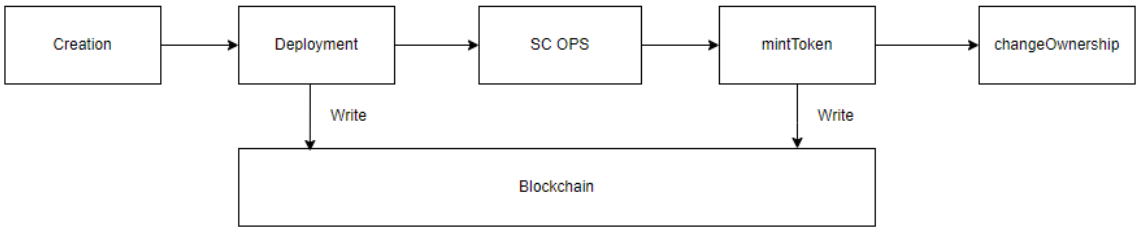

Figure 5 A simplified process of the creation of NFT (adapted from Wang et al., 2021)

The NFTs can be continuously transferred within the blockchain environment. Typically in this operation, the transfer operation of the token refers to the transfer of ownership from one entity to another. The transaction and ownership history, including the minting entity, the previous owners, and the current owner, are recorded on the blockchain ledger. Moreover, the underlying decentralized infrastructure ensures that each transaction, identity, and provenance history related to the NFT are auditable and verifiable. (Wang et al., 2021 & Valeonti et al., 2021)

2.5 Blockchain in Healthcare

In the healthcare domain, the properties associated with blockchain appear to provide advantageous properties for healthcare applications. The properties, such as transparency, integrity, and verifiability, enhance traditional centralized solutions by enabling a more

secure and interoperable environment (Agbo et al., 2019). This section discusses the recent implementations of blockchain in healthcare data management, supply chain management, and Internet of Medical Things.

2.5.1 Data Management

Due to the distributed nature of blockchain, it is often observed that blockchain can enhance the traditional centralized servers and data-storing solutions by enabling a more interoperable environment. The blockchain-based healthcare applications can overcome the limitations on interoperability among healthcare stakeholders by allowing more efficient and distributed data sharing. (Agbo et al., 2019)

Blockchain-based solutions enhance data integrity and verifiability compared to the common healthcare data management systems. By its nature, blockchain can detect alteration of the data recorded in the blocks. Therefore, blockchain has the potential to protect healthcare data from potential loss of data, fraud, and security attacks. (Agbo et al., 2019) Similarly, Pane et al. (2020) state that the limited third-party interaction the blockchain provides could enhance the quality of healthcare research data.

Recent research indicates that using smart contracts, tokens, and similar data structures allows data representation in the blockchain environment. Data structures, such as NFTs, represent healthcare-related objects in many implementations. According to Musamih et al. (2022), utilizing NFTs to represent assets and attributes such as health data sets, medical devices, or other comparable physical equipment establishes a digital twin type of mechanism for the medical asset. The utilization of NFTs enables the assets to become transportable across different digital environments while ensuring the recording of the interactions involving the asset on the blockchain.

The emphasis in many works is on the governance and ownership of medical data. The authors (e.g., Azaria, 2016, Jennath et al., 2020, Baiju et al., 2022 & Vijayalakshmi et al., 2022) propose blockchain-based medical data management systems that focus on patient consent-based data sharing. The underlying smart contracts are encoded to control access, distribution, and other equivalent operations over healthcare records. According to Ismail et al. (2021), the main notion is that a smart contract validates the access policies in the token's

metadata possessed by the subject when considering the access request to an object. The access is granted based on the validation result. However, it is worth noting that none of the proposed solutions present implementation details of such a system, and it is unclear how the proposed access control mechanisms help with external data integrity and link to real-world data.

Hapiffah & Sinaga (2020) demonstrate the use of smart contracts, particularly NFTs, in representing traceable medical data. The authors emphasize the properties of NFT that enable establishing ownership structures on the blockchain and real-world environment. These properties can accelerate a patient's control over personal data in both environments.

Similarly, Subramanian & Subramanian (2022) demonstrate an implementation of a digital pathology system that uses NFT data structures and IPFS to distribute medical images. The authors state that the proposed architecture improves privacy, reduces costs compared to traditional medical image distribution systems, and potentially makes the diagnosis process more efficient. In both works, the authors propose linking the real-world object to the NFT by encoding a hash of the medical object into the token metadata but do not explain how this hash is created or any other cryptographic properties, such as a signing of that hash. Kumar et al. (2022) propose a health data marketplace system based on NFT medical records. The approach of representing different medical entities as NFTs on the blockchain enables monetizing personal medical information and trading amongst patients, healthcare organizations, and insurance parties.

2.5.2 Supply Chain

Similarly to data distribution, blockchain is often utilized in the medical supply chain works to enhance the supplied assets' management, traceability, and integrity. According to Clauson et al. (2018), blockchain allows the establishment of monitoring and auditing processes over the entire medical asset distribution chain. Given the nature of blockchain, information on each interaction with stakeholders and processes is securely recorded on the chain. Consequently, blockchain can be utilized to authenticate the provenance of medical assets, distributors, or other relevant entities throughout the supply chain.

According to Pane et al. (2020), the utilization of blockchain to monitor the different stages of the medical device supply chain, for example, production, usage, and maintenance, enhances the data traceability and integrity of the medical device. For instance, the verifiability properties can be used to mitigate the counterfeiting of medical documents and assets.

The utilization of data structures, such as tokens, is often introduced to accelerate the tracking and tracing of different digital and physical medical assets through their lifecycle. Many authors (e.g., Chiacchio et al., 2022, Alkhader et al., 2021 & Marchesi et al., 2022) propose solutions for the supply management of medical assets. In the solutions, the token metadata contains identifying information about the medical object, which enables the identification and tracking of the asset in the blockchain environment. Marchesi et al. (2022) emphasize that such an approach could be used to certify asset components at different stages of their lifecycle. This procedure could enhance the verifiability of the asset and its components.

When considering other implementations, dos Santos et al. (2021) and Omar et al. (2020) propose systems that utilize smart contracts and token variations in the supply chain context. These approaches aim to establish provenance and auditing properties for the supplied assets. By using these frameworks, it is possible to enhance information availability and reliability within the supply chains. Similarly, Westerkamp et al. (2020) demonstrate a system utilizing NFTs for tracing components in a manufacturing supply chain. The components are identified by applying physical variables of the asset, such as QR code, weight, or size of the asset, to the metadata of the associated NFT. However, it is evident that the link between the physical asset and NFT can be compromised and cannot guarantee reliability in a real-world context.

Arcenegui et al. (2021) state that creating a link between a real-world physical asset should not rely on intrinsic identifiers, such as QR codes or physical size, due to the ease of counterfeiting such characteristics. Moreover, the efforts attempting to represent real-world assets, especially devices, as NFTs, should consider defining them with more tangible attributes.

2.5.3 Internet of Medical Things

As stated before, blockchain and smart contracts have the potential to automate a variety of operations. In IoT, smart contracts are typically exploited in operations, including authentication, payment processing, and data and agreement management (Maksymyuk et al., 2022). Blockchain enables a secure environment where IoT devices can share and store data over virtual applications. In typical implementations, the operations of the IoT devices over data are conducted autonomously through smart contracts while ensuring that each operation records on the chain in a verifiable manner. (Maksymyuk et al., 2022) For instance, blockchain infrastructure and NFT data structures are often utilized to automate service-level agreement (SLA) negotiations between network service providers. (Maksymyuk et al., 2022 & Faisal et al., 2022) Malamas et al. (2019) use the principle of smart contracts to implement an access control model for medical IoT environments.

In the medical area, Seliem & Elgazzar (2019), Azbeg et al. (2021), and Bhattacharjya et al. (2022) all propose using blockchain as a data trading framework for medical IoT devices. Bhattacharjya et al. (2022) demonstrate the utilization of blockchain in a medical application. The authors state that the solution provides more trust and security in the data in comparison to, for example, traditional cloud-based solutions. Azbeg et al. (2021) implement a blockchain-based medical data system for remote patient monitoring. The system utilizes IPFS and proxy re-encryption mechanisms to enhance secure data management. However, the works do not discuss securing the state of the device or ensuring the accuracy of the data.

Maksymyuk et al. (2022) state that the use of unique data structures, such as NFTs, allows the synchronization of physical infrastructure, such as robots, sensors, and manufacturing processes, with the corresponding simulated models in the blockchain environment. By representing different entities as NFTs on the blockchain, trading and capitalizing the assets amongst users and services can be established. (Maksymyuk et al., 2022) Moreover, blockchain and related programs are expected to have an essential role in supporting the development of future-generation networks and potential applications, including virtual healthcare environments (Kalla et al., 2022 & Huynh-The et al., 2023). Nevertheless, specifics of implementation, design, and external data integrity are not covered.

A few further efforts have been proposed to create digital twins of real-world IoT devices and NFTs. Arcenegui et al. (2021) propose a system that utilizes Physically Unclonable Functions (PUFs) to create unique and tamper-resistant identities for IoT devices. These identities are represented as NFTs on the blockchain, ensuring the authenticity and integrity of the devices.

2.6 Limitations in the Implementation of Blockchain

Several authors (e.g., Zheng et al., 2017 & Agbo et al., 2019) have emphasized the challenges in the real-world implementation of blockchain that are yet to be overcome. Blockchain projects typically face problems, including cross-chain interoperability, scalability, security vulnerabilities, inefficiency, and problematic consensus mechanisms. (Agbo et al., 2019) In addition, blockchains and related smart contract programs are often criticized due to their inability to be compliant with standard regulations and compliance measures (Zheng et al., 2017).

Furthermore, integrating blockchain into legacy systems still requires great research and investment efforts (Musamih et al., 2022). The technology is at the preliminary stages and requires significant advancements in terms of scalability and interoperability before it can support higher transaction throughput and service offerings (Zheng et al., 2017 & Jennath et al., 2020). Interoperability challenges typically refer to the varying degrees of protocols, transaction architectures, and consensus processes that the various blockchain technologies inherit. Moreover, obtaining interoperability between different chains is challenging due to the limitations of common practices. (Pane et al., 2020, Jennath et al., 2020, & Huynh-The et al., 2023)

In addition, several challenges exist regarding the security of the real-world infrastructure employing blockchain technology. One of the crucial concerns is the security of the real-world systems interacting with the blockchain environment. (Hardjono & Smith, 2019) For example, oracles are mechanisms that provide external data to smart contracts that interact with blockchain. These mechanisms can introduce incorrect information into the blockchain when external data is altered. (Ethereum, 2023)

2.7 Trusted Computing

Trusted Computing is a concept and a combination of technologies that enhance the security and integrity of computing systems and data. Trusted Computing focuses on creating a secure and trustworthy environment to carry out computations, store data, and execute critical tasks. It utilizes hardware and software-based components, such as TPM, to establish an identity and integrity of a system or parts of a system. (Trusted Computing Group, 2019)

This chapter discusses the concepts of Trusted Platform Module (TPM) and remote attestation (RA). Moreover, the utilization of these concepts in establishing a chain of trust for a system and the process of verifying a system's integrity are introduced.

2.7.1 Trusted Platform Module

Trusted Platform Module (TPM) is a component, typically a single chip, embedded on a system board that approaches security from a hardware standpoint. As embedded in a system, TPM serves as a local root of trust for operations, including establishing an identity, authenticity, and integrity of the system. (Trusted Computing Group, 2019) Figure 6 illustrates an overview of the relationship between the significant concepts of TPM discussed in the following sections.

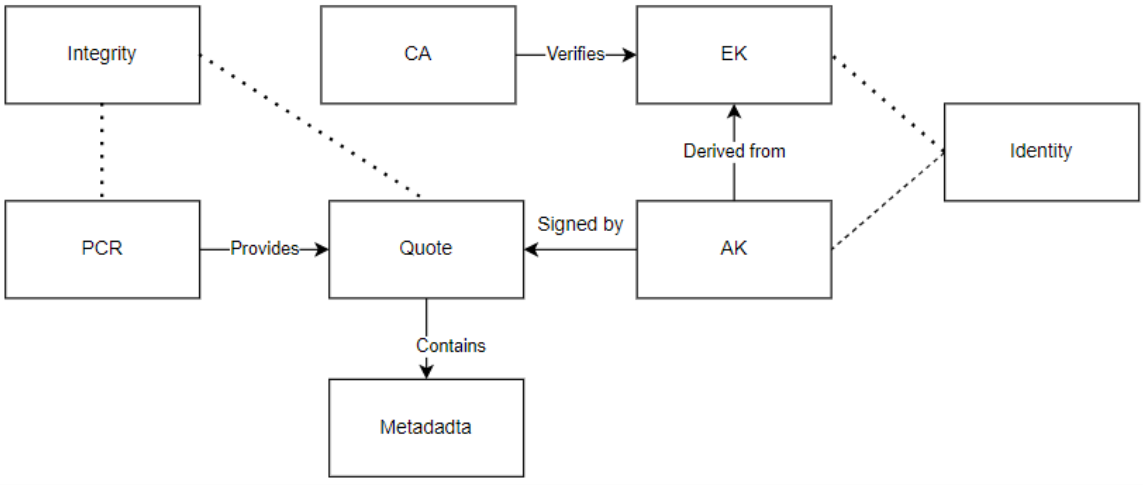

Figure 6 The relationship between the concepts of TPM

A TPM implements capabilities such as cryptographic functions and secure registers known as Platform Configuration Register (PCR). The cryptographic functionality enables operations, including encryption, hashing, key generation, and digital signature. Whereas the primary purpose of PCRs is to securely store information related to the state of the components of the system. Each PCR contains a particular value of a system configuration. In addition to these capabilities, a TPM contains non-volatile random-access memory (NVRAM) to deposit data and cryptographic keys. (Trusted Computing Group, 2019)

2.7.1 Key Derivation Function & Measured Boot

The Key Derivation Function (KDF) generates cryptographic keys from the root key. A root key is generated during manufacturing and securely embedded in the TPM. The KDF takes input from the root to derive different cryptographic keys. For instance, a unique public-private key pair is formally known as an endorsement key (EK). The key combination enables the notion of a unique identity for the particular TPM. The primary purpose of EK is to derive new keys to TPM, for example, attestation keys (AK). The EK can be used for encryption and decryption. An AK is a restricted signing key primarily used for signing TPM-generated data structures, such as system measurements. Moreover, signing information with the keys unique to a specific TPM ensures that the integrity of the data can be proven. (Arthur et al., 2013 & Trusted Computing Group, 2016)

In the TPM area, the keys are typically certified against a certificate authority (CA) in order to provide additional evidence of the TPM's provenance. In typical instances, manufacturers and TPM vendors may provision the TPM with a set of keys and related certificates before the platform's distribution to an end user. An EKcert comes from signing the public key of the TPM against a manufacturer's CA. This is performed at manufacturing time. (Arthur et al., 2013)

Upon bootup of a system, TPM conducts a measurement operation on the different components of the system, such as BIOS, boot records, applications, and operating systems. The TPM uses hash functions, for example, SHA1 and SHA256, to fingerprint the collected measurements and store the resulting outputs by extending the PCRs. (Arthur et al., 2013 &

Trusted Computing Group, 2016) The measurements intend to represent the system's state, from which further integrity analyses can be conducted.

