


ORIGINAL RESEARCH

Privacy-Conflict Resolution for Integrating Personal and Electronic Health Records in Blockchain-Based Systems

Aleksandr Kormiltsyn, MSc¹; Chibuzor Udokwu, PhD²; Vimal Dwivedi, PhD³; Alex Norta, PhD⁴; Sanam Nisar, MSc¹

¹Department of Software Science, Tallinn University of Technology, Tallinn, Estonia; ²Austrian Blockchain Centre Research, Vienna, Austria; ³School of Electronics, Electrical Engineering and Computer Science, Queens University Belfast, Belfast, Northern Ireland, United Kingdom; ⁴Baltic Film, Media and Arts School, Tallinn University, Estonia; Dymaxion OÜ, Tallinn, Estonia

Correspondence: Aleksandr Kormiltsyn, Email: Aleksandr.kormiltson@taltech.ee

Keywords: blockchain, conflict management, e-healthcare, preventive healthcare, privacy, smart contracts

Abstract

Integrating personal health records (PHRs) and electronic health records (EHRs) facilitates the provision of novel services to individuals, researchers, and healthcare practitioners. Simultaneously, integrating healthcare data leads to complexities arising from the structural and semantic heterogeneity within the data. The subject of healthcare data evokes strong emotions due to concerns surrounding privacy breaches. Blockchain technology is employed to address the issue of patient data privacy in inter-organizational processes, as it facilitates patient data ownership and promotes transparency in its usage. At the same time, blockchain technology creates new challenges for e-healthcare systems, such as data privacy, observability, and online enforceability. This article proposes designing and formalizing automatic conflict resolution techniques in decentralized e-healthcare systems. The present study expounds upon our concepts by employing a running case study centered around preventive and personalized healthcare domains.

Plain Language Summary

This paper suggests using blockchain technology for privacy concerns in integrating personal health records and electronic health records in decentralized e-healthcare systems. This report focuses on designing automatic conflict resolution techniques to ensure patient data ownership, transparency, and privacy in inter-organizational processes. This paper proposes designing automatic conflict resolution techniques in decentralized e-healthcare systems, which can improve inter-organizational processes in healthcare. Using blockchain technology to integrate personal and electronic health records can ensure patient data ownership and promote transparency in data usage, addressing privacy concerns in healthcare systems. This paper emphasizes the importance of data privacy and protection in healthcare systems, highlighting the need for compliance with laws and regulations. The research results, including the proof-of-concept prototype, can provide practical insights into implementing conflict resolution techniques in decentralized e-healthcare systems.

Submitted: June 26, 2023; Accepted: November 13, 2023; Published: December 14, 2023

Healthcare systems suffer from high costs¹ and the economic interests of healthcare providers. For example, after privatization, the Irish hospital sector faced an increase in patient beds in private for-profit hospitals, while in not-for-profit hospitals, this number decreased.²

A personal health record (PHR) is an individual's electronic health-related information. It is managed and

maintained by the individual who controls access to the data. The PHR stores and organizes medical history, treatments, medications, notes, diagnoses, and other relevant health information, which can be shared between the individual and their healthcare providers. The PHRs provide a comprehensive and organized account of an individual's medical history, which can be invaluable for quick and

efficient diagnosis, improved safety, and quality of care. In addition, PHRs can be used to track a patient's medical history, identify trends and correlations, and provide feedback to the patient about their healthcare providers.

A feedback loop in healthcare refers to a process in which information about a patient's health status or the performance of a healthcare system is collected, analyzed, and used to make improvements or adjustments to patient care or healthcare processes. A feedback loop involves exchanging information about a patient's condition, treatment options, and progress. Patients provide feedback on their symptoms and treatment experiences, which helps healthcare providers make educated choices concerning their treatment.

Research defines the value of PHR as improving communication between a patient and a doctor, resulting in patient education leading to lifestyle changes.³ Patient engagement simplifies collecting and processing personal health and well-being data, increasing the value of personalized preventative healthcare services.⁴ According to Kormiltsyn and colleagues,⁵ a novel classification of personalized preventative health coaches is anticipated to arise. These coaches will use their expertise and proficiency in comprehending and analyzing health and wellness data. In our scholarly article published in 2019, we elucidate the economic and financial predicaments of the healthcare system and scrutinize the potential of blockchain technology to facilitate decentralized and patient-oriented systems.⁶ In a patient-centric system, individuals are responsible for generating and administering their data, while healthcare providers employ these data in their procedures instead of possessing them. The issue of transparent data exchange is illustrated by Norta and colleagues.⁷

The collection and processing of PHR entails many legal, technical, and emotional challenges. Scholars concentrate on the technical and security prerequisites of PHR systems when data are managed centrally.⁸⁻¹⁰ This methodology proves to be effective in situations where the number of PHR data sources is restricted. Thus, the number of processes that use PHR increases, and the need for more trust between stakeholders such as private companies, legal institutions, and individuals and integration complexity increases. Therefore, a centralized approach is not scalable, while decentralized inter-organizational processes based on blockchain technology provide a foundation for trustable and scalable connections.

An integrated PHR and electronic health record (EHR) system is socio-technical and involves people from different organizations that use different sets of technologies for collaboration and problem-solving.¹¹ An EHR is a patient's data created by healthcare professionals and stored digitally. Such data include the medical history, medications, immunization status, laboratory test results, and radiology images. It allows healthcare professionals to effectively plan and provide personalized patient care while also enabling them to securely

share medical information between healthcare providers and other authorized users. In addition, EHRs can help reduce healthcare costs and improve the quality of care. The decision to use a patient-centered system that shares PHR is emotionally motivated and creates a sense of uncertainty about the way personal data are used.

Using EHR-integrated PHR creates security, data protection, and privacy conflicts. Privacy is a legal term that limits knowledge and control over the content and performance of a (smart) contract, which should only be distributed between the parties to the extent necessary.¹²

While privacy, as defined in the Charter of Fundamental Rights of the European Union,¹³ is the right of any individual to respect their private and family life, home, and correspondence,⁷ data protection pertains specifically to the processing of personal data and is geared toward safeguarding this privacy.⁸ The Charter emphasizes that personal data must be processed fairly for specified purposes and based on the consent of the person concerned or some other legitimate basis laid down by law. This distinction is crucial in our research, as it underscores the importance of implementing blockchain-based systems in a manner that respects both the privacy rights and data protection principles laid out in these fundamental rights.

The standard, as defined by the European Commission (EC), proposes European Union contractual clauses approved by the EU in June 2021.¹⁴ It is important to note that these clauses were set to be replaced by updated versions in December 2022 as part of the EC's ongoing efforts to enhance data protection standards in line with evolving legal and technological landscapes. As outlined in the Standard Contractual Clauses (SCC) documentation by the EC, this update is a significant step in ensuring robust and up-to-date data protection measures in cross-border data transfers.

In 2010 Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing,¹⁵ the European Data Protection Board (EDPB) and the Spanish Data Protection Authority (AEPD) elucidate that when identifiers are linked to a hash, such as a telephone number, the information can be unequivocally traced back to a specific data holder. This linkage introduces additional vulnerabilities to the hash's confidentiality, as the linked identifier can potentially reduce the effective message space for that particular hash, thereby compromising its intended pseudonymization function. This insight highlights the potential limitations and challenges in utilizing hash functions for data protection, underlining the need for careful consideration in their application in blockchain-based systems.

Sun and colleagues¹⁶ define the main requirements for medical systems employing the Internet of Things (IoT) as data integrity, usability, auditing, and patient

information privacy. Al-Muhtadi and colleagues¹⁷ focus on cybersecurity and privacy issues when integrating mobile healthcare applications and propose a secured architecture for multi-cloud environments. Research by Katurura and Cilliers¹⁸ states that users lack data control and transparency. In addition, researchers have discovered a lack of knowledge of security- and privacy risks related to personal data for wearable devices.¹⁹ Several authors have highlighted that sharing medical data leads to security and privacy risks.^{20–22} Simultaneously, the authors assert the necessity for further investigation into developing secure and integrated healthcare systems. Autonomous health data collection proposes new challenges for data privacy when using smart home systems.^{23–25}

Using equitable algorithms to resolve civil conflicts has been proposed by Salehi and Giacalone.²⁶ These algorithms are based on different technologies, such as artificial intelligence (AI) and algorithmic decision systems (ADS). In their publication,²⁷ Xu and colleagues presented a systematic investigation employing the Graph Model for Conflict Resolution (GMCR) as a viable approach to address real-world conflicts. Other scholars²⁸ use Hidden Markov Models (HMM) to scrutinize the incoming data and reconcile any conflicts that may arise. The analysis includes customization and training of the HMM models, which are later used with a rule-based system to detect conflicting information, resolve the identified conflicts, and use past data and decisions to prevent conflicts before they occur. Some researchers²⁹ suggest using a mediator who detects conflicts and offers a possible solution to the conflicting parties.

The main research question is how to automatically resolve conflicts in integrated e-healthcare inter-organizational processes. To answer the main research question, we deduce the following sub-questions. What are the requirements for individual-centric PHR inter-organizational collection and -processing? The answer to this question aims to define the logical requirement space that includes stakeholder assignments. What conflicts arise in inter-organizational e-healthcare processes? To address this inquiry, conflicts within inter-organizational e-healthcare processes are delineated and aligned with processes outlined in the preceding research query.

Furthermore, these processes are devised utilizing the Business Process Model and Notation (BPMN). What are the automatic conflict-resolution techniques in decentralized e-healthcare? The objective of the privacy conflict-resolution technique is to create a conflict-resolution process for e-healthcare, utilizing BPMN, based on the process design in which conflicts arise, as defined in the preceding research inquiry.

Presented here is an outline of the remainder of this review.

- A literature review, preliminaries, and a running case.
- Discussion of patient-centered PHR collection and processing requirements.
- Present conflicts in the decentralized e-health process by mapping them to specific functional goals and business processes.
- Address the privacy conflict-resolution techniques when processing medical data in inter-organizational processes.
- Evaluation of the devised process and juxtaposes the findings with those of other research endeavors.
- Conclusion offering insights into the limitations, unresolved matters, and potential avenues for future research.

Literature Review and Preliminaries

Here, the authors review related literature and further provide the preliminaries that outline the background for this research.

Literature Review

Research on blockchain technology in healthcare has notably increased.^{30–32} The primary focus areas within this field are data sharing, health records, and access control. A distributed ledger, as proposed by a blockchain, puts forth the concept of participants adding new records. The information stored on a blockchain is immutable, which is ensured by cryptography.³³ The data contained within the blockchain are securely stored in transactions, which are then organized and linked together in blocks through cryptographic methods.

Each block is intricately connected to the subsequent block in the chain. Utilizing the cryptographic technique referred to as the Merkle tree, or hash tree, ensures that the transactions stored on a blockchain are correlated through mathematical hashes,^{34,35} thereby assuring that no alteration can render the entirety of the recorded data invalid. Hashes streamline the process of validating new transactions, obviating the necessity to analyze all the information stored within a blockchain.³⁵ Some blockchains, such as Ethereum, support smart contracts that nodes can execute.

Research Methodology

Design-science research (DSR) is used in this paper to “conduct the research.” The DSR offers a framework for developing and assessing new artifacts.³⁶ The environment, DSR evaluation, and knowledge base are the three main components of DSR. The research’s environment describes the issues that organizations and application domains face. The knowledge base offers theoretical support to develop new artifacts that solve identified

organizational issues. The created artifact is evaluated as part of the DSR.³⁶

Previous research by Narendra and colleagues¹¹ conducted by the authors on the conflict-resolution approach in the M2X (Machine-to-Everything) environment serves as the environment pillar for this study. In this article, the previously proposed approach is adapted to an e-health environment where the parties involved in the inter-organizational processes lack trust.

The knowledge base represents existing strategies, techniques, and models that serve as the building blocks for designing the conflict-resolution methods and the decentralized inter-organizational process flow. We use the Trustable DApp Modeling (T-DM) framework for defining design-process requirements as it extends the Agent-Oriented Modeling (AOM) approach and introduces tokenized goals used in blockchain systems. We refer the reader to “Preliminaries” below for a more detailed Test Data Management (T-DM) framework description and BPMN to define process flows.

The designed automatic conflict-resolution techniques are evaluated in the decentralized e-healthcare processes with Colored Petri Nets (CPN) modeling. In addition, we provide a proof-of-concept (PoC) prototype that illustrates the implementation of the running case. The evaluation approach is similar to the one used in the previous research.¹¹ In addition, we provide the implementation of the modeled running case with the PoC.