2.7.2 Remote Attestation

Remote Attestation (RA) is a process that enables a third party to verify the intactness and trustworthiness of a system's software and hardware configurations. A system can be trusted when the state measurement values match expected values and no alterations from a secure standard process occur. Moreover, using TPMs in RA is possible due to the ability to provide identity and integrity measurements from the system. (Trusted Computing Group, 2019) This thesis focuses on attestation procedures utilizing TPMs.

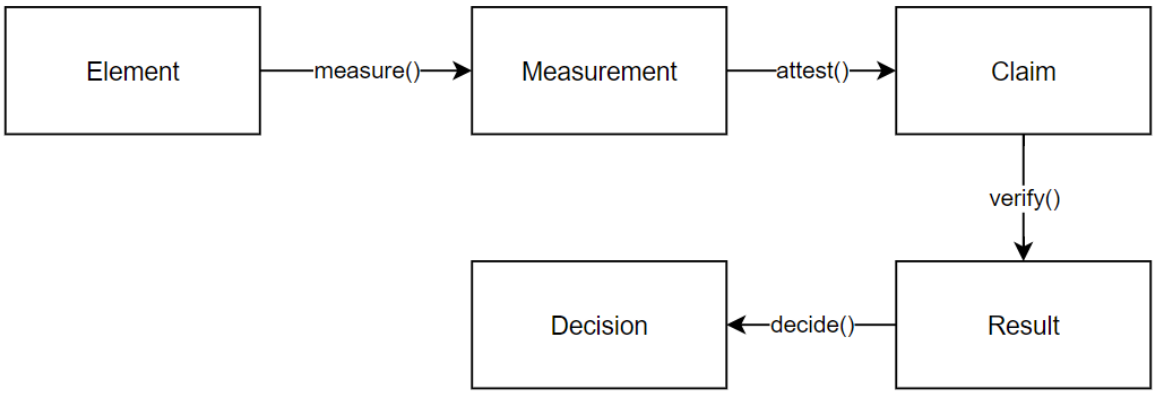

Figure 7 The operations of the attestation process (Adapted from Turcanu, 2021)

Figure 7 illustrates an example of an attestation scenario. A client entity requests the attestation server to report the system's trust status. The subject of attestation is any system component that can be measured. The RA interacts with the system's TPM by requesting a measurement of the system's state. (Arthur et al., 2013 & Oliver et al., 2019) The measuring process refers to a mechanism in which the TPM obtains measurements of the PCRs and signs them with an attestation key. A measurement comprises a value computed from the hashed values in the PCR and metadata about the system configuration, including a TPM's firmware version, clock value, and reset values. (Trusted Computing Group, 2019) This process establishes the integrity of the system.

Once the measurements are obtained, the attestation server compares the quoted values with the expected values of the system registered on the attestation server. The comparison determines the trust status of the system by considering if the system components have been compromised. At last, the attestation mechanism output presents a decision on the attested system's state. The client entity receives an indication of the result, from where the decision of the further steps to be taken. For example, events that could raise concerns over the state of the system are key failures, differing PCRs, unexpected shutdowns, unpredicted reboots, and excessive clock values. (Arthur et al., 2013 & Oliver et al., 2019)

2.7.3 Trusted Computing in Healthcare Systems

The main concerns in employing technology in healthcare systems are security and privacy (Altamimi & Zriqat, 2016). Medical device failures are typically linkable to specific challenges related to the device's operation. Incorporating TPMs into medical devices can ensure the integrity of medical operations. It allows the employment of RA, which becomes particularly useful when the medical device interacts with a remote healthcare infrastructure or similar remote servers. In these scenarios, assurance of a non-compromised device can be provided. (Oliver et al., 2020)

Oliver (2020) explores incorporating security mechanisms provided by TPM with a medical ventilator to establish a trusted medical system. The author states that incorporating TPM into the system allows the monitoring of individual components and enhances the device's security (Oliver, 2020). When considering blockchain-related implementations, trusted computing is mainly noted in the context of node security (Hardjono & Smith, 2019 & Schüpany & Pirker, 2022).

2.8 Summary

To summarize this Chapter, the findings of the literature review are discussed. The literature on blockchain in the healthcare area primarily focuses on aspects such as data integrity and management. While numerous solutions have been proposed in which blockchains and the subsequent token data structures theoretically facilitate efficient and secure data sharing and enhance data authenticity through the inherent immutability of blockchain, there is limited

evidence of practical implementations. The studies presented fail to demonstrate the validity of these blockchain use cases in the real world.

The previous sections discuss a few experiments related to data storage and trade scenarios in the context of blockchain. These experiments lack approaches to bridging the gap between real-world and virtual environments. In addition, the proposed applications have no concentration on the security aspects of these applications. It is identified that blockchain and smart contracts, by their inherent nature, do not possess mechanisms to ensure the authenticity of the data appended on-chain. Thus, there is a lack of measures to prove the legitimacy and provenance of the data stored in the blockchain. While blockchain shows promise for data integrity, practical implementations, security aspects, and the integration of technologies, such as TPMs, are a few of the aspects that are still widely unexplored.

3 System Description

The proposed system aims to establish an environment where data integrity can be maintained throughout its lifecycle by utilizing the technologies discussed in Chapter 2. Blockchain is utilized to ensure the unalterability and auditability of the different elements and the remote attestation to establish the trust of the device and data in the real world. By combining these two environments, data verification can be conducted on both environments. The system components are discussed in detail in the following sections.

3.1 Case Study

A medical case study, based on medical ventilator, is established to demonstrate the use of remote attestation to maintain a link between entities on the blockchain and in the real world. Remote attestation is coupled with hardware security through the TPM and its capabilities to uniquely identify devices and provide integrity information about the devices' current state and operation. Figure 8 depicts the architecture and behaviour of the proposed medical system.

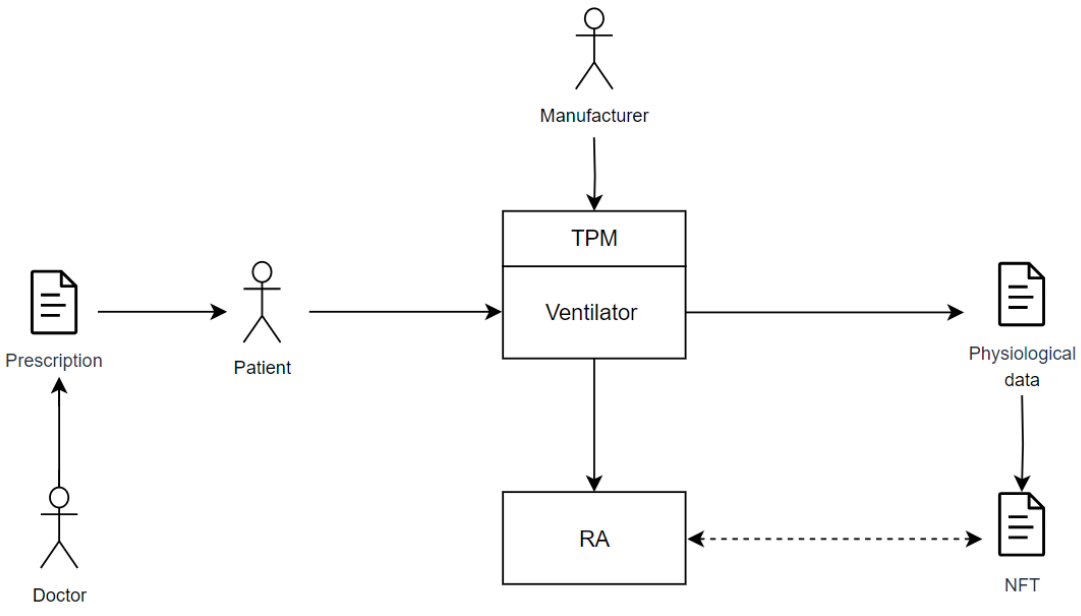

Figure 8 Proposed system design

The integrity chain is established by a manufacturer who delivers a trusted medical device to a healthcare operator. The medical device refers to, for instance, a home-use ventilator such as a continuous positive airway pressure device (CPAP) machine. In the healthcare environment, a doctor assigns the trusted medical device to a patient through a prescription, after which the patient continues to use the device in a remote home environment.

Moreover, the use of the trusted ventilator ensures that data generated by the ventilator is associated with the user and device in a form that there can be no dispute over the provenance of that data against the patient using that device or the device itself. The remote attestation ensures the verification of the identity of the ventilator is as expected and that the ventilator has been operating expectedly while generating the data.

3.2 Ventilator system

A ventilator or continuous positive airway pressure device (CPAP), based on Oliver (2020), is constructed. The ventilator system is equipped with trust components, such as TPMs and related infrastructure. The incorporation of TPM allows the attestation operation over the ventilator. The TPM provides further operations, such as system integrity monitoring, a core root-of-trust, measured boot mechanisms, and a trust agent for interacting with a remote attestation environment. In this work, it is assumed that the device maintains an internet connection via Wi-Fi, 5G, or similar, which allows the ventilator to transmit data to an external medical record system.

The ventilator includes a motor for blowing air and various pressure and flow sensors to control and monitor airflow, oxygen concentration, and flow rate. In addition, the system includes gas analysis sensors, communications, a display, and other auxiliary parts. (Oliver, 2020) Figure 9 illustrates an example of a ventilator with trust components.

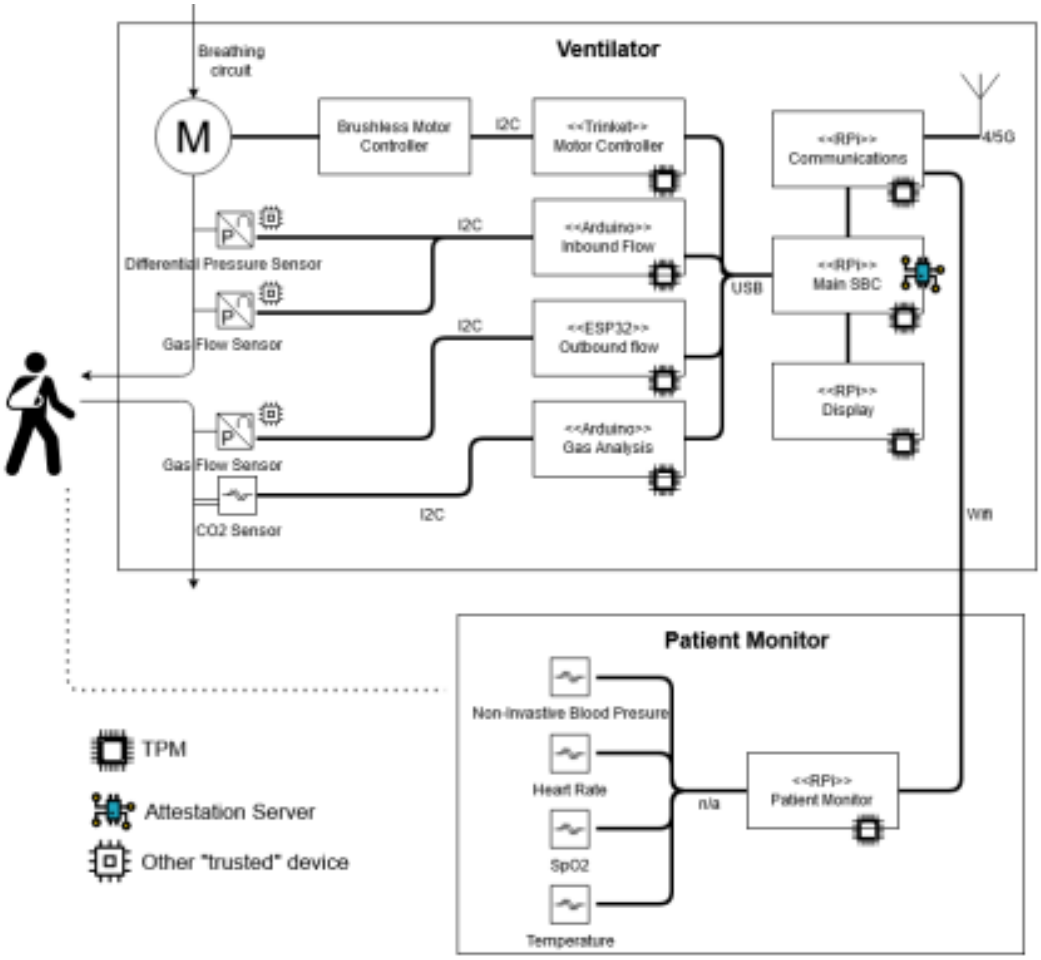

Figure 9 Example of a ventilator with trust components (Oliver, 2020)

A remote attestation (RA) mechanism (Oliver et al., 2019, Turcanu, 2021 & Risto, 2023) is integrated. The RA is responsible for providing operations for attesting and verifying the integrity of the firmware and software of the ventilator by involving components such as TPM. During a ventilator's lifecycle, several events can cause a change in its configuration. Examples of such events could be occasional over-the-air updates or physical setting modifications, for example, airflow pressure initiated by a patient. Any change in the ventilator's mode of operation typically changes the device's configuration and may initiate a remeasurement, such as a restart, of the ventilator. In case of a restart, information on the event is collected and updated in the boot log and PCRs accordingly.