The Running Case and Background Preliminaries

To ensure confidentiality and facilitate conflict resolution, we offer a comprehensive analysis in the section “Running Case and Privacy Conflict Scenario” that presents a practical scenario from a patient-centric standpoint. The present case study aims to facilitate the understanding of the ongoing case and the subsequent sections of this paper. The “Preliminaries” section offers the necessary introductory information essential for comprehending the subsequent segments.

Running Case and Privacy Conflict Scenario

Figure 2 presents a description of the ongoing case within the domain of cancer prevention. While physiotherapists primarily evaluate clinical outcomes by assessing pain level, range of motion, and muscular strength, the domains of patient goals consist of physical activity, workplace environment quality, and sleep quality. The observed disparity can be elucidated by considering the intricate nature of comparing individuals using The Patient Specific Functional Scale.³⁷ Consequently, it is unfeasible to quantify patient-goal domains. In our running case, healthcare data are monitored by the patient with a smartwatch and air- and water-quality sensors. These

devices collect patients’ activity-, health, and ecological environment data and share it if necessary.

The aforementioned information is gathered continuously, with the healthcare provider receiving a feedback loop during patient monitoring. Additionally, when the patient seeks medical attention from a general practitioner at a hospital, the latter conducts laboratory tests, obtains a medical history, and subsequently incorporates these data into the EHR. In conclusion, the EHR is collaboratively accessed by both healthcare professionals and general practitioners. These individuals are responsible for submitting comprehensive reports to the insurance provider to secure reimbursement for the medical interventions provided. The medical reports vary as a consequence of the information accessible to the healthcare professional, which encompasses the PHR together with continuous input from the patient.

The aforementioned phenomenon serves to augment the understanding of health-related circumstances, which, in turn, facilitates the delivery of personalized healthcare services by the healthcare practitioner. In contrast, the general practitioner is limited to accessing solely the EHR due to the lack of a feedback mechanism.

The discrepancy in asserting medical information contradicts the insurance company, which lacks guidelines for processing PHR data. Such a disparity further complicates the utilization of recently developed healthcare amenities that rely on processing PHR. It is plausible that implementing a feedback mechanism may enhance the situation.

The patient encounters privacy conflicts due to the vulnerability of his data in smart autonomous devices or various applications, leading to privacy conflicts. Upon the patient providing his PHR to the primary care physician after he has agreed with an explicit explanation to use the patient’s data under the regulatory requirement, the latter is able to employ it within the internal procedures of the healthcare provider, such as for the purposes of generating reports, conducting statistical analysis, and facilitating research endeavors. These procedures might involve external participants such as the National Bureau of Statistics, independent research firms, or private enterprises specializing in data reporting services. The opacity of processes for the patient renders them non-transparent. Consequently, the possibility of mishandling PHR data may arise.

In this article, we define three conflicts during the inter-organizational insurance process. First, home monitoring involves privacy conflicts when patient data are collected. Wearable devices and PHR systems, which retain amassed data, are susceptible to the potentiality of unauthorized individuals extracting said information. Next, an integrity conflict arises when PHR traverses various processes and is susceptible to alteration by the

parties involved. Lastly, the consistency conflict arises when the insurance provider receives claims from both the healthcare professional and the doctor, wherein they provide dissimilar information in the insurance claim.

Preliminaries

This article considers e-healthcare processes mapped to blockchain systems for achieving immutable traceability, security, and privacy-assured distributed disintermediation and decentralization in inter-organizational collaboration. Blockchain technology provides a distributed ledger that allows participants to add and verify records on a ledger, and cryptography ensures that the records are immutable.³³ When participants add records to the ledger, they are stored as hashed transactions and grouped in blocks. The cryptographic linkage between each block and its predecessor is a fundamental characteristic of the system under consideration. Smart contracts are executable programs that run and are stored on the blockchain.³⁸ According to Nguyen and Kim,³⁸ the common blockchain platforms are Bitcoin,³⁹ Ethereum,⁴⁰ Hyperledger Fabric,⁴¹ etc.

Blockchains use different consensus mechanisms to validate transactions. For example, Bitcoin uses a proof-of-work (PoW) consensus algorithm. This mechanism assumes that all the participating nodes are solving a difficult mathematical problem. It rewards the first node with the number of tokens by allowing it to add the next block.³⁸ Ethereum uses a proof-of-stake (PoS) where validation is based not on the resources spent on mathematical problem-solving but on a node's reputation. We refer to our previous research⁴² for further details about the practical usage of blockchain technology.

For blockchain technology, different token types are available. Here, we propose using two token types: utility- and non-transferable "soul bound" tokens (SBT). The account represents "Soul", and tokens held by the accounts as "Soulbound Tokens" (SBTs).⁴³

The utility token is integrated into an existing protocol on the blockchain and used to access the services of that protocol. In addition, it is used as a cryptocurrency representing access to a product or service. In contrast to utility tokens, SBTs are defined by their uniqueness and rareness. This token type provides token ownership and corresponding transfer functions. The utilization of SBT in the decentralized e-healthcare system is being suggested due to the requirement for effective management of identity and access control pertaining to e-healthcare data.

To control access to their identity management, individuals need the capability to manage not only their identifiers but also the data associated with them. This approach is fundamental to self-sovereign identity, representing a shift from traditional identity management systems to a user-driven identity administration model. In such a model, enabled by blockchain technology, users have full control over their identifiers and the personal

data linked to these identifiers, ensuring greater autonomy and privacy in digital interactions.⁴⁴

The blockchain ecosystem supports different types of participants, such as oracles and Decentralized Autonomous Organizations (DAOs). In the blockchain context, oracles are used to fetch external data that are unavailable in the blockchain. Oracle is centralized and trusts the third-party external data provider, but there is a known problem with unsecured data retriever channels.⁴⁰ However, there are problems with oracles in trustworthiness and reliability.⁴⁵ While test oracles cannot be fully automated, this results in the agent's intervention to ensure the correctness of the oracle's behavior. Caldarelli and Ellul⁴⁶ state that a DAO is an autonomous organization implemented with smart contracts. The behavior and business rules of DAO are predefined with smart contract logic.

The derived e-healthcare system is used in an inter-organizational collaboration based on dynamic service outsourcing specified in electronic contracts.⁴⁷ In healthcare, inter-organizational processes include data sharing between patients and healthcare providers or other organizations such as insurance companies. This paper considers a patient-centric, decentralized system perspective where PHR data flow through different systems and are available to human- and non-human agents such as autonomous smart devices. Such devices include wearables that monitor patient health with sensors, smart home components, autonomous drones, or even vehicles involved in healthcare processes. Research by Grefen and colleagues⁴⁸ presents a conceptual framework for an intelligent e-health gateway that acquires and analyzes the collected medical information. In our investigation, we integrate the privacy-conflict resolution strategy proposed in the article by Narendra et al.¹¹ into a decentralized healthcare ecosystem, which encompasses self-governing smart devices and their collaboration, as delineated in Ref. 49.

In socio-technical systems, fulfilling societal functions becomes central.⁵⁰ Since such systems do not function autonomously but are the outcome of human action, research proposes an agent-oriented approach when modeling complex socio-technical systems.⁵¹ As simulated actors are similar to humans because of their cognitive and social binding with the knowledge of themselves and dependency on their history, an agent-oriented approach utilizes that in agents' behavior. In the realm of blockchain and smart contracts, the oracle problem is predominantly concerned with the trustworthiness and reliability that oracles bring forth.⁴⁵ As asserted by Barr,⁵² this conundrum emerges when test oracles are unable to execute in a fully automated manner. In the event that oracles are not automated, the intervention of an agent becomes obligatory to ascertain the veracity of the observed behavior. We consider multi-agent systems (MAS) and use an AOM approach⁵¹ to define the requirements of

the privacy-oriented PHR- and EHR data-integration process.

Goal modeling is used to analyze socio-technical domains⁵³ as goal models represent the value proposition of a system. The system’s value is represented by functional and quality goals and roles. The system requires some capacity or a position represented by a role to achieve its goals. A functional goal represents the system’s functional requirement, and a quality goal represents a system’s non-functional or quality requirement.⁵³ Quality goals are synonymously called non-functional requirements in software engineering.⁵³ The functional-, quality-, and emotional goals are inherited by all their subgoals.

As a patient-centric e-healthcare system is a social system driven more by emotional engagement than functionality, research⁵⁴ proposes an Emotional Attachment Framework that includes emotional goals in the early design stage. This framework is integrated into the T-DM framework. It extends it with emotional goals representing user feelings of negative emotions, such as distrust and lack of ownership of private and confidential data.⁵⁴ Research by Kormiltsyn⁵⁵ defines positive and negative emotions from appraising a product or a beneficial or harmful service. Mendoza and colleagues⁵⁶ describe how quality goals trigger different positive and negative emotions among users. Examples of such goals are usefulness, adaptability, and ease of use. In this paper, we place the emotional goals between a role and a functional goal to define emotions that influence the functional goals of the system.

The topic of privacy- and security-conflict management increases in importance with the increasing usage of IoT, social networks, etc. Research by Mendoza and colleagues⁵⁷ defines basic concepts of secure computing,

stating that privacy focuses on the governance of an individual’s data. Security measures are implemented to safeguard against unauthorized access, with a primary emphasis on fortifying data against various forms of attacks and preventing data theft.⁵⁸ Several research publications confirm the importance of defining conflict-management techniques when sharing personal data.^{59,60}

To design a goal model for the decentralized e-health system, we use the approach defined in the T-DM framework⁶¹ that focuses on designing decentralized applications (DApps) to support inter-organizational processes. The T-DM framework extends the AOM goal diagrams^{53,61} and introduces a new concept of tokenized goals representing the decentralized services that perform transactions in the blockchain and spend or gain tokens. The model-driven approach in the T-DM framework supports mapping AOM goal models to the Unified Modeling Language (UML) component architecture model.

To evaluate the proposed conflict resolution technique, we designed a formal CPN⁶² model. CPN, a language with a graphical orientation, possesses the capability to identify potential design flaws, absent specifications, as well as security and privacy concerns within systems. It serves the purpose of designing, specifying, simulating, and verifying systems. A CPN model is a bipartite graph comprising tokens, places, arcs, and transitions. Places have the ability to hold multiple tokens with color, indicating attributes with corresponding values. The transitions in CPN are triggered only when all input places have the required tokens in place. Finally, transitions produce condition-adhering tokens into output places.⁶³ Our model uses the CPN ML programming language to simulate the running case described in Figure 1. Research⁶³ provides more detailed information about CPN.

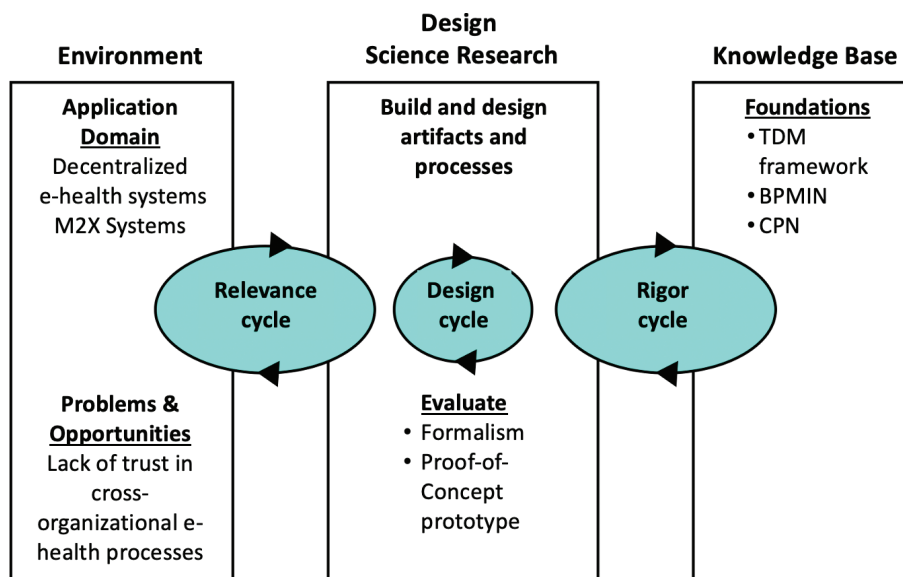


Fig. 1. Design Science Research Cycles. BPMN: Business Process Model and Notation; CPN: Colored Petri nets; DSR: design-science research; M2X: Machine-to-Everything; TDM: Trusted Document Management.

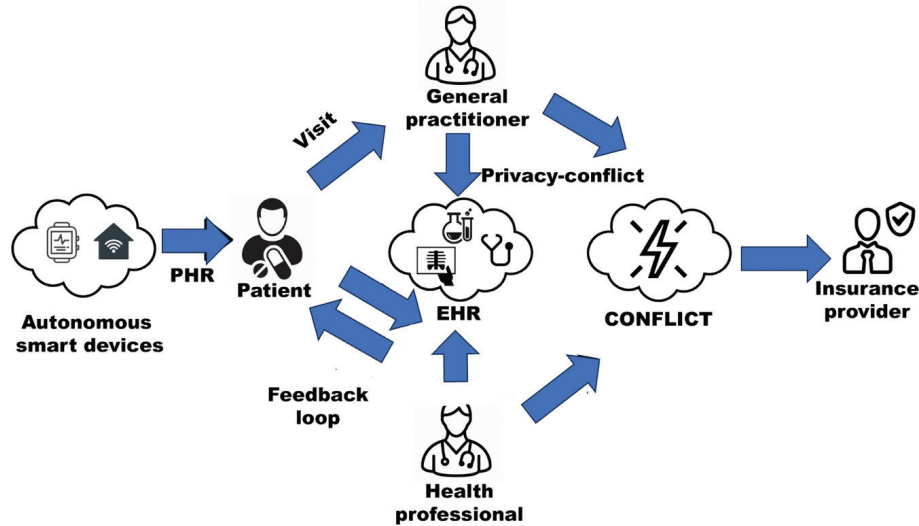


Fig. 2. Conflicts while processing the (EHRs) electronic health records and (PHRs) personal health records.

In a blockchain-based e-health system, trusted data sharing may be enabled by the multi-factor self-sovereign identity authentication (MFSSIA)⁶⁴ for humans and machines managed with smart-contract blockchain technologies.

Figure 3 illustrates how human users (note that smart autonomous devices may also be put in place of humans) create challenges for other entities and ask them to respond. Either the corresponding entity fails to do so or can complete the challenges with correct responses. The chosen challenge depends on the use case, the required security level, and the threat level of the involved entities.

In the example of Figure 2, the organization identity authenticates an autonomous device by providing challenges the device needs to perform to confirm its identity. The organization decides whether the response satisfies its request. Both upload the request and response to the blockchain. In this case, the authentication fails if the corresponding entity fails to respond correctly. Otherwise, the entity is successfully authenticated.

Multi-factor challenge-set self-sovereign identity authentication (MFSSIA) enables cross-blockchain interoperability by utilizing blockchain oracles. The oracles are digital agents that aim to fetch external world information into a blockchain. Data from various sources (blood pressure monitors, PHR, EHR, etc.) are then submitted to the blockchain as transactional data.⁶⁴ Oracles are used as data feeds for real-world information to be queried by smart contracts running on blockchains and by pushing data into data sources from the blockchain itself.⁶⁵

The challenge sets in MFSSIA are stored in a decentralized knowledge graph (DKG¹). In DKG, information

is stored as a graph of entities and relationships relevant to a specific domain or organization. DKG provides immutable, queryable, and searchable graphs that are used across different applications.

Results

The present section furnishes the outcomes that constitute the responses to the research inquiries delineated in this scholarly document. To specify the requirements for individual-centric PHR collection and processing (sub-question 1), the “Requirements for the Patient-Centric PHR Collection and -Processing” section provides the goal model for the decentralized person-centric e-health inter-organizational process for preventive healthcare. This goal model lays the groundwork for the system design by capturing key functional and quality requirements. To identify where conflicts arise (discussed later), the “Integrated PHR- and EHR-Processing Privacy Conflicts Between Healthcare Providers and Individual Patients” section (sub-question 2) defines conflicts in the decentralized e-health process and describes the mapping of conflicts to specific functional goals and business processes. Finally, to present the conflict resolution techniques, the “The Conflict-Resolution Techniques When Mapping the BPMN-Designed e-Healthcare Process to a Blockchain System” section (sub-question 3) proposes techniques in the blockchain system to resolve the identified data and claimer definition automatically conflicts transparently and decentralized.

Requirements for the Patient-Centric PHR Collection and - Processing

As posited by Norta et al.,⁵³ a goal model has the potential to serve as an analytical tool for scrutinizing the issues that arise within a socio-technical domain. The goal models act as an interface for exchanging information between stakeholders possessing technical and non-technical

¹ <https://docs.origintrail.io/general/dkgintro>

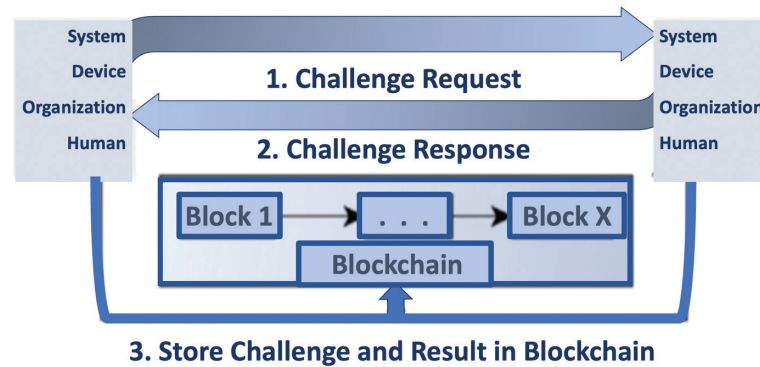


Fig. 3. Conceptual depiction of the (MFSSIA) Multi-factor challenge-set self-sovereign identity authentication lifecycle for challenge-response management.

backgrounds with the purpose of generating comprehensible knowledge of the e-health domain. Due to the complexity of the goal model, we split it into two parts, where Figure 4 defines goals related to the patient and healthcare professional, and Figure 5 includes insurance provider and general practitioner goals. Figures 4 and 5 depict a goal model, which delineates functional, quality, positive, and negative emotional goals. It is important to note that each functional goal is further subdivided into subgoals in a hierarchical manner, with the highest level being positioned at the top and the lowest level at the bottom. In our previous research,⁶⁶ we use goal modeling in requirement engineering. We use the notation described in Ref. 57, where several symbols correspond to different goal types. Thus, the heart shape represents the positive emotional goal, the cloud shape defines quality goals, and a parallelogram represents the functional goals. In this research, we extend the goal model notation with the tokenized functional goals that represent the functional goals that communicate with a blockchain. In our designed system, we consider the M2X context, where agents can be both human and non-human.

We put forward the suggestion of employing a utility token that has been incorporated into a pre-existing protocol on the blockchain and is utilized to gain access to the various services offered by said protocol. These tokens serve as means of payment for the services provided within their respective ecosystems in the proposed system. Our suggestion is the introduction of a token named “Personal Health Token (PHT)” as a utility token for the decentralized person-centric e-health system.

In addition to the utility token, we propose the usage of SBT tokens that are created by medical data providers such as smart devices, PHR-, and EHR systems and include the medical data that is owned by the patient. For example, if a patient decides that some of his health data are useful for medical research, he proves his ownership with SBT to the research company. The primary objective of the value proposition is to *prevent disease*

in connection with an individual who possesses self-motivated incentives and anticipates being informed and empowered throughout the preventive course of action. The principal value proposition of the system revolves around the prevention of diseases in individuals. The subgoal of providing home care involves a patient who collects his medical data in a trustworthy manner. The subgoal of providing ambulatory care is executed by the general practitioner, whereas the subgoal of providing insurance is carried out by an insurance provider. Additionally, the subgoal of onboarding stakeholders is performed by an acceptor agent. The stakeholder’s objective, which is found within the system, is crucial for the stakeholders to engage in the inter-organizational procedure, while they undertake verification using a protocol known as MFSSIA, which is based on blockchain technology.⁶⁴ Onboarding includes the usage of PHT tokens for accessing authentication services. Both a health professional and a general practitioner submit medical cases to the insurance provider for requesting claims. The initial objective encompasses two additional sub-objectives: to monitor health status executed by the smart-hub agent and to keep a healthy lifestyle conducted by a healthcare specialist. The latter employs the system, provided that he possesses self-assurance, possesses the capability to render expert judgments, and is not overwhelmed by the intricacies of the system.

The goal of monitoring health status encompasses three sub-objectives: the generation of a PHR from the data gathered by two entities, namely, a smartwatch and an air quality home sensor; the semi-automated analysis of said PHR; and the secure sharing of the PHR, ensuring the processing of interoperable information. The security is provided by validating SBT to ensure the ownership of shared data. The produced PHR possesses the capability to be seamlessly integrated, enabling its dissemination among various involved parties. Following its creation, the PHR is subsequently inserted into the blockchain-distributed ledger, ensuring that it can be shared

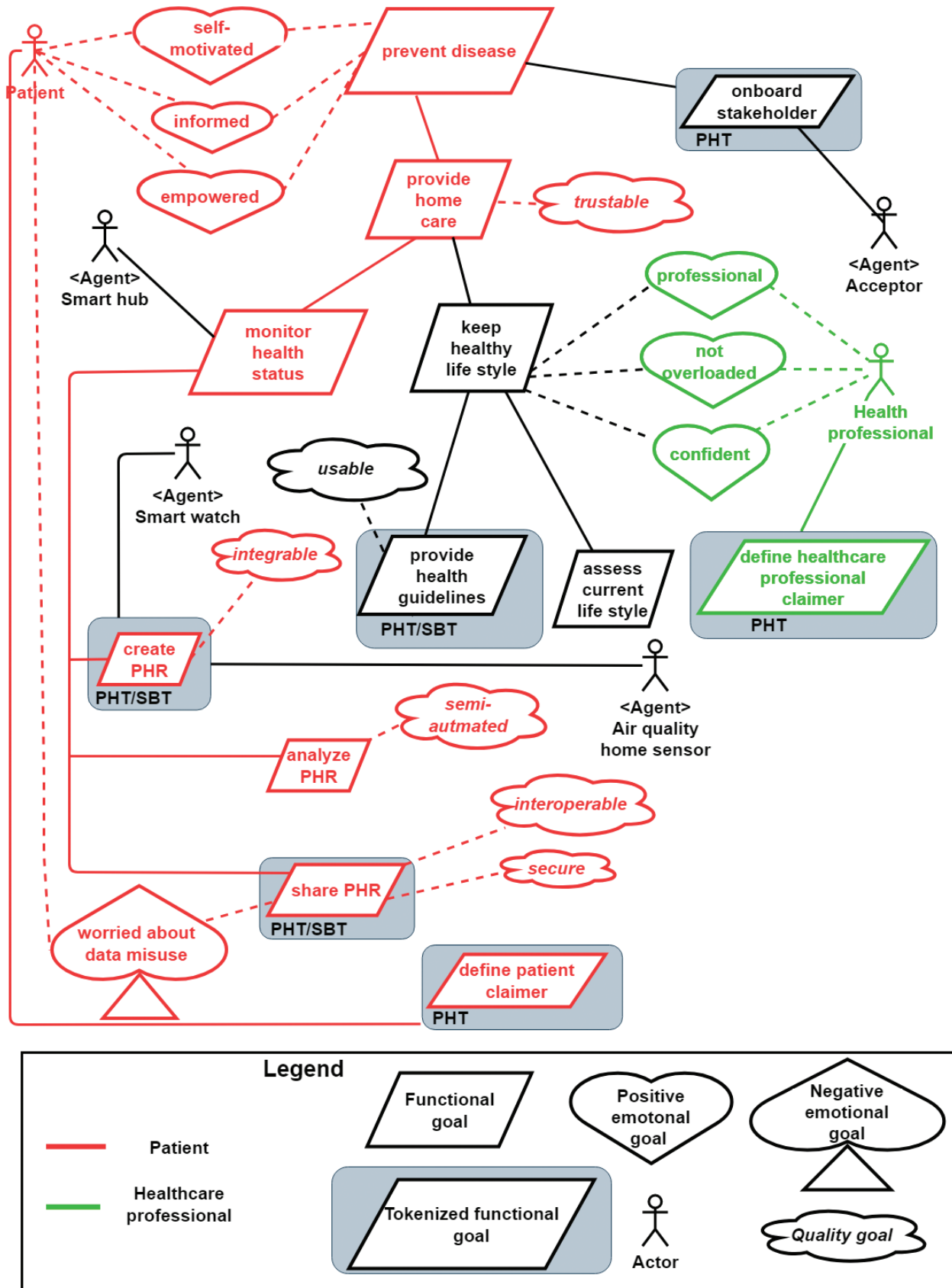


Fig. 4. The goal model for a decentralized individual-centric system. Patient and healthcare professional goals.