This proposal suggests two approaches for attestation: attestation records and blockchain records. The RA obtains a quote from the TPM indicating the state of the ventilator (PCRs and boot log) and verifies it against predetermined expected values and other desired policies

on the attestation server. The expected values refer to a set of values that indicate the state of the device in stable situations. In typical scenarios, the expected values are delivered by the manufacturer. Furthermore, the attestation record can be cross-referenced against a blockchain record that is expected to be a twin to the attestation record and contain the same values. The constitution of the records is discussed in the following Chapters.

The verification process can capture alterations between the quoted and expected values from both environments, indicating changes in the ventilator's configuration and expected state. For example, in scenarios where a device experience multiple reboots and contains variations in the TPM's PRCs. These variations can be used to detect that the patient is acting maliciously, the device may be compromised, or it is not what is claims to be.

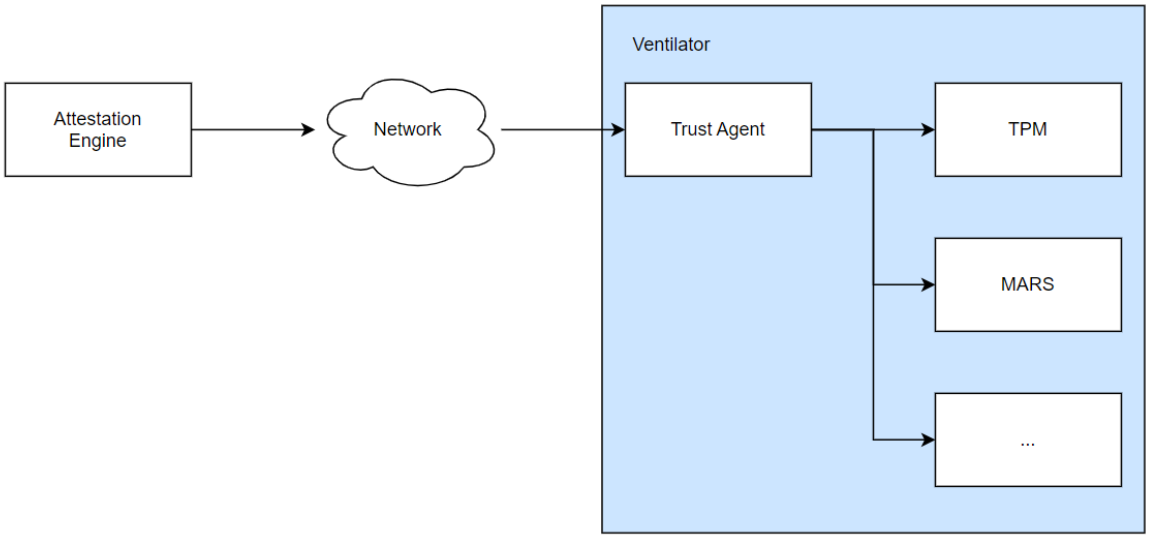

Figure 10 Medical device attestation architecture

Figure 10 illustrates the proposed ventilator attestation architecture. The given architecture consists of a library layer providing the attestation, verification, and element management services, a services layer providing external interfaces, and a trust agent providing access to the necessary information for attestation.

3.3 Data Models

The data model in Figure 12 illustrates the relationship of real-world elements in the proposed medical system. The elements are mapped to the blockchain elements by utilizing the given model.

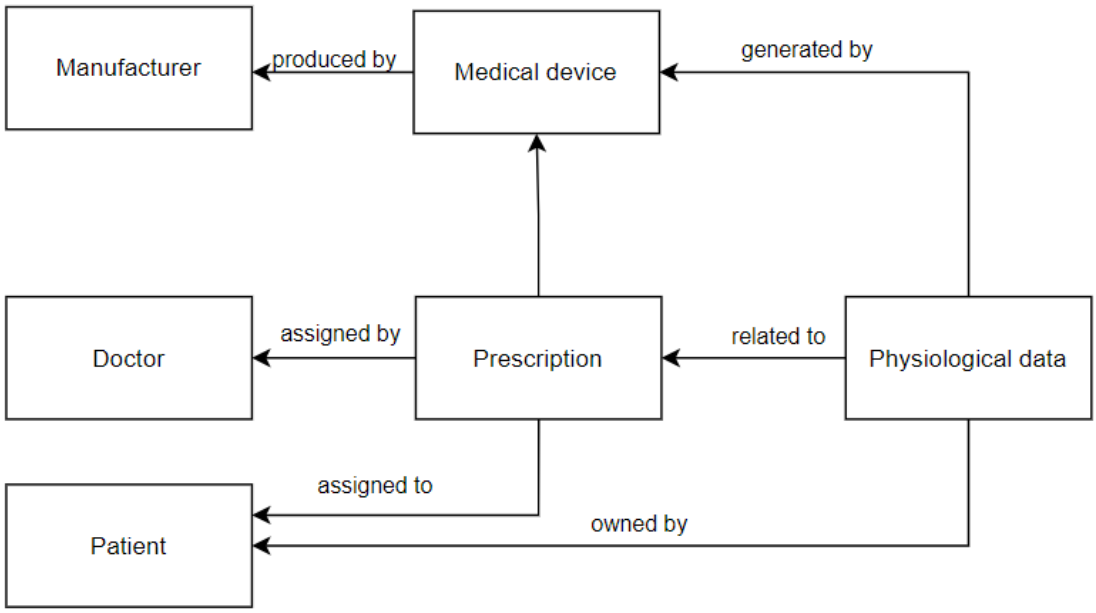

Figure 11 Data model of the proposed medical system

As illustrated in Figure 11, data generated by the ventilator is provided in the context of the user, associating that user identity with that data in such a way that there can be no dispute over the provenance of that data against the device itself and the patient using that device. Furthermore, any item of data can be cross-referenced with the given ventilator, either directly through the key names/public parts, or via the references given in the data structure to the prescription and physical machine. When data is read from the blockchain, it is possible to test that the data came from that given machine and query the attestation records made at that time from the attestation server itself.

Table 2 summarizes the real-world elements that are represented ad NFTs on the blockchain. These elements match with the properties of NFTs, including ownership, minting, and

transferability, which makes them suitable to be represented as NFTs. The elements are discussed in detail in further sections.

Table 2 Summary of elements

Asset type	Contract ownership	Data structure	Data content
Medical device	Manufacturer, transferred to a healthcare operator (doctor)	NFT/ smart contract	deviceID, a hash of the attestation quote, doctorID
Prescription	Doctor, transferred to patient when minted	NFT	doctorID, patientID, prescription ID, device ID
Physiological data	Patient, may be transferred to a third party	NFT	device ID, a hash of the attestation quote, IPFS URL, patientID

3.3.1 Medical Device

Medical devices are provisioned and delivered by manufacturers to healthcare operators. These devices are provided with a record of compliance statement that must be untamperable and auditable. Thus. NFTs is a suitable structure for representing medical devices. The statement of compliance, in this case, is the quote derived from the ventilator's TPM, which provides information on the device's identity and integrity.

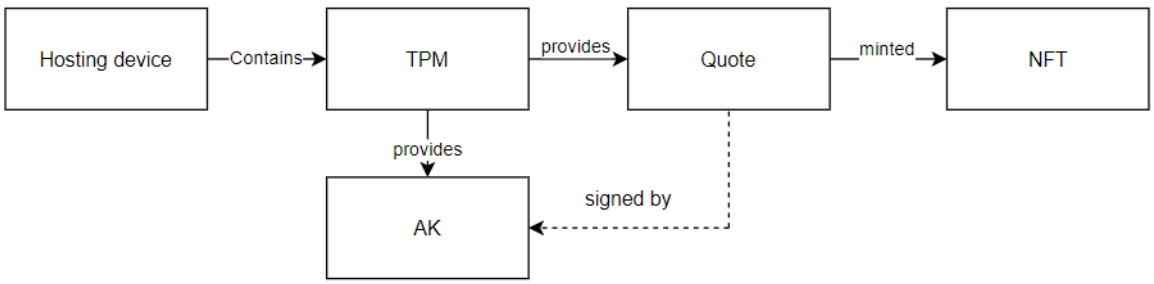

Figure 12 The process of linking a device with NFT

Figure 12 illustrates the proposed mechanism for establishing a link between a ventilator and an NFT structure. The quote, signed by the AK derived from the TPM is stored in NFT. This process ensures that each entry on the blockchain contains a record of the device state derived at the point of the creation of the data entry, corresponding simultaneously to an entry in the real-world attestation environment.

The manufacturer confirms the device's state at the moment it is dispatched from the manufacturer. This action is equivalent to the minting operation, which ensures no record alterations are possible after the current point in time. When the device is handed over to an authorized medical operator in the real world, the token ownership is transferred from the manufacturer to the medical operator. In this case, the notion of ownership claims the manufacturer and the entity responsible for the ventilator at a certain point in time. Through this process, the medical authority is able to audit the state of the device at the point in time the device is dispatched from the manufacturer (e.g., the expected state) and verify it against the given information.

3.3.2 Prescriptions

Prescriptions are NFTs due to the requirements to become untamperable and auditable. A prescription represents a record written by a doctor that contains information related to a specific medical procedure. This process typically involves assigning a patient and a medical device to the prescription. Table 3 below displays an example of data elements associated with a prescription.

Table 3 Prescription data elements

Property	**Value**
doctorID	Doctor’s account identifier on the blockchain
patientID	Patient’s account identifier on the blockchain
prescriptionNotes	Description of the treatment
deviceID	Blockchain address of the device in question

The prescription is signed by a doctor in order to make it a valid medical document. The signing operation is equivalent to the NFT minting operation, which ensures that the content

of the prescription can no longer change. The ownership property is leveraged to denote the entity that has the authority over the prescription at a certain point in time. As only the owner of an NFT can mint, it is logical that the owner of the NFT should be the same as the issuer of the prescription. When the prescription is issued to a patient in the real world, token ownership is transferred from the doctor to the assigned patient. As a result, the patient preserves the right to transfer the NFT.

3.3.3 Physiological Data

Physiological data is an element that is generated and delivered by a medical device. These data records must be untampreable and traceable to the prescription and patient using the device. Therefore, the prescription data element behaves similarly to the previous elements utilizing NFT structures. Table 4 below displays an example of the data elements associated with the physiological data.

Table 4 Physiological data elements

Property	**Value**
deviceID	Blockchain address of the device in question
prescriptionID	Blockchain address of the prescription
patientID	Patient's account identifier on the blockchain
physiloigcalData	Physiological data set including physiological metadata
owner	Patient's account identifier on the blockchain
signature	Signature of the physiological data generated by the TPM

Once the medical device generates the data, it is signed by the TPM, after which it cannot be modified. This operation is equivalent to the minting operation that ensures the record cannot be altered from this point forward. In this scenario, the notion of token ownership refers to the patient's ability to make decisions concerning the future use of the data.

3.4 Operations

As stated in previous sections, this work aims to establish an environment where data integrity is maintained throughout its lifecycle by systematically referring elements to each other. Figure 14 illustrates the relationship and operations between the entities in the context of the medical environment.

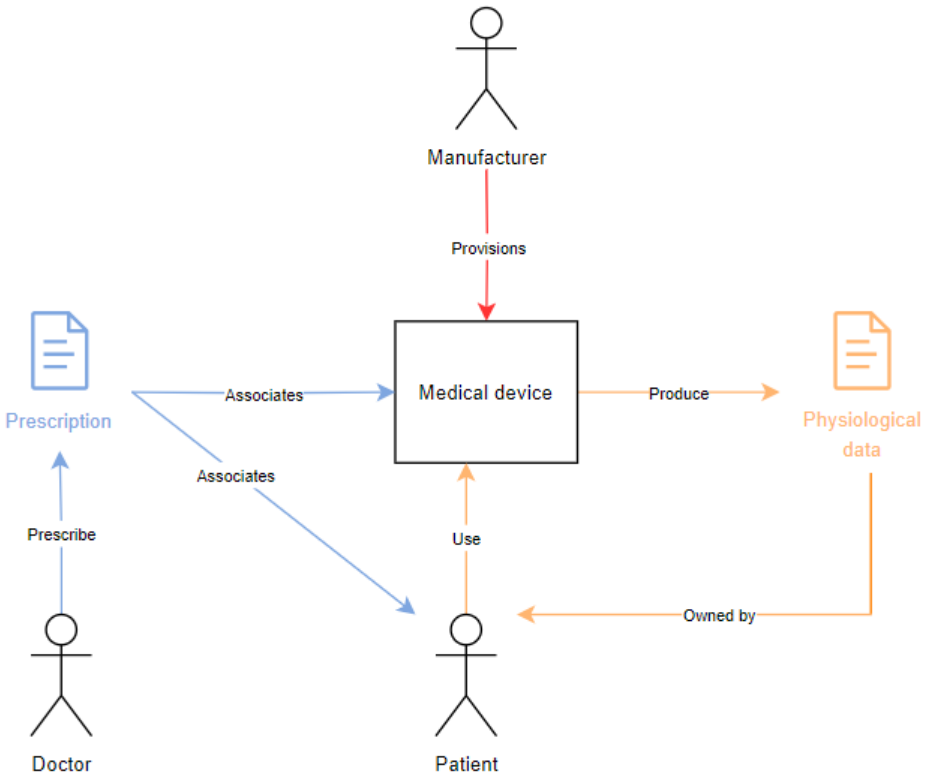

Figure 13 Operations between the entities in the proposed medical environment

As depicted in Figure 13, the application contains a number of operations, each explained in more detail in the following sections. The primary operations discussed in this work are the manufacture and provisioning of the ventilator, doctor-patient interaction with the creation of a prescription (involving said ventilator), use of that medical device by the patient and data collection thereof, and potential trading scenarios for the data produced.

3.4.1 Provisioning

The first process addresses device provisioning executed by medical device manufacturers. Provisioning is a process that is typically conducted before a medical device is supplied to the medical authorities. With the provisioning procedure, the manufacturer aims to create an authoritative record for the device that serves as a statement of compliance. Provisioning enables the creation of artifacts such as software and hardware bill of materials and the detection of changes in the device system.

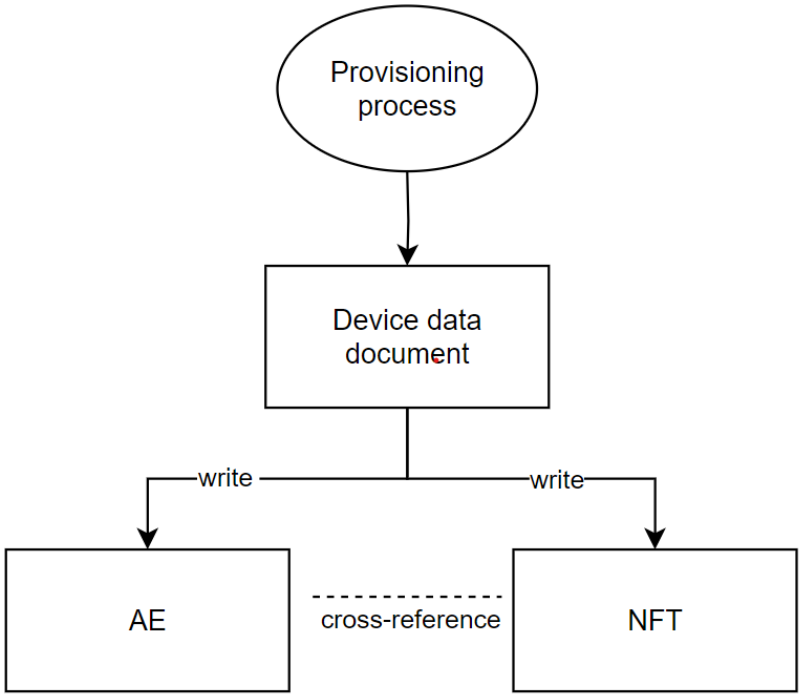

Figure 14 Device provisioning process

The manufacturer's device provisioning process is shown in Figure 14. The provisioning process is responsible for deriving relevant information about the medical device's identity and integrity. The information produced includes device identification (for example, using cryptographic keys derived from the TPM), integrity measurements of firmware and software recorded in the TPM, and other relevant information as required. Once the relevant data of the medical device is obtained through provisioning, the data is entered into a real-

world attestation environment and blockchain environment. In each environment, an identifier for the data instance is obtained and cross-referenced against each other.

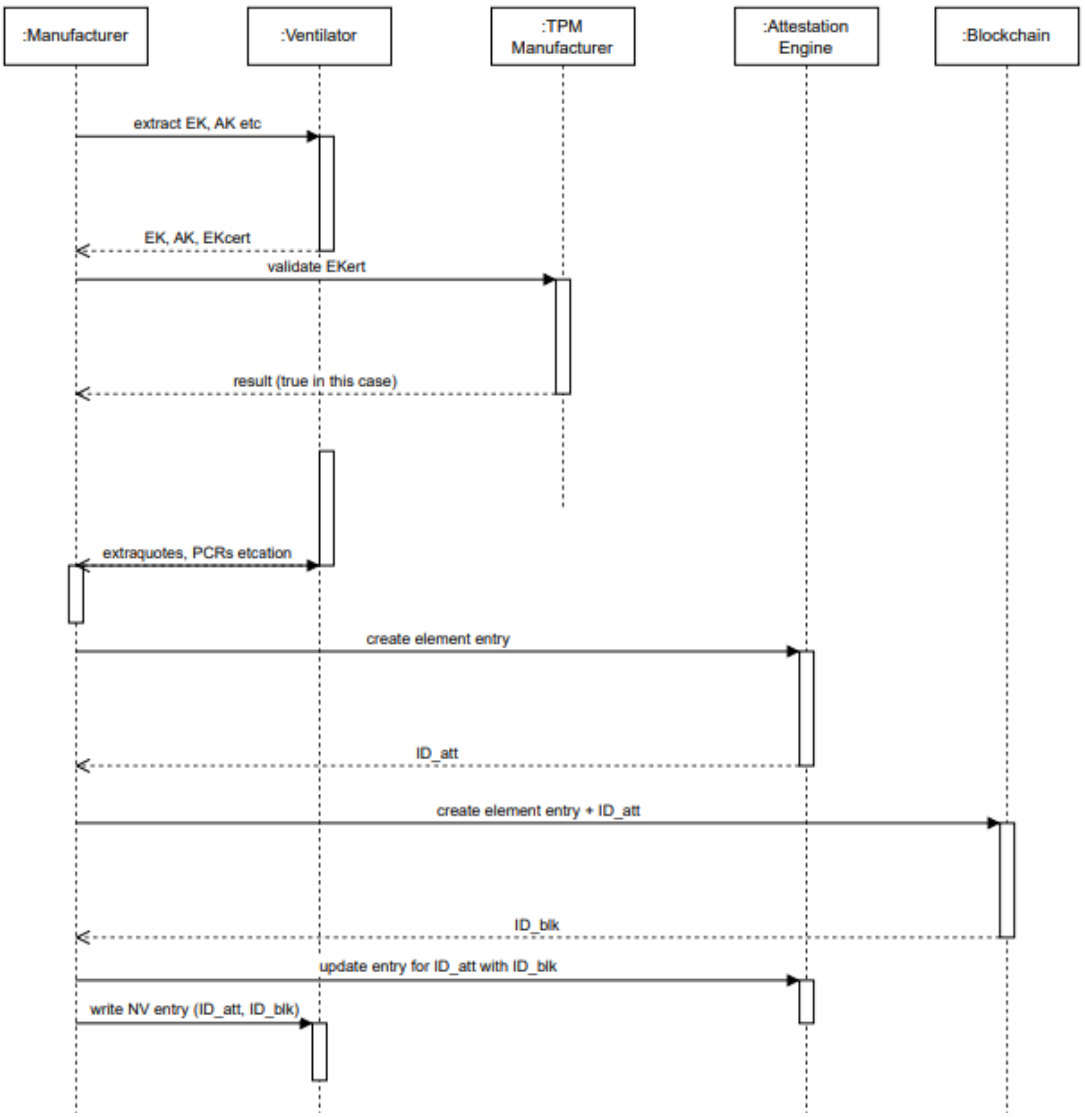

Figure 15 Medical device provisioning process

Figure 15 illustrates an example of the provisioning process. The first step of provisioning is the establishment of device identity. The device's endorsement key is generated, and the attestation key is derived from that. TPM manufacturers typically place the EK certificate signed against their manufacturer certificate authority keys on the TPM additionally. This allows verification of the authenticity of the TPM.

In the next phase, a request is made to the AE to create a new element entry. The entry contains information such as the obtained identity information (keys) and other obtained measurements (quotes) related to the integrity of the device, for example, PCR values. Once the registration is completed, the AE returns an identifier value (ID_att) for the device. Similarly, the medical device's measurements and ID_att are recorded in the blockchain environment (BE). In this process, an entry is created to the BE requesting data to be encoded and minted as an NFT. At the BE, the minting operation is conducted immediately as it is desired that the state of the token cannot be changed afterward. After the NFT minting operation, an identifier ID_blk is returned that corresponds to the entire set of data stored in the BE. The entry in AE is updated with ID_blk along with ID_att. Finally, the identifiers ID_att and ID_blk are recorded in the TPM's NVRAM.

The attestation engine drives the later attestation processes by communicating with a trust agent on the device to request identity and information from the root of trust for reporting, in this case, a TPM. When a customer obtains a device, this can be cross-referenced against the data stored in an immutable form on the blockchain. Ideally, the two records should be the same initially; but any changes can be checked and verified that these changes are valid over time. In one case, it is now possible to reset the machine to a factory setting and compare this against the original record on the blockchain.

3.4.2 Verification

Verification is a process that can be performed at different points of the device’s lifecycle. For instance, a verification process may be required at a point in time a medical authority receives the device from the manufacturer. Verification enables the confirmation of the expected state or detection of changes in the device system.

In the verification process, the attestation obtains relevant information of the medical device’s identity and integrity. The information obtained includes device identification (for example, the public key), integrity measurements of firmware and software recorded in the TPM, and other relevant information as required. Once the relevant data of the medical device is obtained through the attestation, the data is verified against the expected values registered on the real-world attestation environment and blockchain environment.

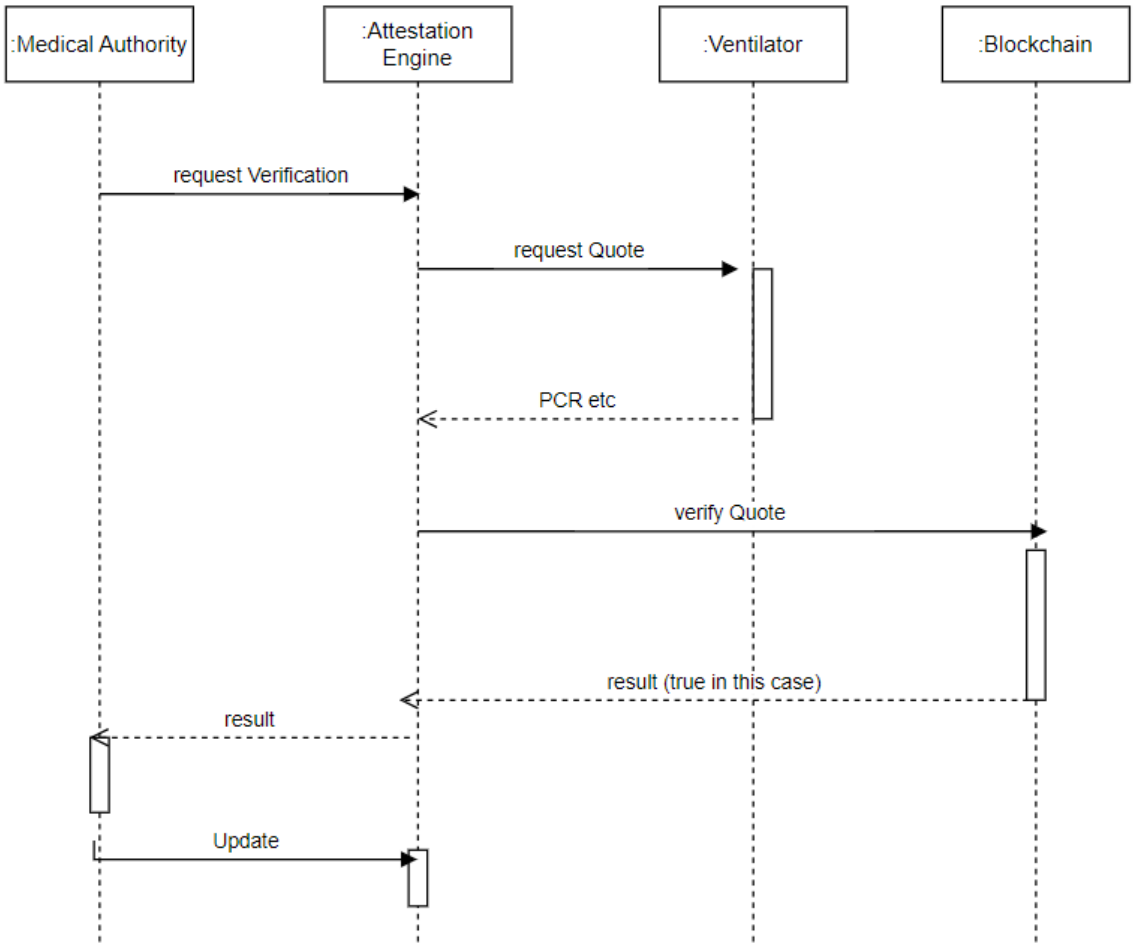

Figure 16 Medical device attestation process

Figure 16 illustrates an example of the verification process. The verification process is initiated by requesting the AE to attest the device. In this process, the AE requests a quote from the TPM onboard the medical device. The TPM quote mechanisms report the values defined by the request, for instance, ID_att, PCR values, clock, and reset information. Once the relevant data is obtained, the TPM signs the quote with its AK.

Once the relevant data of the medical device is obtained through the attestation, the AE performs multiple verifications on the quote, essentially comparing the quote against a set of expected values recorded in the attestation environment. Following the attestation procedure, the NFT associated with the device is derived from the blockchain. The given

quote values are compared against the identity and integrity values (expected values) recorded on the BE during the provisioning process. Based on the verification, the AE concludes whether the device is what it claims to be and is in an expected state. Thus, the two records should correspond to each other for an untampered device. In case deviations are detected, a further forensics operation can be launched. Finally, the decision is updated on the AE, and the output result about the device state is communicated to the medical authority, who makes the final decision regarding the device's integrity.

3.4.3 Operations on Prescriptions

This section addresses the doctor-patient interaction with the creation of a prescription. A number of fundamental operations a doctor can perform on a prescription according to a given process are defined, for example, as shown in Figure 17.