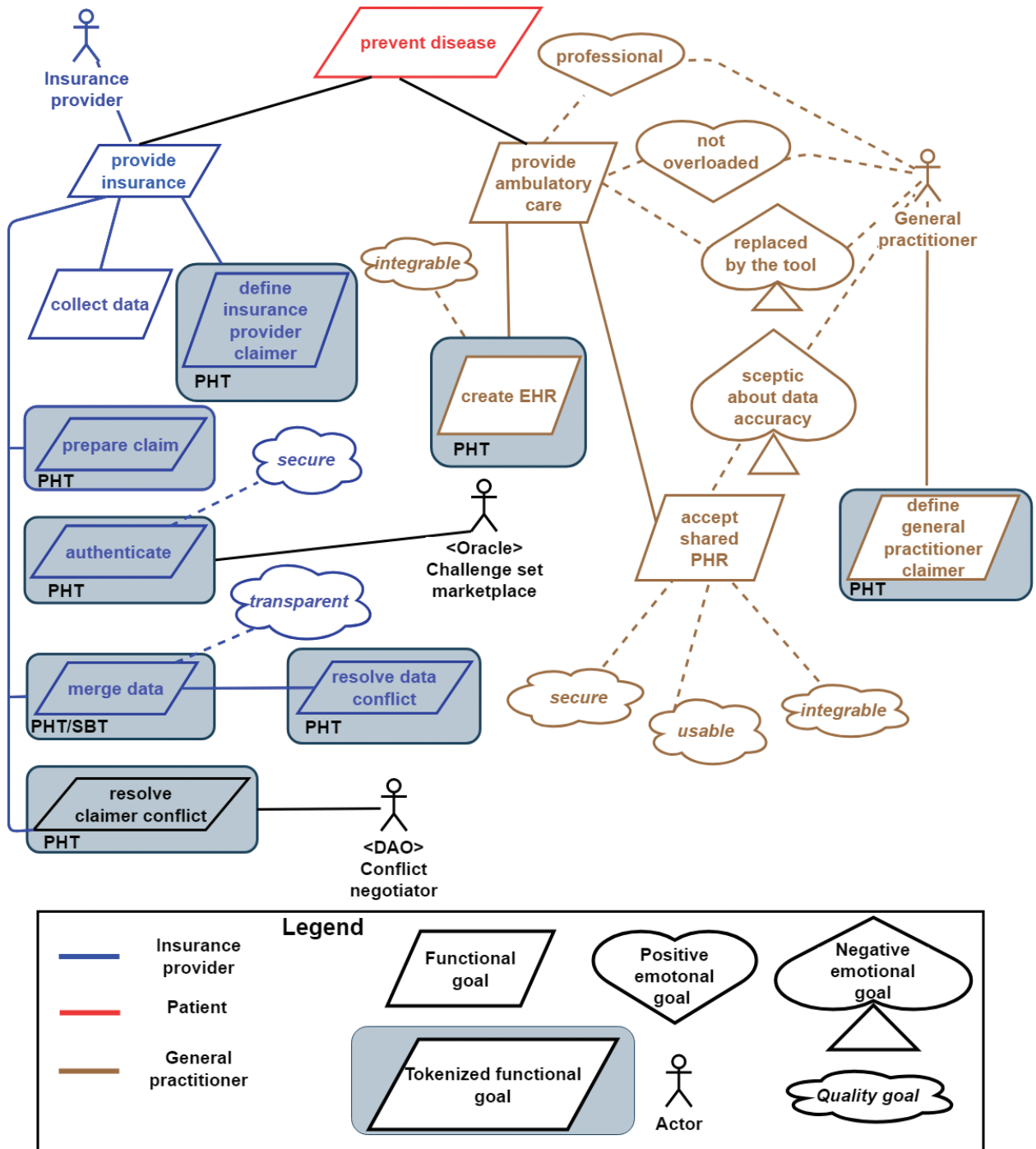


Fig. 5. The goal model for a decentralized individual-centric system: insurance provider and general practitioner goals.

with other stakeholders while simultaneously guaranteeing its immutability. The objective of achieving a healthy lifestyle encompasses two specific subgoals: evaluating one’s present lifestyle and offering health recommendations. Guidelines are shared with a patient via blockchain and should be usable.

The goal of providing ambulatory care encompasses the involvement of a primary care physician who harbors

apprehensions regarding being substituted by technology and necessitates the need to maintain a sense of professionalism without experiencing excessive workload. This objective is further divided into three sub-objectives: establishing an interoperable EHR system, embracing shared PHR, and administering medical diagnosis. The created EHR is stored on a blockchain to be available for the patient in a secure and immutable way. Adding data

to the blockchain requires PHT. When a general practitioner agrees to accept PHR, they have reservations about the accuracy of shared data. This phenomenon can be attributed to the potential for erroneous data generation or the likelihood of an alternative individual asserting ownership over the furnished data. The MFSSIA protocol supports the authenticated and secure way to produce medical data and eliminates distrust. Medical data are frequently stored in various standards and contexts, resulting in semantic heterogeneity. The process of standardizing PHR and EHR data aids in the prevention of such heterogeneity. Moreover, this standardization facilitates the simplification of PHR and EHR processing. The secure, integrable, and usable acceptance of PHR is imperative.

The provided insurance goal encompasses a total of nine subgoals, namely, data collection, verification, data consolidation, claim preparation, resolution of conflicts between claimants, definition of the insurance provider's claim, definition of the claimant's claim, definition of the healthcare provider's claim, and definition of the general practitioner's claim. The data that have been collected are utilized during the process of claim preparation, and they necessitate the process of authentication for the various sources of data within the interorganizational framework, which is based on the decentralized protocol known as MFSSIA. Authentication is executed through the utilization of the challenge set marketplace, wherein the blockchain oracle facilitates the provision of secure challenge sets for the purpose of user authentication. In order to assemble a claim, it is imperative for the insurance provider to meticulously integrate data in a transparent manner, resolving any potential conflicts that may arise. Both actions are performed with smart contracts. As each and every stakeholder incorporates business regulations into their respective functional goals (namely, delineating the claimant for insurance providers, delineating the claimant for patients, delineating the claimant for healthcare providers, and delineating the claimant for general practitioners), it becomes imperative for the insurance provider to address any conflicts that may arise among the claimants. We propose to use smart contracts to keep conflict resolution transparent and, thus, trustable to the stakeholders involved in the interorganizational processes. The smart contracts are accessed by the conflict negotiator, DAO, implementing the complex logic of conflict resolution algorithms.

Integrated PHR- and EHR-Processing Privacy Conflicts Between Healthcare Providers and Individual Patients

In the present case, it is posited that the insurance provider is composed of three partners: a patient, a general practitioner affiliated with a hospital, and a healthcare professional, as depicted in Figure 1. Distinct business

rules are taken into consideration for each stakeholder, representing the identity of the claimant and the recipient of payment from the insurance provider under specific circumstances. The claimant in our ongoing scenario is posited to be determined by the measurement of systolic blood pressure.

According to a business rule, when a patient's systolic blood pressure drops below 160 mmHg, the patient is designated as the claimant; otherwise, the claimant is a general practitioner. In common practice, a systolic blood pressure reading of 120 mmHg is deemed as a normal value. Hence, the patient experiences no issues with regard to blood pressure. The decision is founded upon the supposition that in the event that the patient does not experience any complications, their way of life is praiseworthy, and they meet the criteria to be considered as a beneficiary for the insurance provider. A systolic blood pressure ranging from 120 to 160 mmHg presents problems and necessitates the patient's diligent attention and engagement to restore it to a normal range. Consequently, the patient also perceives themselves as a claimant within this specific data slot. Systolic blood pressure surpassing 160 mmHg poses a dangerous situation and warrants the attention of a medical practitioner. Consequently, the patient views the general practitioner as a claimant.

According to a regulation governing the practices of a primary care physician, it is stipulated that if a patient's systolic blood pressure falls below 120 mmHg, the patient shall be classified as a claimant; conversely, when the systolic blood pressure surpasses the norm of 120 mmHg, the claimer assumes the role of a general practitioner. In instances where the systolic blood pressure of the patient diverges from the anticipated norm, the primary care physician conscientiously monitors the patient's state and subsequently administers the requisite medications and interventions in accordance with the preliminary assessments. Consequently, the general practitioner perceives himself as a claimer.

To conclude, the healthcare professional adheres to a set of business rules that assert the following: if the patient's systolic blood pressure is below 120 mmHg, then the claimer is classified as a patient; in contrast, if the systolic blood pressure exceeds 160 mmHg, the healthcare professional assumes the role of a claimer. In situations where the systolic blood pressure registers between 120 and 160 mmHg, healthcare practitioners exercise discretion in explicitly identifying the claimant.

The emergence of conflicts can be attributed to the internal regulations of all three entities involved, as illustrated in Figure 6. These conflicts become apparent when a patient's systolic blood pressure exceeds the predetermined threshold of 120 mmHg.

Functions Where Conflicts Occur

In this section, we define functional goals presented in the goal model in Figure 4 and Figure 5 where conflicts occur. In order to simplify the research, we have chosen to exclude any conflicts that may arise in relation to quality and emotional objectives. The correlation between functional objectives and potential conflicts has been presented in Table 1.

In our case, two possible conflicts are considered during the interorganizational insurance claim process. Initially, a data conflict may arise when an insurance provider gathers and consolidates data from various sources, including the patient’s PHR system, the healthcare provider’s EHR system, and the healthcare professional’s records. Given that each stakeholder may maintain data in distinct formats and standards, there exists a possibility that the amalgamated data may not correspond or synchronize appropriately when integrated by the insurance provider, leading to incongruous or contradictory data.

Second, a claimer definition conflict can arise when each stakeholder defines the insurance claimer based on their internal business rules and the data value, such as the patient’s blood pressure reading. As illustrated in Figure 6, the rules for proposing a claim from the patient, healthcare provider, and healthcare professional may differ, depending on the data circumstances. For example, if the patient’s blood pressure is between 120 and 160 mmHg, the patient and healthcare provider will propose different claimers based on their distinct rules. The incongruity between the definition of the claimant gives rise to a conflict that necessitates resolution.

Processes Where Conflicts Occur

The definition of an insurance claimer entails the retrieval of data from PHR and EHR data sources, followed by their integration and the elimination of irrelevant data. The insurance provider claimer definition process is defined in Figure 7. To facilitate the interorganizational claimer definition process, we have subdivided it into

Conflicts-Based Difference of Opinion on Rules Dissense

Patient	Hospital	Healthcare Professional
Patient	Hospital	Healthcare Professional 120 mmHg
Patient	Hospital	Healthcare Professional 160 mmHg
Patient	Hospital	Healthcare Professional

Fig. 6. The implementation of business rules has been found to result in conflicts in behavior.

Table 1. Functional goals where conflicts occur.

Functional Goal	Actor	Conflict
Collect data	Insurance provider	Data can be different
Merge data	Insurance provider	Data can be different
Define insurance provider claimer	Insurance provider	Claimer can be different
Define patient claimer	Patient	Claimer can be different
Define healthcare professional claimer	Healthcare professional	Claimer can be different
Define general practitioner claimer	General practitioner	Claimer can be different

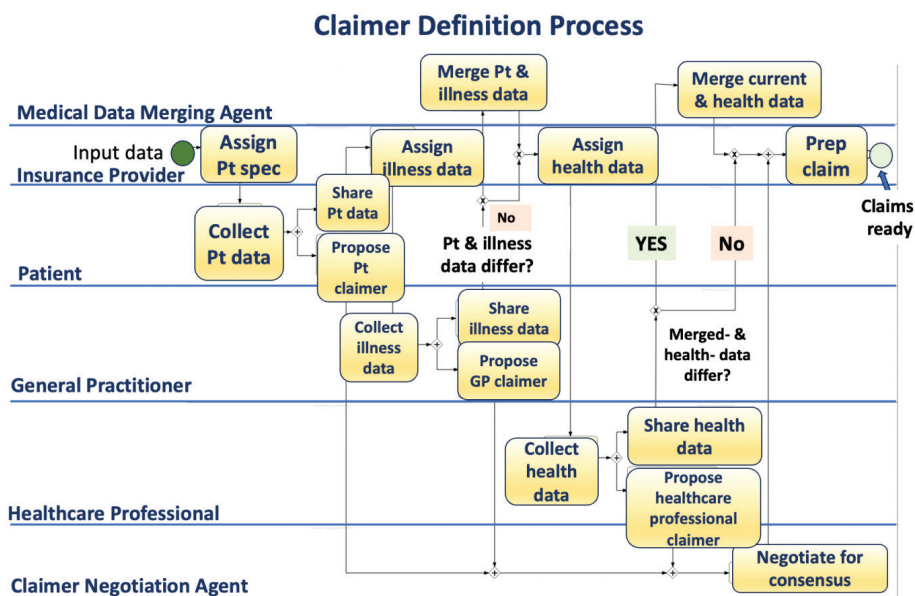


Fig. 7. Claimer-definition process for the insurance provider.

three subprocesses, namely, the decision-making process for healthcare professionals, healthcare providers, and patients. Additionally, we shall expound on these three internal processes utilizing the BPMN notation.