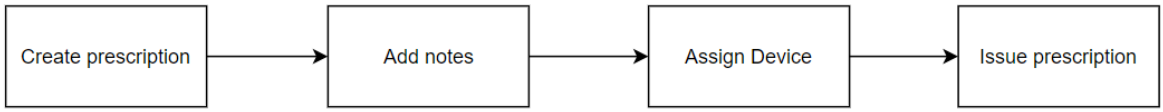

Figure 17 Operations on prescription

A prescription is a record written by a doctor containing information about a specific medical procedure. In this process, a doctor assigns a prescription for a patient. Additional freeform notes can be placed on the prescription, for example, the operating mode of the medical device on the prescription. The operating mode can refer to the volume of the oxygen input and output of the device during the treatment.

The doctor assigns a medical device to the prescription, such as the CPAP device discussed in the previous sections. In this proposal, the process is extended by attesting and verifying the medical device's state before assigning it to the prescription. Furthermore, certain requirements must be met for the assignment to take place, including provisioned device, ownership of the NFT representing the device associated with the doctor in question, and the device being in an expected state. Moreover, an attestation process is conducted, as described in the previous section, before the device can be assigned to the prescription.

The prescription process is completed when a doctor issues the prescription. In this process, the NFT minting operation is conducted, which records the prescription data as an NFT on the BE. The minting operation is conducted immediately as it is desired that the state of the token cannot be changed afterward. Once the minting operation is completed, the BE returns an identifier value corresponding to the prescription data stored in the BE.

3.4.4 Medical Data Generation

This section addresses the use of the medical device and data collection. Prior to medical treatment, a patient receives the medical device from the medical authority. At this point, the device is expected to be provisioned, and all the previous steps discussed are completed. As stated earlier, the state of a medical device can be verified at different points in time. In this scenario, the device must provide information about its state before the patient can operate it.

Once a patient logs onto a medical device, the prescription, which the patient owns, is obtained from the blockchain. Relevant device identifiers are then extracted from the blockchain record and verified by the AE. Thus, certain requirements must be met before the device can be operated, including the device being in an expected state and a correct patient using the device. Moreover, the AE verifies the device's identity by requesting information on the identity from the TPM and then cross-referencing the ventilator's identifiers claimed on the prescription against the ventilator's identifier recorded on the AE and the blockchain record representing the ventilator. Following the verification procedure, the AE performs an additional state check by attesting the ventilator, as described in the above sections. An example of the data generation process is illustrated in Figure 18.

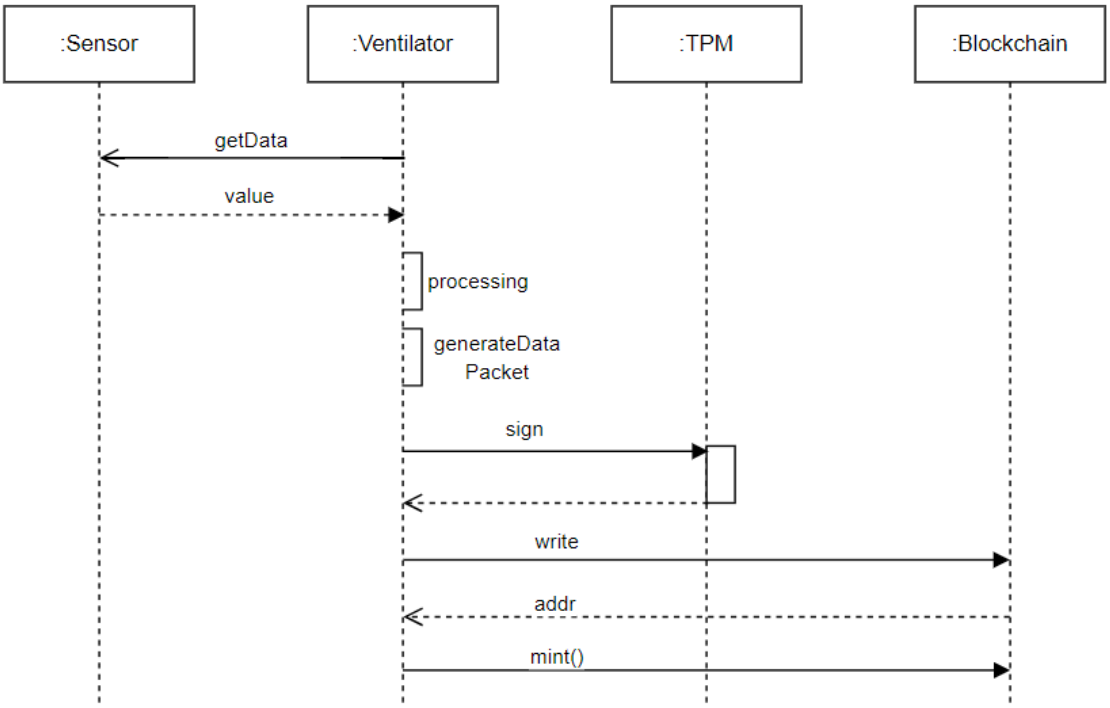

Figure 18 The process of data generation

The data generation process is responsible for collecting physiological data from the patient as required and recording the data instance and the device state to the blockchain environment using similar data structures as discussed in Chapter 3. In this process, the ventilator captures various physiological data (for example, gas flow, NID3, and SpO2) from the patient. For convenience, these values can be collected over five seconds. A quote of the configuration of the medical device is taken, and the quote and data set are cryptographically hashed and signed with the same private key that was used to construct the quote. This process is repeated throughout the medical procedure.

Table 5 shows an example of the data produced by the ventilator. Once the data set is generated in the given interval, BE is requested to encode and mint the data set as an NFT. At the BE, the minting operation is conducted immediately as it is desired that the content of the records cannot be changed afterward. This process ensures that data can be cross-referenced with a given medical device. The referencing can be conducted directly through the key names and public parts or through the references in the data to the prescription and medical device. When data is derived from the blockchain, it is possible to verify that the given machine generated the data by querying the attestation records.

Table 5 Contents of the physiological data

Parameter	Value
start time	Indicates the start time of the operation
End time	Indicates the end time of the operation
Duration	Indicates the duration of the operation
Number of samples	100
List of samples	Individual datapoint for the measurement
Quote	Integrity measurement structure returned by the TPM of the device
Signature	cryptographic hash of the above data singed by the private attestation key of the device stored on the device's TPM

3.4.5 Medical Data Transfer

One of the properties of NFTs is the ability to change ownership. In the context of the given use case, transfer of ownership can occur in operations such as medical data trading or similar operations. One example of the given operation could be a patient trading the data with third-party data consumers, such as insurance companies requiring medical data for various objectives. In this scenario, the AE is utilized to perform a set of verifications over the data before the data trading operation can occur. An example of such a precondition is verifying data against the attestation server at that point in time to test that the data came from the given medical device that was in a good state.

In order to achieve this, the medical data record is retrieved from the blockchain, from where the physiological data and its quote and signatures are extracted. The AE is queried to establish the ventilator's state at the point in time the physiological data was generated. The AE verifies the quotes and signatures from the physiological data record. Following the verification, the AE outputs a decision concerning the state of the device. In this example, the transfer cannot continue unless all the physiological data was generated a known machine in a known good state at point in time the physiological data was generated. This provides

guarantees that the data is related to the correct machine, the data has not been tampered and the new owner gets valid data.

3.5 Blockchain Architecture

In this proposal, medical applications are constructed as decentralized applications, the unit of construction of a blockchain application, with each application implementing one individual block of functionality. These blocks are based upon the data model in Figure 11. As defined in the data model, the application contains four individual functionalities: device provisioning, doctor-patient interaction with the creation of a prescription, data collection, and data transfer. The NFT ERC-721 standard from Ethereum is utilized as the basis of the structures entered onto the blockchain. In this experiment, there are no implementations of authentication mechanisms or other functionality for simplicity.

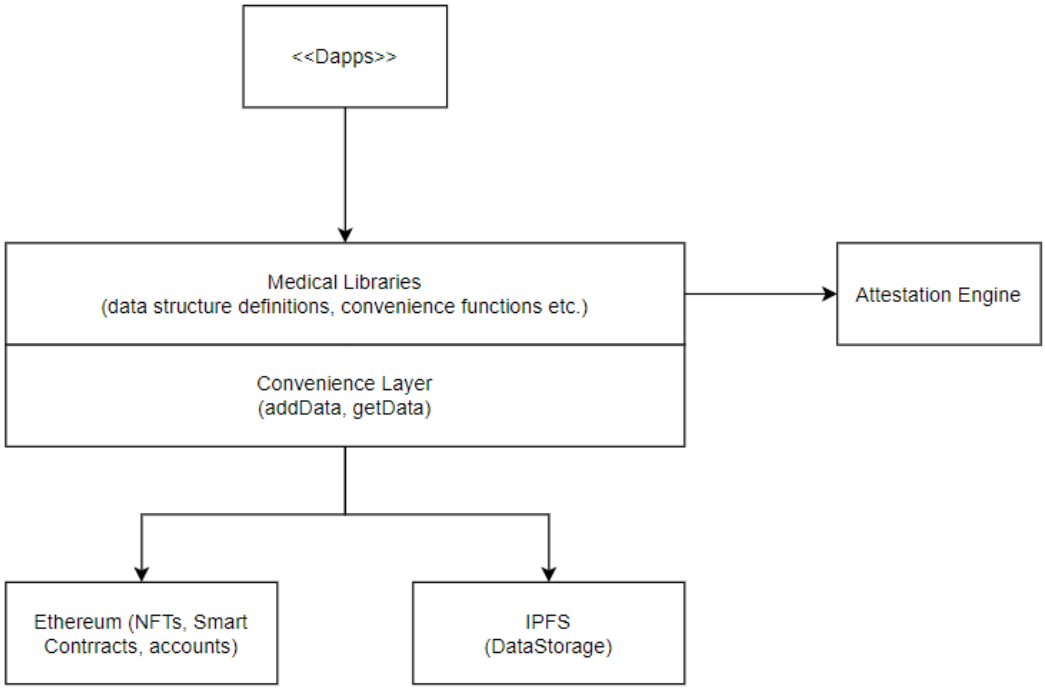

Figure 19 The system architecture

Figure 19 illustrates the system architecture comprising five operational layers: user interface, medical libraries, convenience layer, Inter Planetary File System (IPFS), and blockchain. IPFS is used to store large amounts of data, which is neither possible nor practical in the ERC-721 structure. A convenience library is constructed to hide these functionalities. Further convenience functions related to specific medical operations are provided in the further library. This library is where the interactions with remote attestation take place.

4 Implementation

To demonstrate the implementation of a system with the properties discussed in Chapter 3, a simple proof-of-concept of a medical system that utilizes trusted computing principles and remote attestation is established. The experiment involves establishing a medical application on the Ethereum blockchain infrastructure.

4.1 Trusted Infrastructure

A ventilator based on a modified CPAP device is constructed with a TPM and related infrastructure, as defined by Oliver (2020). The medical device is implemented using a Raspberry Pi 3B as its main board, including a display, two Sensirion SFM3000 flow sensors driven by Arduino Nano boards, a small brushless motor controller, and a brushless motor from a commercial CPAP device. To perform a measured boot, the Pi runs Raspbian with TPM drivers and a modified WolfBoot boot loader. The Raspian kernel is compiled with Linux IMA to perform file system integrity monitoring and report values to the TPM additionally. An example of the ventilator is shown in Figure 20.

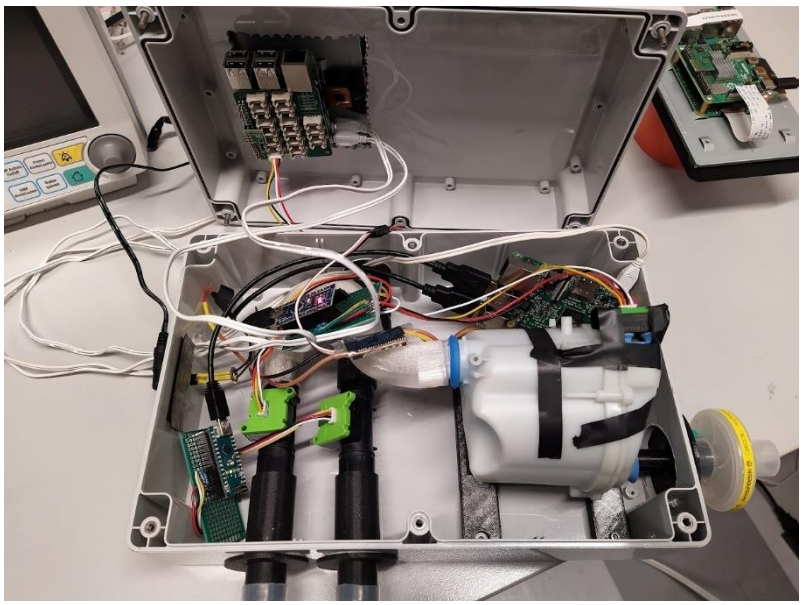

Figure 20 Trusted ventilator

Nokia Attestation Engine (NAE), based on work done by Turcanu (2021) & Risto (2023), is used to provide attestation services, such as attestation, verification, and element management (Nokia, 2023). The attestation engine runs the attestation processes by communicating with a TPM on the ventilator to request identity and information from the root of trust for reporting.