Figure 8 illustrates the internal decision-making process undertaken by the patient, which is directed by the business rules described earlier. At the outset, the patient ascertains the presence of the requested data from the insurance company within their PHR repository. In the event that the requested data are not present, the patient proceeds to record the blood pressure measurements and subsequently stores these new data within the PHR repository. Subsequently, the patient retrieves the aforementioned data from the PHR repository and shares it with other relevant stakeholders involved in the interorganizational process. Finally, to propose the claimer, the blood pressure value is assessed. If the blood pressure value is equal to or less than 160 mmHg, the patient asserts themselves as the claimer.

Conversely, if the blood pressure value exceeds 160 mmHg, the healthcare provider is proposed as the claimer.

Figure 9 illustrates the internal decision-making procedure for the healthcare provider, such as a hospital. Initially, the healthcare provider acquires the illness (EHR) data from external EHR systems, which may be affiliated with a hospital. Once the external EHR data are obtained, it is transformed into the healthcare provider’s health data standard and stored within its own system. Subsequently, the imported external data are disseminated among the other participants involved in the interorganizational process. Lastly, the healthcare provider’s claimer proposition is formulated based on the business rules delineated in the “Integrated PHR- and EHR-processing privacy conflicts between healthcare providers and individual patients” section. This proposition encompasses three potential claimants: the patient, the healthcare provider, and an undefined claimer. Specifically, if the blood pressure value is

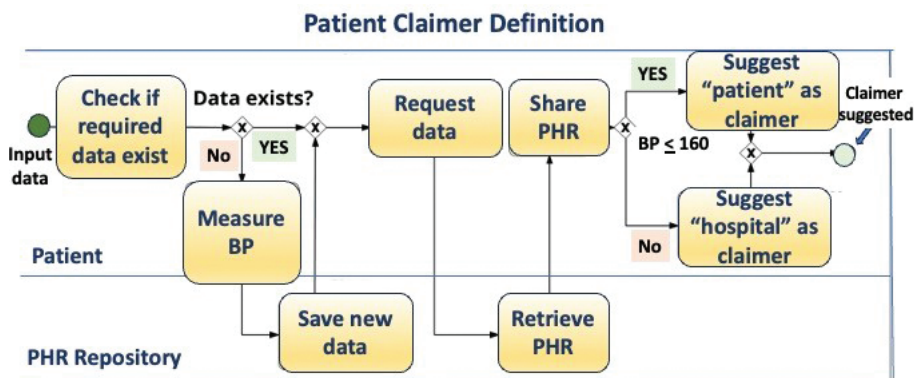


Fig. 8. Patient-claimer internal decision process. BP: blood pressure; DAO: Decentralized Autonomous Organizations; PHR: personal health record.

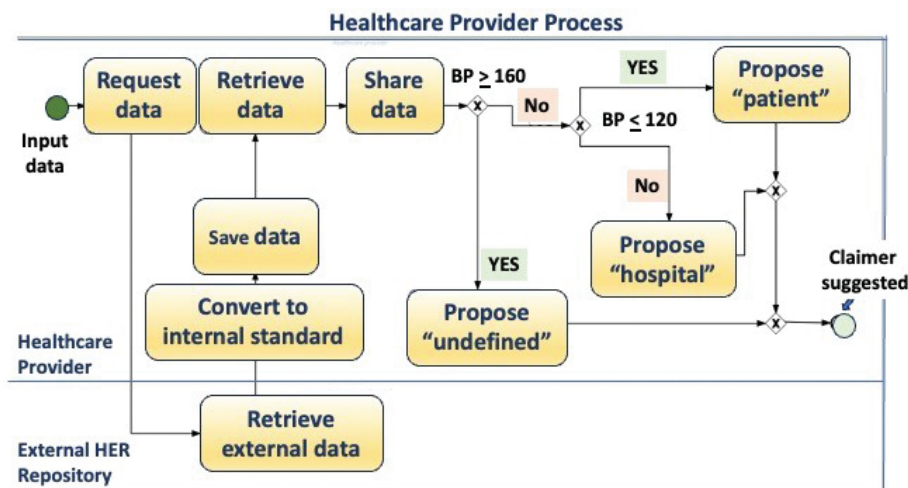


Fig. 9. The internal decision-making process of healthcare providers with regard to claimants. BP: blood pressure (systolic blood pressure in this case).

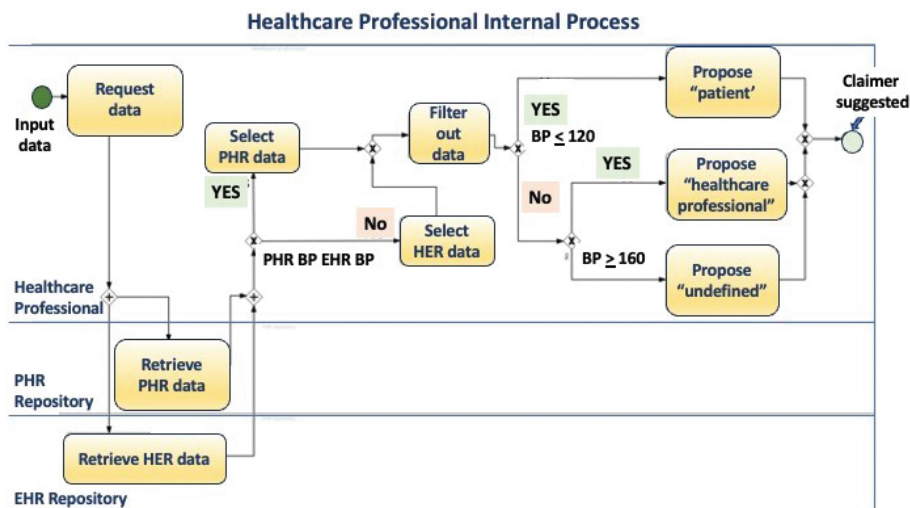


Fig. 10. Healthcare professionals assert that the internal decision-making process plays a crucial role in their practice. BP: blood pressure (systolic blood pressure in this case); EHR: electronic health record; PHR: personal health record.

equal to or less than 120 mm Hg, the patient is suggested as the claimer. The healthcare provider is ultimately suggested as an asserter in the event that the blood pressure falls within the range of 120 and 160 mm Hg.

Figure 10 delineates the internal process of decision-making within the realm of healthcare professionals. Notably, the disparity between the decision-making processes of patients and healthcare providers lies in the healthcare professionals' ability to access both EHR and PHR data. Initially, blood pressure measurements are obtained from both PHR and EHR databases simultaneously. Subsequently, after eliminating extraneous data, the healthcare professional proposes a claimant. In the event that the blood pressure is equal to or below 120 mmHg, the patient is presented with a claim. However, if the blood pressure falls between 120 and 160 mmHg, the claimant remains undefined. Lastly, if the blood pressure surpasses or equals 160 mmHg, the healthcare professional presents himself as a claimant. The incorporation of EHR and PHR integration is founded on our prior research,⁶⁶ while the regulations for the claimant proposal are expounded upon in Figure 6.

The Conflict-Resolution Techniques When Mapping the Bpmn-Designed E-Healthcare Process to a Blockchain System

In this section, we provide the conflict-resolution techniques that support automatic resolution of conflicts occurring in the e-health interorganizational processes. In our running case, two possible conflicts result from internal business rules- or collected medical data differences.

This study posits the utilization of a DAO as a conflict resolution mechanism in decentralized e-health systems. The conflict resolution process for medical data

consistency in the insurance provider process is depicted in Figure 11. Initially, the insurance provider gathers medical data from three sources, namely, patients, healthcare providers, and general practitioners, to prepare a claim. Subsequently, the collected data undergo validation to ascertain its integrity. Following the validation process, the DAO either approves or disapproves the data's validity. Based on the final validation outcome, a claim can be generated.

Figure 12 explains how data validation from a single data source is performed in more detail. The exact process is performed for all three medical data owners: patient, healthcare provider, and general practitioner. The DAO employs a consensus algorithm that necessitates all nodes to reevaluate the incoming data. The data are deemed valid only if a majority of nodes, exceeding 50%, concur that it is accurate. Conversely, if the data fail to garner sufficient agreement, it is regarded as tampered with and consequently unsuitable for utilization in claim preparation.

Finally, the single-node medical data validation process is delineated by Figure 13 within the context of the comprehensive data validation managed by the DAO. Within this process, every blockchain node affiliated with the DAO undertakes an examination of the medical data under scrutiny. The node requests specific medical data, such as a blood pressure reading, from the original data source, such as the patient's PHR system. The node then compares the data from the source to the data being validated on the blockchain. If the data match exactly, the node considers it valid and confirms this through its vote in the consensus algorithm. In the event that the data fail to correspond, a disparity arises between the initial data source and the data stored on the blockchain. Under such

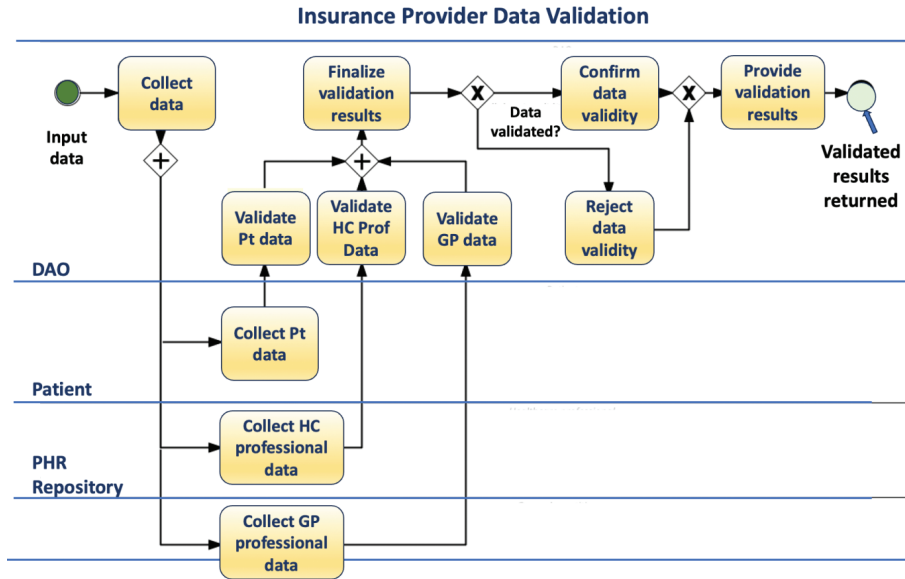


Fig. 11. Insurance provider data conflict resolution process. DAO: Decentralized Autonomous Organizations; Pt: patient; GP: general practitioner; HC: healthcare.

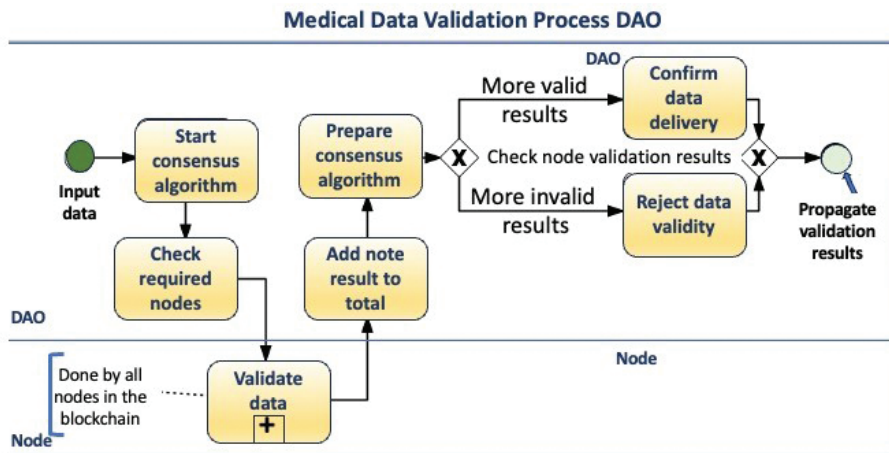


Fig. 12. DAO data validation process. DAO: Decentralized Autonomous Organizations.

circumstances, the node deems the data as either invalid or tampered with, consequently dismissing it through a voting process that opposes its validity within the consensus algorithm.

Having each node directly check the data from the source can identify issues with data tampering, even if a subset of nodes are malicious. The consensus algorithm verifies valid data if most nodes' validation checks succeed. This redundant validation by each node provides greater security and accuracy in identifying data tampering than relying on a centralized validator.

In the decentralized architecture we have proposed, individual units known as 'nodes' participate in a decision-making process to validate the accuracy and integrity of data. Such a process is governed by

a DAO, which serves as a conflict resolver. Each node casts a vote to either confirm or reject the validity of the data in question. Once all votes are collected, a final decision is made based on the majority consensus among the nodes. In essence, if a majority of nodes reach a consensus regarding the validity of the data, it is deemed acceptable; otherwise, it is deemed unacceptable and subsequently rejected. This democratic approach ensures a more robust and transparent validation process.

Evaluation and Discussion

The section provides the evaluation of this work using the multi-method evaluation approach that DSR infers. First, we perform a formal evaluation with CPN and further

provide the discussion of CPN evaluation results and implications of the main results of this work with other related literature. Then, we present a PoC prototype implementing the workflow evaluated by the CPN.

First, we evaluate the conflict-resolution process with CPN modeling. The conflict-resolution process in the CPN model has multiple layers. The top layer is the internal processes of stakeholders. Then, the assessment of the given CPN is presented, followed by the PoC prototype implementation. Finally, the current results compared with similar research discussed.

CPN Formal Evaluation of the Claimer Definition Conflict Resolution Process

The classical Petri net is a directed bipartite graph with two node types called places and transitions. The nodes are connected via directed arcs. Connections between two nodes of the same type are not allowed. Places are represented by circles and transitions by rectangles.⁶⁷

To assess the claimant’s characterization of the conflict resolution process, we propose a structured CPN model⁶⁸ for the identification and rectification of potential design deficiencies, absence of specifications, as well as security and privacy concerns.

The full CPN model description can be found in the technical report.⁶⁸ Our evaluation model focuses on a decentralized data-sharing process and omits all functional goals defined in Figure 4 and Figure 5.

These goals are related to conflict occurrence and resolution. The goals covered by the CPN model are:

- Propose insurance claimer
- Collect data
- Share PHR
- Resolve data conflict
- Resolve claimer conflict.

We use the formalization of the eSourcing framework,⁶⁹ where Workflow nets (WF-nets) are contained. Thus, the CPN models for stakeholders’ internal processes are arranged, so the control flow resembles the eSourcing formalization. WF-net defines the dynamic behavior of a single case in isolation.

WF-nets are a formalization for describing process models in parallel and distributed systems.⁷⁰ Research⁷¹ describes a WF-net as a Petri net that has a 3-tuple $N = (P, T, F)$, where P and T are two disjoint and finite sets that are, respectively, called places (circles visualize them) and transitions (rectangles represent them), and $F \subseteq (P \times T) \cup (T \times P)$ is a set of flow relations in N . The set F is a subset of the union of the cartesian product of P and T with the cartesian product of T and P . $P \times T$ represents the Cartesian product of sets P and T . The cartesian product consists of all possible ordered pairs where the first element is from set P , and the second element is from set T .

Figure 14 depicts the WF-net that has a unique start place and a unique end place with one token in the start place (all other places are empty). All nodes lead from the start to the end place such that when the enactment is complete, only one token is in the unique end place, and all other places are empty.¹¹ It should be noted that a WF-net specifies the dynamic behavior of a single case

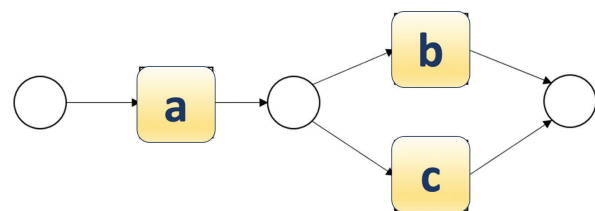


Fig. 14. Workflow net example.⁷²

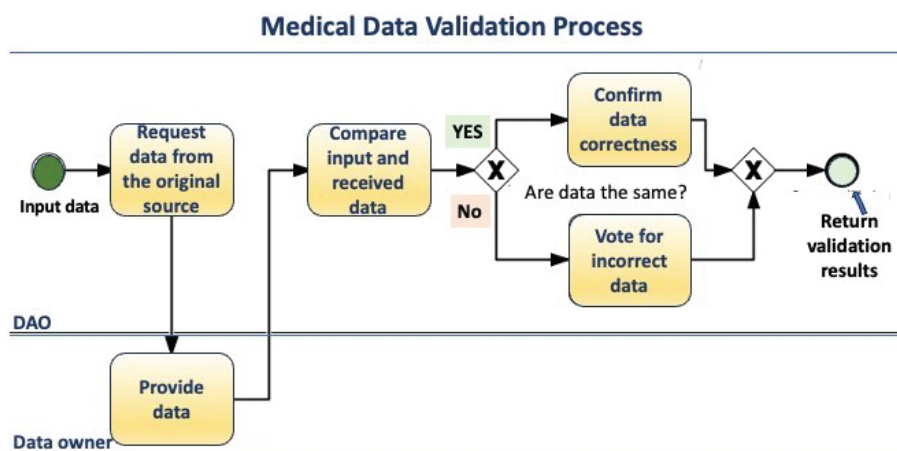


Fig. 13. Node data validation process. DAO: Decentralized Autonomous Organizations.

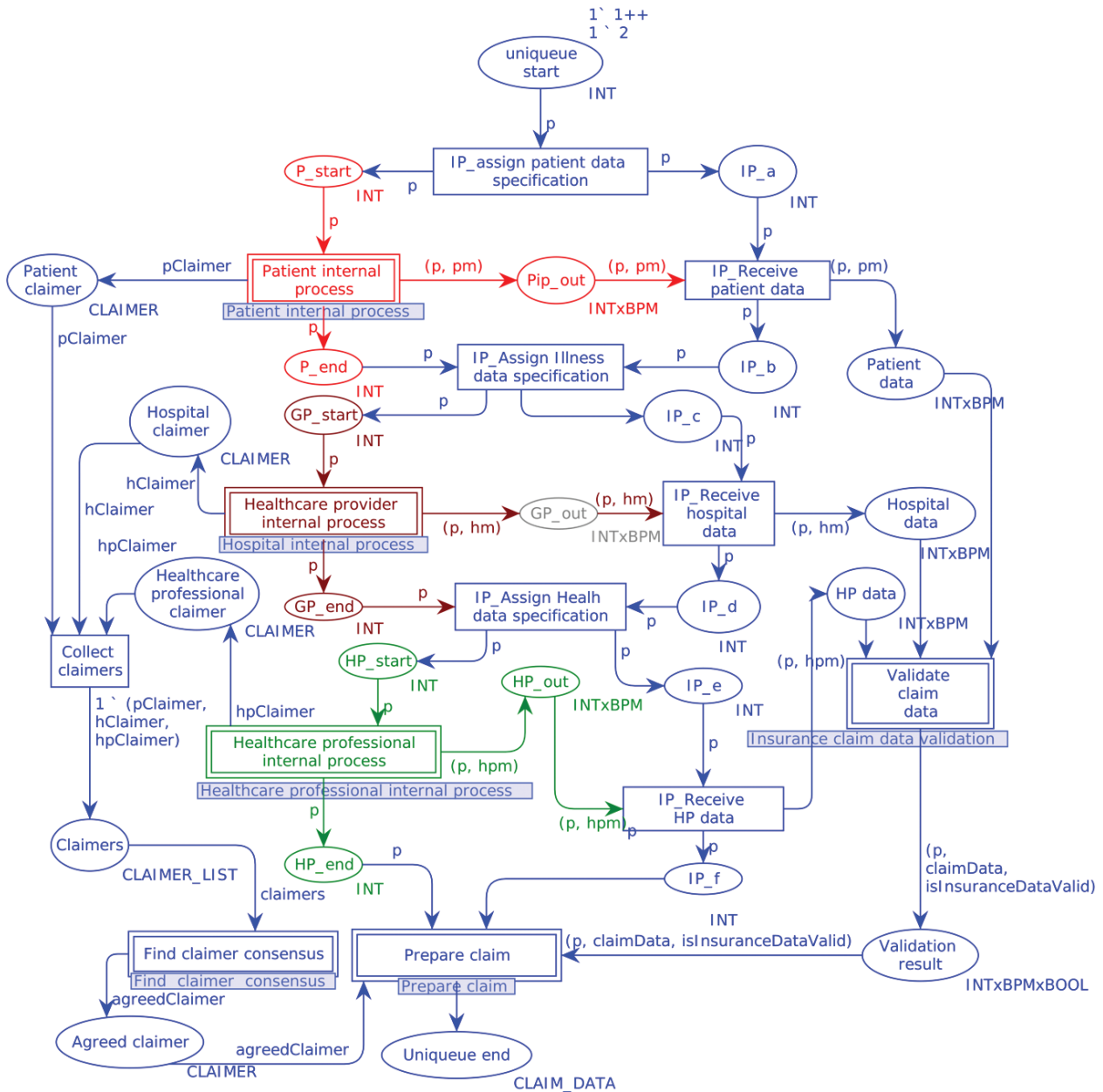


Fig. 15. The CPN model’s external layer defines the interorganizational process. CPN: Colored Petri Nets.

in isolation. This means that every piece of work is executed for a specific case, which is also called a workflow instance.⁶⁷

Formalized Setup Top-Level

Figure 15 illustrates the procedural aspects involved in the formulation of a claim that encompasses multiple organizational entities. To assemble a medical claim, the insurance provider procures healthcare data from diverse origins, such as patient records, healthcare provider systems, and systems utilized by healthcare specialists. Data collection- and claimer definition internal processes involve interaction with stakeholders’ decentralized

systems. We use different colors for internal processes to better visualize an interorganizational process. The patient’s internal process is shown in red, the healthcare provider in brown, and the healthcare professional in green.

Our CPN model is based on the BPMN processes as defined earlier in this article. The whole insurance provider claimer definition process is derived from Figure 10. The CPN layers that define processes encapsulating the internal claimer definition of business logic are based on the BPMN processes. Modeling internal claimer definition processes enables conflict occurrence and simulation when evaluating the CPN model. The mapping between BPMN diagrams and CPN model layers of patient-,

healthcare professional-, and healthcare provider claimer definition processes is shown in Table 2.

The claim preparation process starts from a unique start place with two tokens describing independent process identifiers. The model design supports several parallel process executions when providing process identifiers for each place. All transitions performed by insurance provider are marked with blue color and start with prefix IP_. Subsequently, the initiation of the IP_assign patient data specification transition is instigated, thereby commencing the internal process of the patient. The patient's internal process has two outputs—blood pressure measurement and claimer proposal. The same workflow exists for both healthcare providers and healthcare professionals. The claimer definition is based on the internal rules described in Figure 6.

When all three internal processes are executed, the transition Collect claimers is triggered with three inputs defining the claimer proposed by each stakeholder. The Find claimer consensus transition processes all three proposed claimers and selects one based on the consensus algorithm.

Before a claim can be prepared, another process runs in parallel with the claimer definition—collected blood pressure measurement validation. This process verifies the potential compromise of data and subsequently resolves any discrepancies that may arise in the event of data divergence. After consensus algorithms agree with the claimer and blood pressure measurements, the Prepare claim transition takes place.

Interorganizational Stakeholders' Internal Workflows Processing Integrated EHRs and PHRs

To depict the workflows of different stakeholders, we employ substitution transitions that entail subnets that elaborate on the activities linked to a transition. The subnet that is linked with a transition is commonly denoted as a subpage within academic discourse. The utilization of the CPN formalism enables the hierarchical arrangement of subpages to an indefinite extent, thereby facilitating the representation of system descriptions at diverse levels of intricacy.⁷³

In order to enhance the collaborative scenario we further augment it by incorporating a simulation utilizing CPN. Additionally, we incorporate the conflict scenario into the quantitatively simulatable model. To organize the overall CPN model,² we divide it into multiple subpages, as shown in Table 3.

Figure 16 depicts a screenshot derived from CPN tools, which presents the hierarchical arrangement of subpages within the design model. These subpages, serving

Table 2. Internal claimer definition process mapping from BPMN diagrams to CPN model layers.