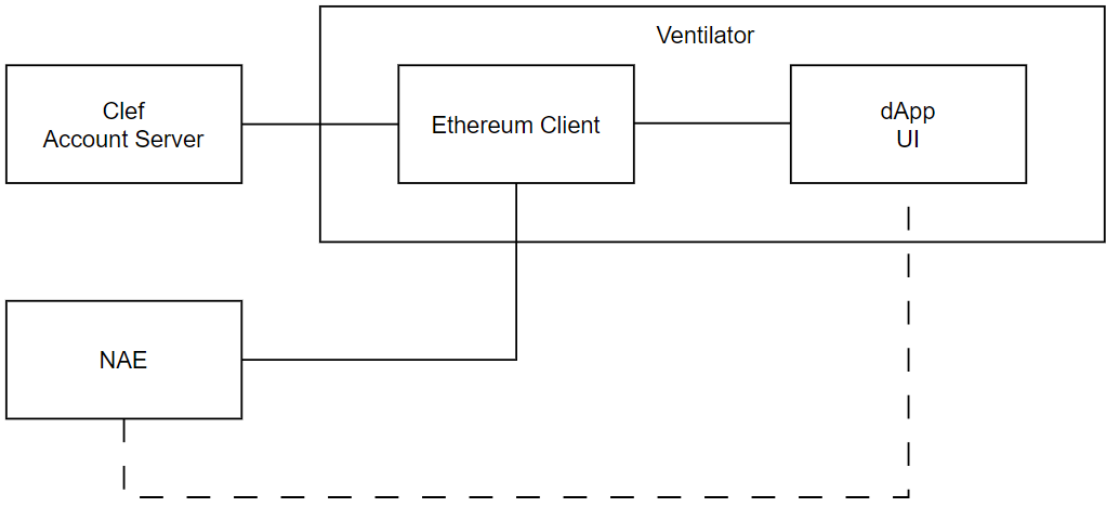

Figure 21 Proposed blockchain architecture

The architecture of the blockchain implementation is shown in Figure 21. A private Ethereum (Dannen, 2017) installation is utilized to enable the blockchain infrastructure, which is deployed across required devices. In the given system, the blockchain accounts are provided by utilizing Clef. Raspberry Pis run with light eEthereum nodes and are not involved in mining processes. The interactions between the attestation engine and the smart contracts are made specifically for this experimentation. In future works, the utilization of Ethereum oracles could be considered.

4.2 Device Provisioning

This section examines the ventilator provisioning process, concentrating on the steps involved in enrolling and verifying the ventilator with the attestation engine and recording the related information as an NFT on the blockchain. A provisioning tool is used in the provisioning process, which follows the process introduced in Chapter 3. The AE interacts with the TPM to obtain identifying information on the medical device. The AE derives an EK from the TPM, after which a signing-only AK is derived from the EK. The process is extended by generating a TPM quote for a given set of PCRs, as seen in the example in Figure 22.

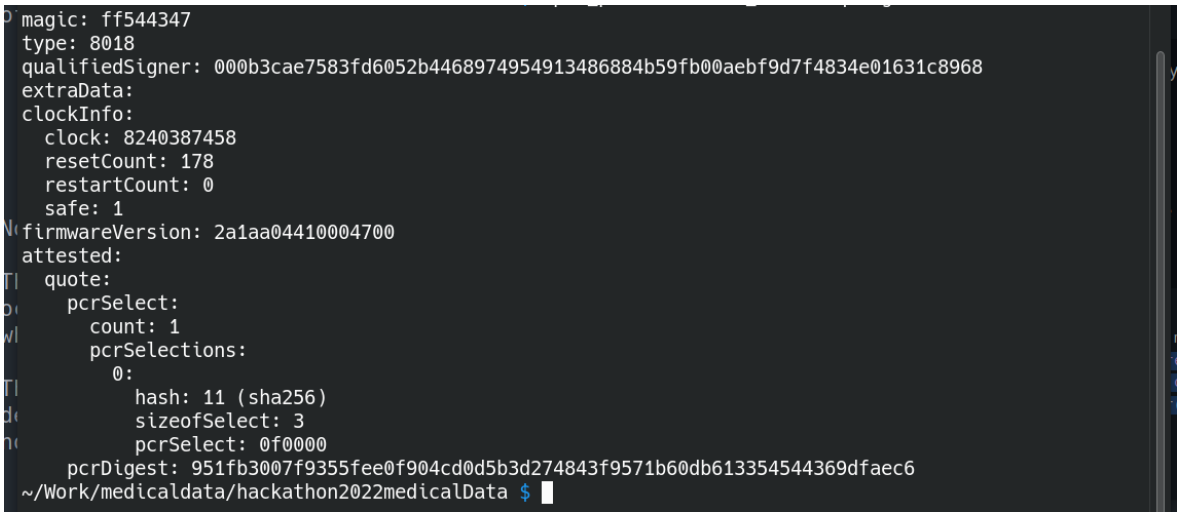

Figure 22 Example of a quote

The selection of PCRs is based on a set of predefined policies provided by the AE. A policy implies AE, which PCR values must be requested from TPM. In this case, two sets of quotes are derived, one for system configuration and one for medical software configuration. These correspond to PCRs 1-5, as presented in Table 6. For example, PCR 0 is a hash of the firmware binary, PCR 1 is the firmware configuration, and so on. PCR 4 and PCR 5 hold ventilator software and configurations in this case.

Table 6 PCR Usages

PCR	Usage
0	Firmware binary
1	Firmware configuration
2	Kernel
3	Kernel and device tree configuration
4	Medical software
5	Medical software configuration

With the given set of integrity (PCRs) and identity (EK, AK) information about the device, the AE generates a new entry considering the device on the AE server. This resulting record for the ventilator appears on the attestation UI for the user, as shown in Figure 23.

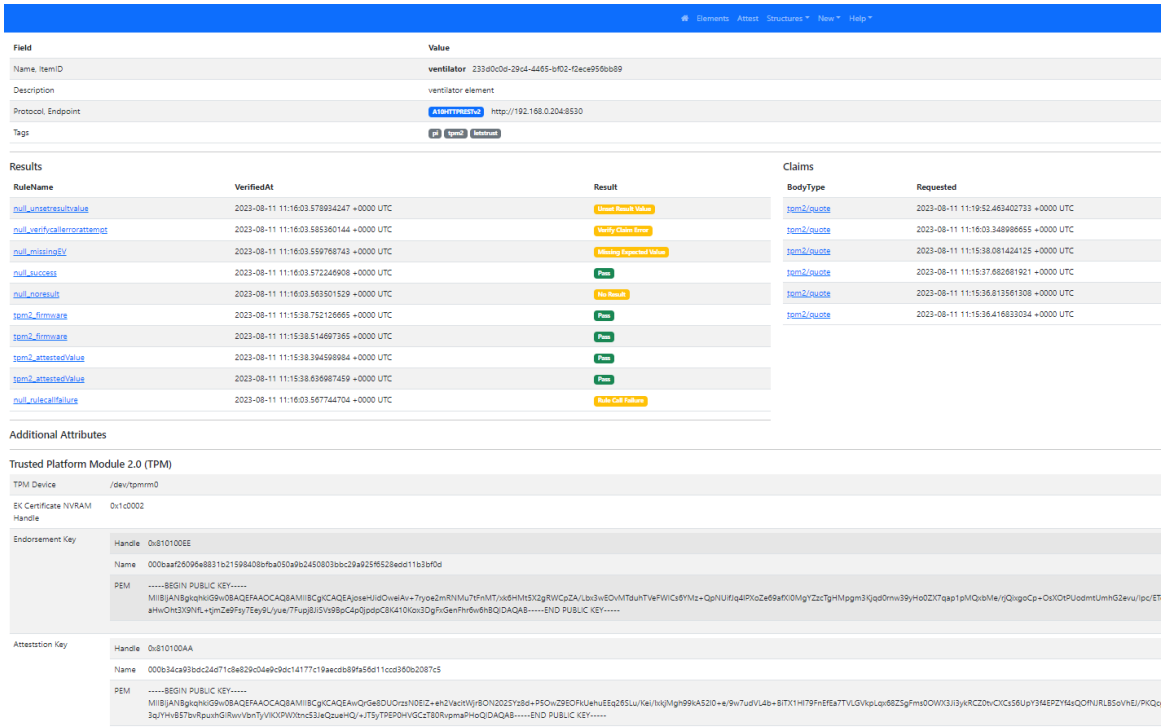

Figure 23 Ventilator entry in NAE

Figure 23 shows the attestation UI view of the information associated with the medical device. The information contains the metadata related to the given device and the TPM responsible for attesting it, including TPM identifiers, such as AK and EK. The AE generates

a unique identifier itemID for the device within the attestation environment. In addition to the device specifications, an overview timeline for previous verification results can be depicted from the UI.

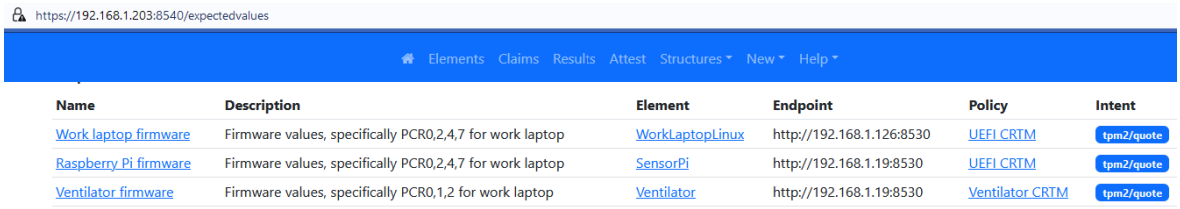

Figure 24 Expected values in NAE

Accordingly, the provisioning process establishes a set of ‘expected values’ for different elements as shown in Figure 24. The expected values represent the measurement of TPM of the medical device in a good known situation. The medical device should confirm to these values later in verification process.

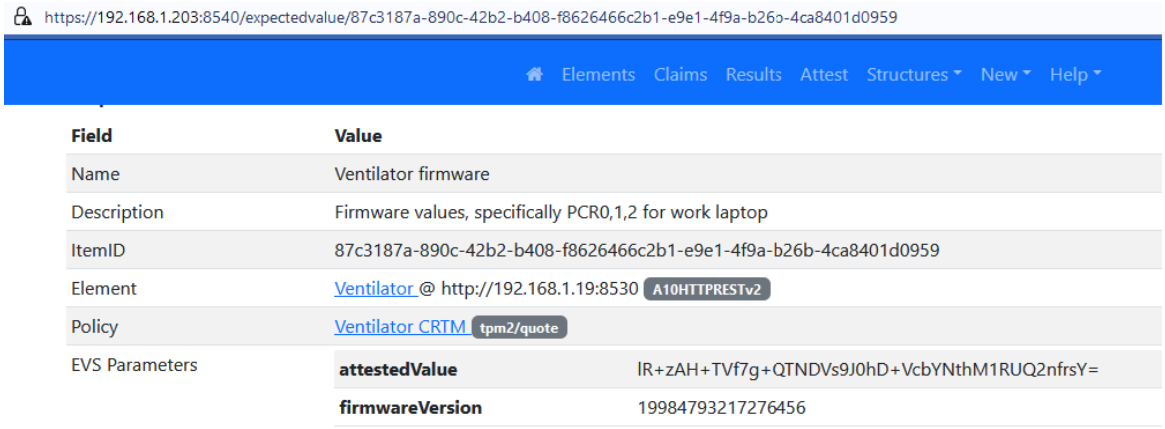

Figure 25 Ventilator expected values in NAE

Extending the above, Figure 25 shows the expected values specifically for a ventilator. For example, in this scenario, the attested value is a hash of a digest of the given PRCs determined by the policy.

4.3 Attestation

This section examines the device verification process with the attestation server as defined in Chapter 3. The ventilator's trust and expected state are checked at critical points during the life cycle of the ventilator. At the attestation operation, the attestation server queries the ventilator's TPM against a predefined attestation policy, according to which an attestation claim is formed. The verification process continues to compare the claim against the given expected values for the ventilator. A new entry is generated on the AE each time the device is verified. For convenience, these mechanisms are provided to the user by the UI.

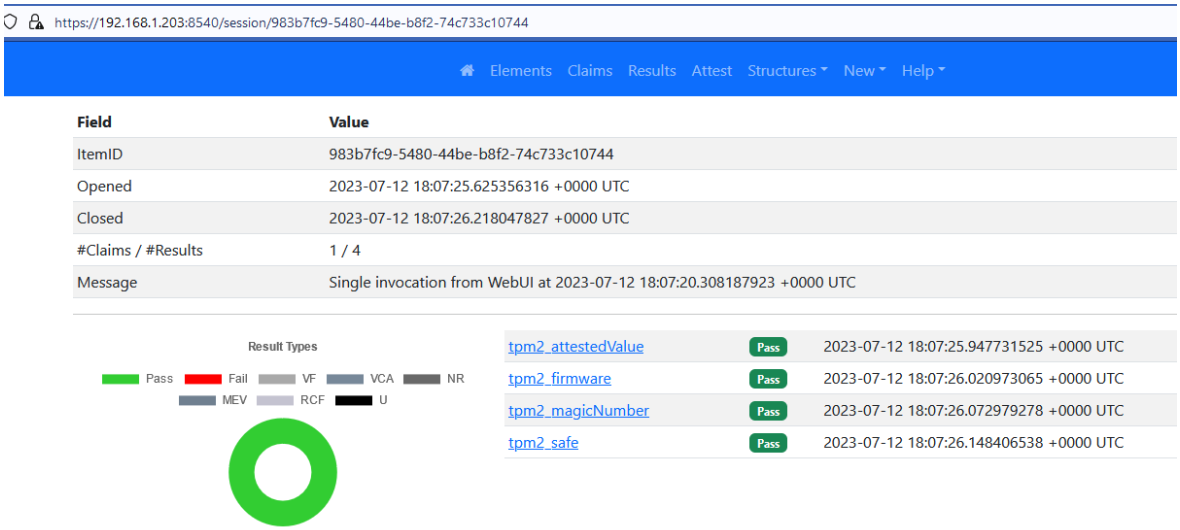

Figure 26 Successful validation in NAE

Following the verification of the state of the ventilator, the AE outputs the information about the subject of verification in the attestation UI, as seen in Figure 26. This summary view demonstrates the output after successful verification against the expected values for the firmware, firmware version, and TPM quote structures (magic number and safe). The most important values to examine are under the green tags indicating a successful verification of the given components.

4.4 Prescription

This section examines the process of assigning a prescription as defined in Chapter 4. This process is extended by ensuring that the ventilator is in a known good state before the assignment is made to the prescription. An example of the medical application UI used by medical authorities to upload the information for the prescription is shown in Figure 27.