BPMN Process	CPN Layer
Patient-claimer internal decision process (Figure 8)	Patient internal process
Healthcare-provider claimer internal decision process (Figure 9)	Healthcare provider internal process
Healthcare professional claimer internal decision process (Figure 10)	Healthcare professional internal process

BPMN: Business Process Model and Notation; CPN: Colored Petri Nets.

as reusable components, contribute to enhancing the comprehensibility of the intricate model. Within this framework, the principal page, referred to as “External,” assumes the role of delineating the interorganizational protocol for the preparation of an insurance claim. The internal procedures of different stakeholders, namely, the Patient internal process, Hospital internal process, and Healthcare professional internal process, are encompassed within separate subpages. Conflict resolution is carried out at a higher level of the process, specifically within the subpages dedicated to Insurance claim data validation and the attainment of consensus among claimants.

CPN Model Evaluation

We assess our model using two different approaches. First, we evaluate the original model through simulation in CPN Tools, ensuring that all initial tokens lead to the unique final state of the model. Given the complexity of the provided CPN model, we conduct a state-space analysis for each subpage individually. If the page incorporates any of the subpages, we imitate its output. This imitation involves substituting the actual execution of the subpage with a single element that generates constant data. By doing so, we maintain the integrity of the main page flow while reducing the complexity of the state-space analysis. The predetermined values are established based on the potential outcomes of the subpage. Throughout the state-space analysis, we compute and present all reachable states and state changes of the CPN model as a directed graph. The graph presents states as nodes and occurring events as arcs. The main goal of the state-space analysis is to describe the system's behavior and check that there are no deadlocks, a given state is always reachable, and the given service is always delivered.⁷¹

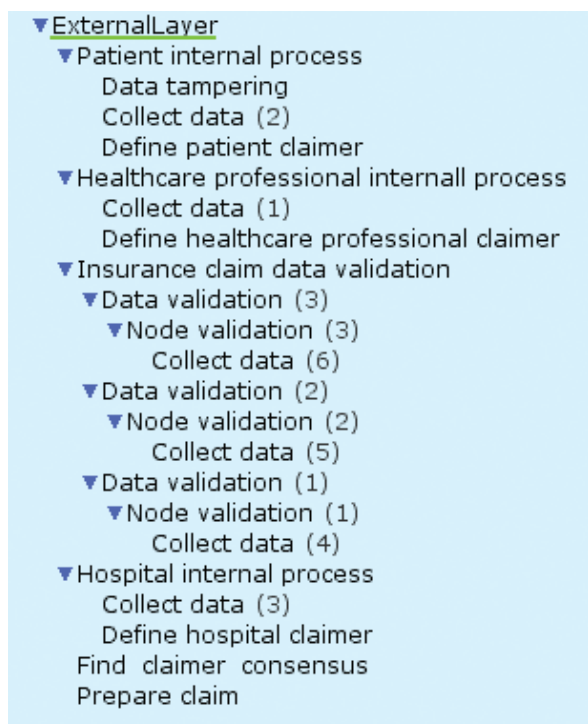
The report on state-space provides an account of both home and liveness properties. The first ones pertain to a specific home marking that is accessible from any reachable marking. In our scenario, each process associated with a subpage will ultimately reach its terminal state. On the other hand, the liveness properties delineate markings without active binding elements. A marking without activity can be both a dead marking

² <https://goo.by/JOQJ8>

Table 3. Subpages in the CPN model's hierarchy.

Subpage	Meaning
Patient internal process	Patient data collection- and claimer definition processes
Hospital internal process	General practitioner data collection- and claimer definition processes
Healthcare professional internal process	Healthcare professional data collection- and claimer definition processes
Data tampering	Data tampering process that takes place during the data collection
Collect data	Data collection process
Define patient claimer	Patient claimer definition process
Define healthcare professional claimer	Healthcare professional claimer definition process
Define hospital claimer	Hospital claimer definition process
Insurance claims data validation	Process of validating all collected data from different stakeholders
Data validation	Process of validating blood pressure measurement by several nodes
Node validation	Blood pressure measurement validation process performed by a single node
Find claimer consensus	Final claimer consensus process

CPN: Colored Petri Nets.

**Fig. 16.** CPN model page hierarchy. CPN: Colored Petri Nets.

and a home marking simultaneously, as any marking can be accessed from itself via a trivial occurrence sequence of zero length. Following this, the state space report delineates live transitions. In an academic context, a transition is deemed live when it is perpetually feasible to identify a sequence of occurrences that include the transition from any attainable marking. The state-space report provides an account of inactive transitions. A transition is classified as inactive if it is either enabled or unattainable. These transitions

delineate the functionality of a model that can never be executed.⁷⁴

All reports analyzing the state space are based on each subpage found within the presented CPN model, as indicated by the corresponding tables provided later. The initial files of the state-space analysis report can be accessed online.³

According to the findings presented in Table 4, it is evident that loops are inherent in the process of data collection. The data repository contains information about various processes, and the data collection process continues to retrieve data until it locates information associated with the ongoing process. All subpages in our process do not contain any dead and live transitions, indicating the absence of unused components. Notably, the state of all subpages aligns with that of home and dead markings.

Proof-of-Concept Prototype Implementation for the Running Case

This study introduces the implementation of a prototype for the e-health data-sharing process⁷⁵ developed in scope of Ref. 76. In our specific context, we propose the utilization of Polygon⁷⁷ Smart Contracts (SCs) for the insurance provider system. At the same time, Ethereum SCs are recommended for the patient, hospital, and healthcare professional systems. The Polygon network is built on a high-throughput blockchain architecture, where each checkpoint selects a group of block producers to achieve consensus. The validation of blocks is conducted through a PoS layer, which also periodically updates the Ethereum mainnet with the proofs provided by the block producers. To enhance scalability and enable interoperability between different blockchain-based systems, we employ Polkadot,⁷⁸ which facilitates secure and trust-free communication among specialized blockchains.

³. <https://goo.by/QaISC>

Table 4. State-space analysis results for CPN model subpages.

Subpage	Loops	Home Marking	Dead Marking	Dead Transitions	Live Transitions
Patient internal process	No	Yes	Yes	No	No
Healthcare professional internal process	No	Yes	Yes	No	No
Hospital internal process	No	Yes	Yes	No	No
Define patient claimer	No	Yes	Yes	No	No
Define healthcare professional claimer	No	Yes	Yes	No	No
Define hospital claimer	No	Yes	Yes	No	No
Find claimer consensus	No	Yes	Yes	No	No
Collect data	Yes	Yes	Yes	No	No
Data tampering	No	No	Yes	No	No
Data validation	No	Yes	Yes	No	No
Node validation	No	Yes	Yes	No	No
External layer	No	Yes	Yes	No	No
Prepare claim	No	Yes	Yes	No	No

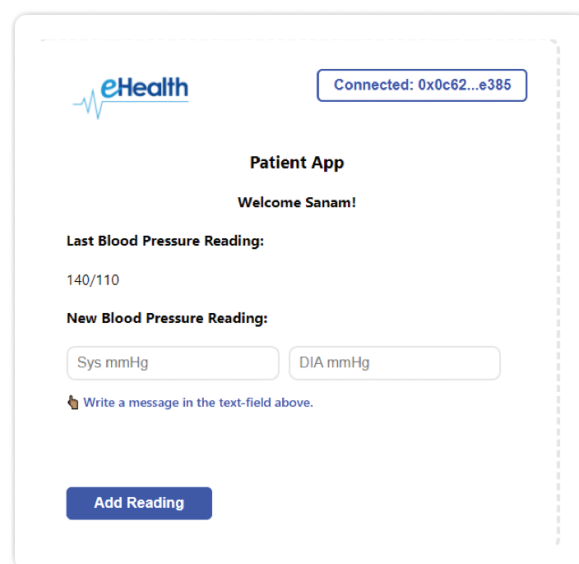
CPN: Colored Petri Nets.

In the decentralized web environment facilitated by the Polkadot foundational layer, users exercise authority over their data. This prototype comprises three primary blockchain-based elements. Specifically, it encompasses two distinct applications for inputting medical records, namely, those of the patient and the doctor. Additionally, it incorporates an application that executes the interorganizational procedure involving the insurance provider alongside a DAO smart contract that undertakes data comparison in the event of conflicts and provides reliable data. The PoC prototype under consideration focuses on the scenario where the patient and doctor input blood pressure measurements.

Figure 17 presents a screenshot of the patient's application interface, explicitly showcasing the input of blood pressure measurements. This application is integrated with the Metamask wallet, enabling the sharing of entered data through a smart contract. Notably, the application incorporates deploying a smart contract on the Ethereum Blockchain.

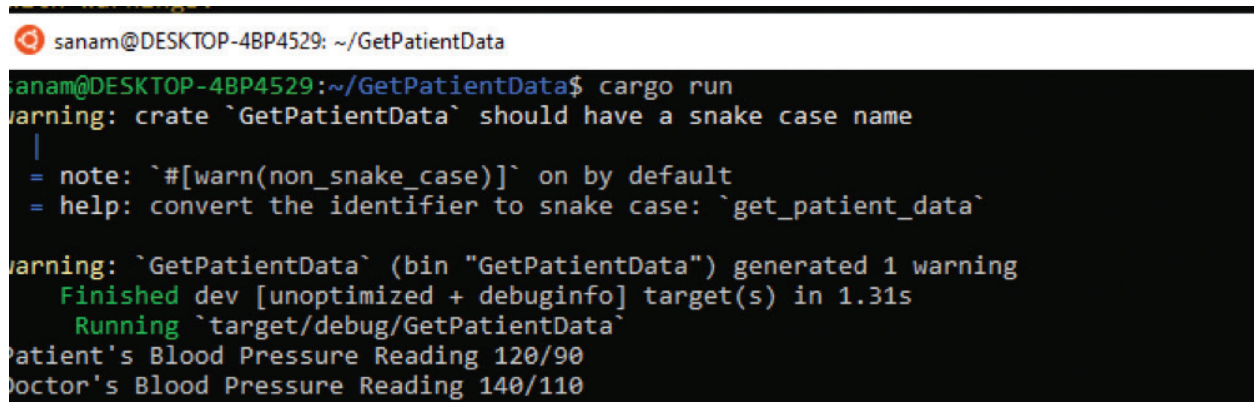
Figure 18 visually represents a conflict that arises while collecting data. The depicted scenario exemplifies a discrepancy between the blood pressure measurements recorded by the patient and those documented by the doctor. In such instances, the data are transmitted to a DAO, which assumes the responsibility of validating the data and resolving any potential conflicts.

The interorganizational process is implemented with the Polkadot parachain that enables cross-blockchain communication. We implement an application-specific blockchain-based module with the Substrate framework.⁷⁹ The insurance provider's application runs as a Substrate backend local node.

**Fig. 17.** Screenshot of a patient's application.

Discussions of Research Implications on Similar Works

This research proposes that blockchain enables autonomous conflict resolution transparently without a single point of trust. Also, blockchain and smart contract technologies support personalized e-health services that include several stakeholders while ensuring the individual's ownership of healthcare data. The rise of the M2X economy and non-human agents in the interorganizational processes require new authentication methods based on the multifactor challenge set mechanism. Such an approach enables new interorganizational processes in situations with a lack of trust between stakeholders. Evaluation with CPN shows that such a process can be feasible with the example of decentralized e-health insurance. Still, we do not have empirical in vivo proof that this is



```

sanam@DESKTOP-4BP4529: ~/GetPatientData
sanam@DESKTOP-4BP4529:~/GetPatientData$ cargo run
warning: crate `GetPatientData` should have a snake case name
|
| = note: `#[warn(non_snake_case)]` on by default
| = help: convert the identifier to snake case: `get_patient_data`
|
warning: `GetPatientData` (bin "GetPatientData") generated 1 warning
Finished dev [unoptimized + debuginfo] target(s) in 1.31s
Running `target/debug/GetPatientData`
Patient's Blood Pressure Reading 120/90
Doctor's Blood Pressure Reading 140/110

```

Fig. 18. Insurance provider's data collection screenshot.

possible; instead, this paper yields the in vitro feasibility proof. The possibility of autonomous conflict resolution in decentralized e-health enables the valuable usage of the person's health data across different industries in a trustable and transparent way. Finally, the implementation of the PoC prototype shows that the running case can be implemented with the current state-of-the-art decentralized technologies.

Our research is based on work by Narendra and colleagues,¹¹ where the authors propose conflict resolution with negotiation depending on the conflict type. This study provides the framework for autonomous participants united in Virtual Enterprises (VE) that proposes the layered structure presenting different business logic contexts. Research shows that conflicts occur on the interorganizational, external layer. Our paper adapts the approach defined in Ref. 11 to the e-health domain. The healthcare use case confirms that conflicts occur in the interorganizational collaboration layer because different stakeholders can have e-health data that differ from each other. Also, the business decisions of each stakeholder can differ from others as all participants have their internal processes.