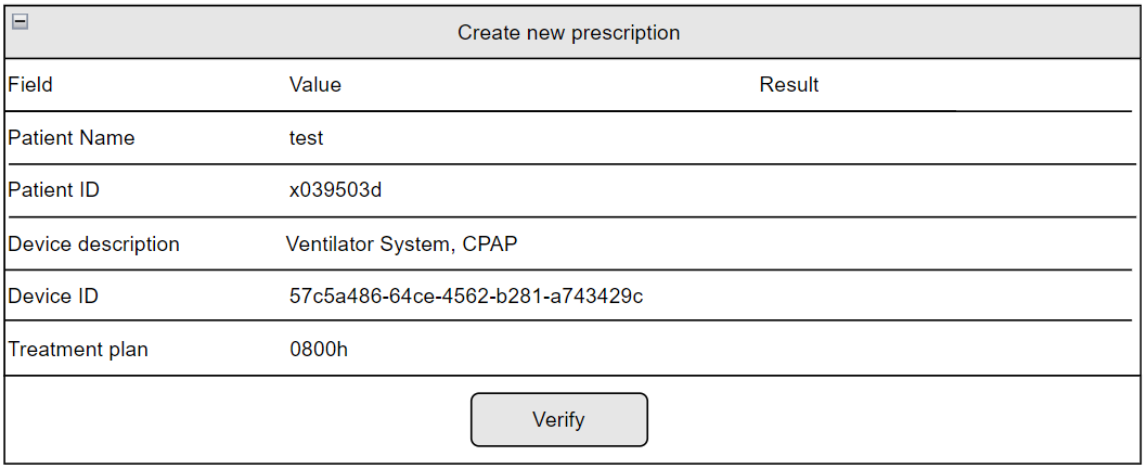

Figure 27 Examle of the medical application UI

The medical authority assigns a patient to the prescription by using the patient's individual identifier. In this scenario, the patient's identity is the blockchain account identifier. In order to assign the given CPAP ventilator, the medical authority inputs the description and identifier of the ventilator. The identifier refers to the blockchain account identifier under which the manufacturer registers the device. The medical authority has an option to input free form notes related to the medical procedure. In this example scenario, the required use time of the CPAP device is added to the prescription.

At this point, the device verification process is triggered. This action requests the AE to perform the attestation and verification process on the device, as discussed in the previous sections. In case the attestation fails, the medical authority receives a warning of the device holding improper software. In a successful verification scenario, the medical authority

receives a message implying a positive outcome of the verification. The outcome of the verification can be seen in Figure 28.

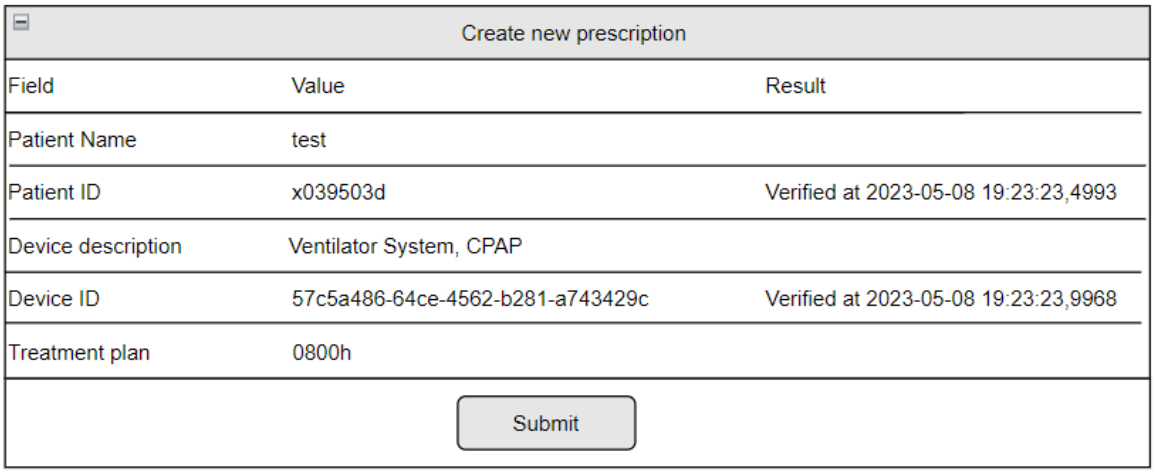

Figure 28 An example of the medical application UI after verification

Following the verification, the verification result appears on the UI view, as seen in the example in Figure 28. Due to a positive verification result, the doctor can proceed to take additional actions or submit the prescription. The submission of the prescription initiates the NFT minting function, after which the information on the prescription is recorded on the blockchain and can no longer be adjusted. This transfers the ownership of the prescription from the doctor to the patient.

4.5 Medical Data Generation

An attestation operation is initiated when a patient logs onto the ventilator, as depicted in Algorithm 3. During this operation, the correct prescription owned by the patient is retrieved from the blockchain from where the device record is derived. The information is cross-referenced against the ventilator's identifier address recorded on the AE and the NFT representing the ventilator.

The verification operation performs an additional attestation using the AE against the ventilator, as described in the above sections. After the device state and the patient-device

relationship are verified, the ventilator outputs a message that informs the patient to continue to operate the device.

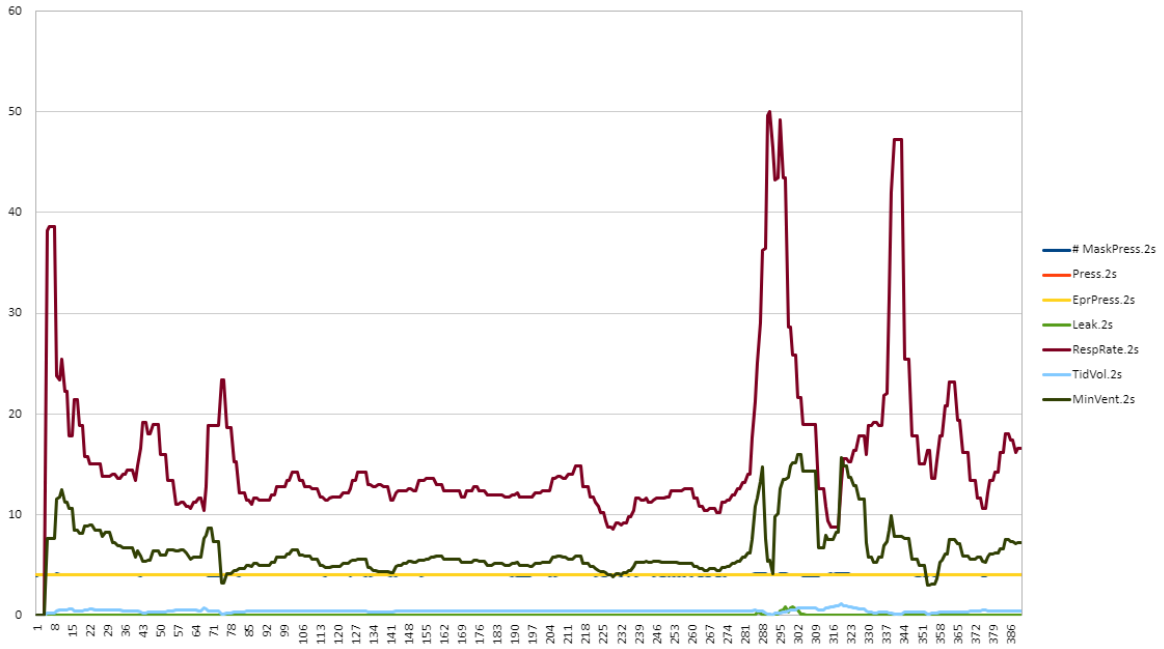

Figure 29 An example data sample generated by a trusted ventilator.

Figure 29 shows a sample of the physiological data batch produced by the ventilator. In this implementation, the ventilator's sensors are sampled at 20Hz. The generated values are batched together in 5 second chunks and minted as NFTs. Included in this data is a quote provided by the ventilator's TPM. The quote indicates the state of the device at the point in time the data is generated. The TPM is commanded to sign the given set of data with a signing key (e.g., the AK) onboard the TPM.

The given structure can be verified against the AK's public part, which is stored on the remote attestation server. An example of the verification of the signature against the TPM's attestation key is shown in Figure x. This process would be hidden from the user of the system.

5 Result & Discussion

The literature of blockchain in healthcare area, as presented in Chapter 2, primarily discusses the speculative benefits of blockchain; the discussion does not consider many of the real-world aspects - humans, data, and infrastructure - and how these relate together and produce a medical application. It is often irrationally considered that the blockchain's inherent untamperable and auditable properties provide sufficient trust. This interaction between real-world elements and blockchain must be properly investigated and understood when combining these two environments.

The integrity of the real-world elements represented on a blockchain is a critical factor in establishing systems that combine real-world and blockchain environments. Without sufficient methods to attest and verify the trustworthiness of the devices providing data, the data on the chain becomes unreliable. Ultimately, remarkably little emphasis has been given to data and device integrity and provenance, which undermines the entire concept of blockchain and the business value of these applications. This must be taken into account when considering the application of blockchain systems in critical real-world areas. Motivated by the above, this work considered two research questions. The first research question of this thesis was to find out how blockchain can be applied in real world environment. The second research question considers what technologies can be used to verify the provenance of the data in the blockchain. The following sections aim to answer the research questions.

5.1 Results

The work demonstrated a systematic way of establishing NFT (digital twin) representations of elements that experience state changes in the real world and require attestation capabilities. In the proposed approach, the identity and integrity information provided by the TPM on the device are cryptographically signed and embedded into the NFT data structures. Data stored on the blockchain becomes cryptographically linked to its real-world source in a way that tampering is impossible, as illustrated in Figure 30.

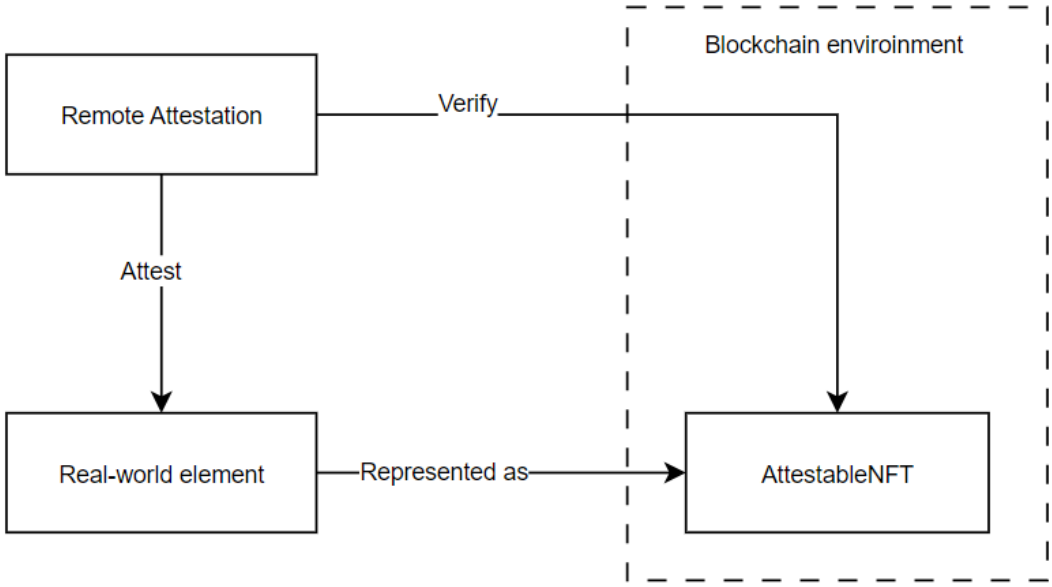

Figure 30 Concept relationships

One of the responsibilities of remote attestation is to verify the expected state of the real-world element by cross-referencing the identity and integrity information of the device to the equivalent information on the blockchain. As demonstrated in the research, the proposed mechanism establishes more rigor on the data provenance, which sets premises for the identification of improper use of the device.

The experiment and use case shown are limited in scope and intentionally simplified. The simplicity of the use case and its operations is an explicit design choice as the emphasis of the work is on integrating attestation with blockchain structures. Consequently, the implementation considered existing blockchain and attestation technologies and mechanisms. This work did not explore the potential of other similar technologies.

This research did not conduct system performance analysis. However, the experiment shows that operations such as quoting, hashing, signing, and creating an NFT require time, which does not support fast data transmission. For example, it was necessary to batch the 20Hz sample rate from the gas flow sensor into larger chunks, for instance, 5 seconds at a minimum. In addition to the above, additional network latencies and blockchain mining

should be considered. This is likely to limit the streaming data and other real-time properties. This is likely to limit the streaming data and other real-time properties.

5.2 Discussion

While the experiment demonstrated in this work is small, the performed experiment confirmed that it is feasible to construct a system that relates real-world elements with integrity technologies to the blockchain. The experiment performed in this work was sufficient to provide a clearer understating of how to construct a blockchain-based medical application. Thus, the experiment allowed the discovery of a number of design patterns related to blockchain applications where a ‘digital twin’ link is required.

The research suggests that the practical purpose of the real-world objects can be used as a guide to align them with the corresponding properties of NFT and is key to understanding how smart contracts are constructed. The meaning of these predefined NFT operations, such as ownership, transferability, and minting, needs to be considered carefully in the real-world context. This is evident, as demonstrated by the prescription and medical data, where the meaning of ownership, transfer, and minting varies regarding the context of the object.

The research demonstrated that objects with properties requiring stability and unchangeability are suitable for NFTs. In contrast, objects that hold dynamic real-world properties and require changeable properties over time best become smart contracts. For example, in the context of the work, devices could also be considered smart contracts as their configuration can change over time, which requires the associated smart contract to be updated accordingly.

Expanding the above, considering the real-world functionality of the objects suggests that each object with a set of operations can be an individual decentralized application within a system. As demonstrated in this work, each operation of the medical objects (e.g., prescription or device) was encoded as an individual decentralized application with clearly defined functionality relevant only to that individual object.

Lastly, the research suggests that integrating remote attestation with blockchain applications could be made using a wrapper to provide a precondition to an operation. As demonstrated in this work, the integration of external resources or devices directly into the blockchain

token operations becomes one of the major limitations. In this experiment, most of this was conducted manually, but it could be considered to be integrated into the token functionality to make the process automatic and transparent. The integration of external capabilities into the token functionality itself suggests a possible extension to the standardized token protocols. For example, Ethereum standards acknowledge the usage of oracles in tokens. However, the implementation of oracles results in performance and security concerns. It remains unclear how this is achieved in a generic manner and is left for future investigation.

When considering further adoption of the proposed system for domains such as healthcare, the use of a distributed system with the properties of a blockchain in a digital twin context with a clearly defined link between the real and blockchain worlds allows for some interesting applications to be built. The proposed system could be adaptable for other industries where security and data provenance are needed. Promising examples of industries with high security requirements could be other medical verticals beyond the use case discussed in this work, amongst other critical infrastructure environments such as aviation, railway, automotive, and IoT systems. In addition to these domains, virtual reality and Metaverse-type use cases that are at least partially based on blockchain infrastructure could be considered relevant.

It should be noted, however, that the overall architecture of blockchain and the required infrastructure are still largely lacking. For example, the implementation lacks viewpoints such as the supply-chain bill of materials, attestation, and provisioning mechanisms to guarantee device security. In the case of medical verticals, the certifications do not take into consideration the security aspects at this time, and the security in the area is primarily achieved through obscurity. Moreover, to support the advantages of the proposed system, a suitable blockchain and supply chain infrastructure are a few of the aspects that are necessary to be considered in the future.

6 Conclusion

The verification of the authenticity and integrity of data recorded on a blockchain is one of the disregarded challenges within the blockchain environment. It is often irrationally considered that the blockchain's inherent untamperable and auditable properties provide sufficient trust. The current limitations of blockchain to provide a verification mechanism suggest the necessity of extending data provenance verification further back into the real-world infrastructure. However, many of the works in the area fail to consider the necessity of establishing and maintaining a link between real-world and blockchain elements. Recent deployments of blockchain in critical areas handling sensitive data, such as healthcare machines, indicate the necessity for these measures.

The thesis aimed to study blockchain in real-world applications. Motivated by the extensive literature review conducted in this work, this thesis proposed a design and implementation of an application utilizing blockchain and remote attestation technologies. An experiment was constructed to demonstrate the application in a real-world medical scenario. The proposed mechanism systematically collects integrity information from real-world devices and records it as NFTs on the blockchain environment. This information is protected by the blockchain, which creates an immutable history of information related to the device's state. Furthermore, the NFTs become linked to real-world elements in a way that the integrity of the elements can be verified in real-world and blockchain environments through remote attestation.

As one of the first implementations in the area, this thesis provides a practical contribution by providing insight into blockchain application design with the requirement of digital twin-like properties. For industries such as healthcare, the adoption of distributed systems with the properties of blockchain with a well-defined link between the real-world environment and blockchain environments potentially enables interesting applications. However, it should be noted that the overall blockchain infrastructure and application development techniques are largely lacking at this time. These are a few of the aspects that are necessary to be considered in future research. As the application of blockchain technology in the healthcare area is still in its early stages, more research is required to better understand and

assess the actual utility of blockchain. Moreover, it would be interesting to further investigate the design and potential applications of the proposed system.

References

Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. 2019. Blockchain technology in healthcare: a systematic review. Healthcare. Vol. 7, no. 2, pp. 56.

Alkhader, W., Salah, K., Sleptchenko, A., Jayaraman, R., Yaqoob, I., & Omar, M. 2021. Blockchain-based decentralized digital manufacturing and supply for COVID-19 medical devices and supplies. IEEE Access. Vol. 9, pp. 137923-137940.

Altamimi, A. M. & Zriqat, I. 2016. Security and privacy issues in eHealthcare systems: Towards trusted services. International Journal of Advanced Computer Science and Applications. Vol. 7, no. 9, pp. 229-236.

Arcenegui, J. Arjona, R. Román, R. & Baturone, I. 2021. Secure Combination of IoT and Blockchain by Physically Binding IoT Devices to Smart Non -Fungible Tokens Using PUFs. Sensors. Vol. 21, no. 9, 3119.

Arthur, W., Challener, D., & Goldman, K. 2015. A practical guide to TPM 2.0: Using the new trusted platform module in the new age of security. California: Apress Berkeley.

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. 2016. Medrec: Using blockchain for medical data access and permission management. 2nd International Conference on Open and Big Data. IEEE. Pp. 25-30.

Azbeg, K., Ouchetto, O., & Andaloussi, S. J. 2022. BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security. Egyptian Informatics Journal. Vol. 23, no. 2, pp. 329-343.

Baiju, B., Saranya, S., Sriram, D., Rifath Ahmed, M. & Mohammed, A. 2022. Decentralizing Electronic Medical Records on the Blockchain Using Smart Contracts. Journal of Pharmaceutical Negative Results. Vol. 13, No. 03, pp. 311–316.

Bashir, I. 2018. Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained. 2nd ed. Birmingham: Packt Publishing Ltd.

Bhattacharjya, A., Kozdrój, K., Bazydło, G. & Wisniewski, R. 2022. Trusted and Secure Blockchain-Based Architecture for Internet-of-Medical Things. Electronics. Vol. 11, no. 16, 2560.

Buterin, V. 2014. A Next Generation Smart Contract & Decentralized Application Platform. Ethereum White Paper. Pp. 1–36. Accessed 28.08.2022. Available at https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf

Chiacchio, F., D'Urso, D., Oliveri, L.M., Spitaleri, A., Spampinato, C. & Giordano, D. 2022. A Non-Fungible Token Solution for the Track and Trace of Pharmaceutical Supply Chain. Applied Sciences. Vol. 12, no. 8, 4019.

Clauson, K. A., Breeden, E. A., Davidson, C., & Mackey, T. K. 2018. Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare: An exploration of challenges and opportunities in the health supply chain. Blockchain in healthcare today. Vol. 1.

Dannen, C. 2017. Introducing Ethereum and Solidity. Vol. 1. Berkeley: Apress.

dos Santos RB, Torrisi NM, Pantoni RP. 2021. Third Party Certification of Agri-Food Supply Chain Using Smart Contracts and Blockchain Tokens. Sensors. Vol. 21, no.16, 5307.

Entriken, W., Shirley, D., Evans, J. & Sachs, N. 2018. EIP-721: Non-Fungible Token Standard. Ethereum Improvement Proposals. No. 721. Accessed 28.08.2022. Available at https://eips.ethereum.org/EIPS/eip-721

Faisal, T., Dohler, M., Mangiante, S., & Lopez, D. R. 2022. Beat: Blockchain-enabled accountable and transparent network sharing in 6G. IEEE Communications Magazine. Vol. 60, no. 4, pp. 52-56.

Hapiffah, S., & Sinaga, A. 2020. Analysis of Blockchain Technology Recommendations to be Applied to Medical Record Data Storage Applications in Indonesia. International Journal of Information Engineering & Electronic Business. Vol. 12, no. 6, pp. 13-27.

Hardjono, T., & Smith, N. 2019. Decentralized trusted computing base for blockchain infrastructure security. Frontiers in Blockchain. Vol 2, No. 24.

Huynh-The, H., Gadekallu, T. R., Wang, W., Yenduri, G., Ranaweera, P., Pham, Q., da Costa, D. B.& Liyanage, M. 2023. Blockchain for the metaverse: A Review, Future Generation Computer Systems. Vol. 143, pp. 401-419.

Jennath, H. S., Anoop, V. S., & Asharaf, S. 2020. Blockchain for healthcare: securing patient data and enabling trusted artificial intelligence. International Journal of Interactive Multimedia and Artificial Intelligence. Vol. 6, no. 3, pp. 15-23.

Kalla, A., de Alwis, C., Porambage, P. & Gür, G. 2022. A survey on the use of blockchain for future 6G: Technical aspects, use cases, challenges and research directions. Journal of Industrial Information Integration. Vol. 30. 100404.

Kumar, V., Lee, J. & Hu, Q. Non-Fungible Token-Based Health Record Marketplace. 2022. SSRN. Accessed 12.02.2023. Available at https://ssrn.com/abstract=4130876

Maksymyuk, T., Gazda, J., Bugár, G., Gazda, V., Liyanage, M., & Dohler, M. 2022. Blockchain-Empowered Service Management for the Decentralized Metaverse of Things. IEEE Access. Vol. 10, pp. 99025-99037.

Malamas, V., Dasaklis, T., Kotzanikolaou, P., Burmester, M., & Katsikas, S. 2019. A forensics-by-design management framework for medical devices based on blockchain. IEEE World Congress on Services. Vol. 2642, pp. 35-40.

Marchesi, L., Marchesi, M., Tonelli, R. & Lunesu, M. I. 2022. A blockchain architecture for industrial applications. Blockchain: Research and Applications. Vol. 3, no. 4, pp. 2096-7209.

Musamih, A., Salah, K., Jayaraman, R., Yaqoob, I., Puthal, D., & Ellahham, S. 2022. NFTs in healthcare: Vision, opportunities, and challenges. IEEE Consumer Electronics Magazine. Vol. 12, no. 4, pp. 21-32.

Nokia. 2023. Nokia Attestation Engine A10 Github repository. Accessed 07.08.2023. Available at https://github.com/nokia/AttestationEngine

Oliver, I. 2020. An approach to combining medical device fault analysis with trusted computing forensics. IEEE International Conference on Big Data. 1831-1837.

Oliver, I., Howse, J., Stapleton, G., Shams, Z., Jamnik, M. 2019. Exploring and Conceptualising Attestation. In Endres, D., Alam, M., Şotropa, D., Eds., Graph-Based

Representation and Reasoning. Vol. 11530, pp. 131-145. Cham: Springer International Publishing.

Omar, A. S., & Basir, O. 2020. Secure anti-counterfeiting pharmaceuticals supply chain system using composable non-fungible tokens. Blockchain for Cybersecurity and Privacy. Pp. 243-259. Boca Raton: CRC Press.

Pane, J., Verhamme, K. M., Shrum, L., Rebollo, I. & Sturkenboom, M. 2020. Blockchain technology applications to postmarket surveillance of medical devices. Expert Review of Medical Devices. Vol. 17, no. 10, pp. 1123-1132.

Saunders, M., Lewis, P., & Thornhill, A. 2016. Research methods for business students. 7th ed. Harlow: Pearson Education.

Schüpany, M. & Pirker, M. 2022. A Revisit of Attestable Nodes for Networked Applications. Proceedings of the 17th International Conference on Availability, Reliability and Security. New York: Association for Computing Machinery.

Seliem, M. and Elgazzar, K. 2019. BIoMT: Blockchain for the Internet of Medical Things. IEEE International Black Sea Conference on Communications and Networking. Pp. 1-4.

Subramanian, H., & Subramanian, S. 2022. Improving diagnosis through digital pathology: Proof-of-concept implementation using smart contracts and decentralized file storage. Journal of medical Internet research. Vol. 24, No. 3.

Szabo, N. 1996. Smart Contracts: Building Blocks for Digital Markets. Accessed 02.09.2022. Available at http://www.fon.hum.uva.nl/rob/Courses/ Information-InSpeech/CDROM/Literature/LO

Trusted Computing Group. 2019. Trusted Platform Module Library Specification. Part 1: Architecture. Accessed 20.11.2022. Available at https://trustedcomputinggroup.org/resource/tpm-library-specification/

Turcanu, V. 2021 Providing Trusted Computing Services for Multi-access Edge Cloud Computing. Master's thesis. Aalto University, School of Science.

Valeonti, F., Bikakis, A., Terras, M., Speed, C., Hudson-Smith, A. & Chalkias, K. 2021. Crypto Collectibles, Museum Funding and OpenGLAM: Challenges, Opportunities and the Potential of Non-Fungible Tokens (NFTs). Applied Sciences. Vol. 11, no. 21, 9931.

Vijayalakshmi, K., Bushra, S. N., Subramanian, N., & Ponnuramu, V. 2022. Blockchain based Medical Record Storage and Retrieval using NFT Tracking System. IEEE 6th International Conference on Trends in Electronics and Informatics. Pp. 01-08.

Wang, C., Dohler, M., Lopez, D., Forbes, R., Steiff, S., Faisal, T., Mary, S. B., Liu, Q. and Arribas, I. 2022. An Introduction of Permissioned Distributed Ledger (PDL). ETSI White Paper. No. 48. Accessed 01.02.2023. Available at

https://www.etsi.org/images/files/ETSIWhitePapers/ETSI-WP48-PDL.pdf

Wang, Q., Li, R., Wang, Q., & Chen, S. 2021. Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. Digital preprint at arXiv:2105.07447.

Wang, S., Yuan, Y., Wang, X., Li, J., Qin, R. & Wang, F. Y. 2018. An Overview of Smart Contract: Architecture, Applications, and Future Trends. IEEE Intelligent Vehicles Symposium. pp. 108-113.

Westerkamp, M., Victor, F. & Küpper, A. 2020. Tracing manufacturing processes using blockchain-based token compositions. Digital Communications and Networks. Vol. 6, no. 2, pp. 167-176.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. 2019. Blockchain technology overview Digital preprint at arXiv:1906.11078.

Zheng, Z., Xie, S., Dai, H. N., Chen, W., Chen, X., Weng, J., & Imran, M. 2020. An overview on smart contracts: Challenges, advances and platforms. Future Generation Computer Systems. Vol. 105, pp. 475-491.

Zheng, Z., Xie, S., Dai, H., Chen, X. & Wang, H. 2017. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. IEEE international congress on big data. Pp. 557-564.