Stahnke and colleagues⁸⁰ state that blockchain technology enables the enforcement of interorganizational workflows. To establish reliable workflows acceptable to all stakeholders involved in interorganizational processes, it is necessary to design and validate these workflows using CPN before converting them into smart contracts. While CPN is employed to validate interorganizational processes, it is important to acknowledge the requirement for legally relevant smart contracts and the necessary support.

A study by Park and colleagues⁸¹ suggests incorporating Enterprise Resource Planning (ERP) systems into the business process simulation model to utilize real-life data in the CPN-designed simulation process. Park and van der Aalst⁸¹ aim to overcome the complexity of ERP systems by implementing a framework that allows to integrate them into the simulation processes. However, we

differ from this approach as we refrain from introducing real-life components into the simulation due to the sensitive nature of e-health data. Additionally, we assume an unlimited number of stakeholders and their internal systems participating in interorganizational e-health processes. Consequently, the integration of individual systems does not yield any additional value.

In their work, Jadav and colleagues⁸² focused on using AI to discover wearable attacks and share healthcare data with a public blockchain. The authors propose the usage of blockchain technology for data immutability. In our research, we also state that blockchain technology enables e-health data immutability, but we do not focus on AI usage to discover data tampering. Still, the interorganizational process design proposed in this paper allows for integrating non-human actors such as AI agents.

The DeepBlockShield framework proposed by Kim and Kim⁸³ aims to solve medical data leakage issues with blockchain technology. The corresponding solution proposes to store data on a blockchain while providing access to special agents. In our research, we assume that medical data can be stored not only on a blockchain and propose the MFSSIA framework to establish safe collaboration between different stakeholders when sharing the e-health data.

A recent study by Abbas and colleagues⁸⁴ proposed a framework for secure sharing and accessing data from wearable devices, utilizing blockchain technology to ensure data transmission security and management between interconnected nodes. The authors have assessed the effectiveness of their research outcomes in terms of accuracy, precision ratio, average trust value, and response time. In our research, we employed the formal CPN Tools to evaluate the design process and ensure no design issues. Furthermore, our designed process emphasizes resolving data processing conflicts in addition to addressing security concerns.

This article primarily focuses on the technical aspects of blockchain implementation in healthcare data

management, specifically in integrating personal and EHRs. Given this technical orientation, this study does not directly involve human subjects or collected data where race or ethnicity would be relevant factors.

In cases like these, where the research is centered on technology development rather than on human subjects, collecting race or ethnicity data is not applicable. Our study is more concerned with the systemic and technological challenges and solutions in healthcare data integration rather than with end-users' demographic characteristics. However, in the broader deployment context, such factors influence the implementation of healthcare technology and its societal impacts.

Conclusions

In this paper, we research automatic conflict resolution in decentralized e-healthcare systems with blockchain technology. The latter enables autonomous and transparent interorganizational processes and a trustful conflict-resolution mechanism without involving a central authority. Our proposed approach is based on several scientific methods, such as DSR, CPN modeling, and frameworks, such as T-DM, eSourcing, and MFSSIA. We use T-DM for a blockchain-based system-requirement definition to lay the foundation for the system's architecture design, token economy defining on-chain transaction sets, and dynamic protocol development. Also, we map T-DM-defined functional goals where conflicts occur to the BPMN process notations. Finally, we evaluate our research results with CPN as it validates conflict-resolution concepts defined with T-DM in the running process. Our evaluation includes a PoC prototype implementation of the running case. With both the CPN's and prototype's PoC evaluation, we ensure that research can be used in real-time processes.

We propose to use a DAO as an automatic conflict-resolver when processing and mapping personal e-health data into interorganizational processes. The requirements for automatic conflict resolution are the creation of both PHR and EHR data by several stakeholders in the decentralized environment. Such stakeholders shall be onboarded and authenticated with MFSSIA to agree on the e-health data sharing and usage conflict-resolution techniques used by a DAO. The e-health data from different sources shall be merged before its usage. After defining the requirement to the e-health data collection and processing, we propose two types of conflicts—internal business rule and data difference conflicts. Finally, we propose that in case of a data-difference conflict, the decentralized system rechecks the data by several nodes and then decides which data are correct.

There are several limitations inherent in our research. First, we need to comprehensively evaluate the integrated MFSSIA in the context of interorganizational data-sharing processes. Additionally, this study has

not thoroughly defined the specific challenges faced in implementing e-health systems. Furthermore, the concept of a token economy, which involves the sharing of community income between content producers and service users who contribute value, is beyond the scope of this paper. Consequently, the aspects of the token economy and transaction costs are not addressed in our research.

Preserving user data privacy is of utmost importance, as failure to do so can have legal implications. However, this study does not explore the legal aspects related to privacy protection in user data. Therefore, the acceptance and implementation of the proposed techniques are contingent upon the legal jurisdiction of the country and the hospital's compliance with relevant laws and regulations.

We work on the e-health-specific challenge-set rules for MFSSIA. After implementing a PoC prototype, we plan to collaborate with healthcare providers to test our research results with real use cases. Also, future work is related to solving the challenges associated with the heterogeneity of the socioadministrative environment. In the proposed design, we define agreements between stakeholders with immutable smart contracts. The future work is related to overcoming this challenge with e-health smart-contract lifecycle development that enables the adoption of the changes in real-life agreements to the ones defined by smart contracts.

Finally, interoperability of e-healthcare data is one of the biggest challenges in e-healthcare. Using common standards, such as SNOMED CT, HL7, LOINC, etc., aims to solve this issue. At the same time, as we consider the interorganizational process to be flexible and to support an unlimited number of stakeholders, there are challenges related to data privacy and interoperability. We assume that both human- and non-human participants in the M2X context must authenticate with the MFSSIA framework to access such processes. As MFSSIA uses challenge sets and responses-based identity authentication, the supported e-health data standards can be a part of challenge sets that will be developed in the future. Future work also includes adopting AI agents that can be utilized in different interorganizational process phases, such as MFSSIA authentication, e-health data collection, and conflict resolution, with more to come.

Funding Statement

No funding.

Financial and Non-Financial Relationship and Activities

Dr. Norta is a BHTY Editorial Board member—no other disclosures to report.

Contributors

All authors contributed to this paper. Aleksandr Kormilt-syn wrote the article and performed research. Alex Norta supervised the article and gave feedback. Chibuzor Udokwu and Vimal Dwivedi edited the paper and gave feedback. Sanam Nisar developed a proof-of-concept prototype.

References

- Susskind RE, Susskind D. *The future of the professions: how technology will transform the work of human experts*. Oxford University Press; 2015.
- Mercille J. Privatization in the Irish hospital sector since 1980. *J Public Health*. 2018;40:863–70. <https://doi.org/10.1093/pubmed/fdy027>
- Archer N, Fevrier-Thomas U, Lokker C, McKibbin KA, Straus SE. Personal health records: a scoping review. *J Am Med Inform Assoc*. 2011;18:515–22. <https://doi.org/10.1136/amiajnl-2011-000105>
- Levitan B, Getz K, Eisenstein EL, Goldberg M, Harker M, Hesterlee S, et al. Assessing the financial value of patient engagement: a quantitative approach from CTTI's Patient Groups and Clinical Trials project. *Ther Innov Regul Sci*. 2018;52:220–9. <https://doi.org/10.1177/2168479017716715>
- Dimitrov DV. Medical internet of things and big data in healthcare. *Health Inform Res*. 2016;22:156–63. <https://doi.org/10.4258/hir.2016.22.3.156>
- Kormiltsyn A, Udokwu C, Karu K, Thangalimodzi K, Norta A. Improving healthcare processes with smart contracts. In: *Proceedings of the international conference on business information systems*. Springer, 2019; pp. 500–13.
- Norta A, Hawthorne D, Engel SL. A privacy-protecting data-exchange wallet with ownership-and monetization capabilities. In: *Proceedings of the 2018 International Joint Conference on Neural Networks (IJCNN)*. IEEE, 2018; pp. 1–8.
- Eccher C, Piras EM, Stenico M. TreC - a REST-based Regional PHR. *User Centred Networked Health Care A*. Moen et al. (Eds.) IOS Press, 2011. <https://doi.org/10.3233/978-1-60750-806-9-108>
- Urbauer P, Sauermaun S, Frohner M, Forjan M, Pohn B, Mense A. Applicability of IHE/Continua components for PHR systems: learning from experiences. *Comput Biol Med*. 2015;59:186–93. <https://doi.org/10.1016/j.compbiomed.2013.12.003>
- Zhang R, Liu L. Security models and requirements for healthcare application clouds. In *Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing*. IEEE, 2010; pp. 268–75.
- Narendra NC, Norta A, Mahunnah M, Ma L, Maggi FM. Sound conflict management and resolution for virtual-enterprise collaborations. *Serv Oriented Comput Appl*. 2016;10:233–51. <https://doi.org/10.1007/s11761-015-0183-0>
- Szabo N. *Smart contracts: building blocks for digital markets*. EXTROPY J Transhumanist Thought. 1996;18:2.
- European Union. Charter of fundamental rights of The European Union [Internet]. Europa.eu; 2012 [cited 2023 Jun 15]. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012P/TXT>
- Standard Contractual Clauses (SCC) [Internet]. European Commission—European Commission. [cited 2023 Jun 15]. Available from: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-ccc_en
- Introduction to the hash function as a personal data pseudonymisation technique. European Data Protection Supervisor [Internet]. edps.europa.eu. 2023 [cited 2023 Nov 15]. Available from: https://edps.europa.eu/data-protection/our-work/publications/papers/introduction-hash-function-personal-data_en
- Sun W, Cai Z, Li Y, Liu F, Fang S, Wang G. Security and privacy in the medical internet of things: a review. *Secur Commun Netw*. 2018;2018:5978636. <https://doi.org/10.1155/2018/5978636>
- Al-Muhtadi J, Shahzad B, Saleem K, Jameel W, Orgun MA. Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment. *Health Inform J*. 2019;25:315–29. <https://doi.org/10.1177/1460458217706184>
- Katurura M, Cilliers L. A review of the implementation of electronic health record systems on the African continent. In: *Proceedings of the African Computer and Information System & Technology Conference*. 2017; pp. 10–11.
- Cilliers L. Wearable devices in healthcare: privacy and information security issues. *Health Inf Manag J*. 2019;49(2–3):150–6. <https://doi.org/10.1177/1833358319851684>
- Luo E, Bhuiyan MZA, Wang G, Rahman MA, Wu J, Atiqzaman M. Privacyprotector: privacy-protected patient data collection in IoT-based healthcare systems. *IEEE Commun Mag*. 2018;56:163–8. <https://doi.org/10.1109/MCOM.2018.1700364>
- Hussein AF, ArunKumar N, Ramirez-Gonzalez G, Abdulhay E, Tavares JMR, de Albuquerque VHC. A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform. *Cogn Syst Res*. 2018;52:1–11. <https://doi.org/10.1016/j.cogsys.2018.05.004>
- Zhang P, White J, Schmidt DC, Lenz G, Rosenbloom ST. Fhir-chain: applying blockchain to securely and scalably share clinical data. *Comput Struct Biotechnol J*. 2018;16:267–78. <https://doi.org/10.1016/j.csbj.2018.07.004>
- Azorin-Lopez J, Fuster-Guillo A, Saval-Calvo M, Bradley D. Home technologies, smart systems and eHealth. In: *Mechatronic futures*. Springer, 2016; pp. 179–200.
- Dittmar A, Meffre R, De Oliveira F, Gehin C, Delhomme G. Wearable medical devices using textile and flexible technologies for ambulatory monitoring. In: *Proceedings of the 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference*. IEEE, 2006; pp. 7161–4.
- Sebestyen G, Hangan A, Oniga S, Gál Z. eHealth solutions in the context of Internet of Things. In: *Proceedings of the 2014 IEEE International Conference on Automation, Quality and Testing, Robotics*. IEEE, 2014; pp. 1–6.
- Salehi S, Giacalone M. Conflict resolution with equitable algorithms: a tool to establish a European common ground of available rights. In: F. Romeo, S. Martuccelli & M. Giacalone (Eds.). *The European common ground of available rights*. Napoli: Editoriale Scientifica; 2009, p.111.
- Xu H, Hipel KW, Kilgour DM, Fang L. *Conflict resolution using the graph model: strategic interactions in competition and cooperation*. Springer, 2018.
- Neyens G. Conflict handling for autonomic systems. In: *Proceedings of the 2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS* W)*. IEEE, 2017; pp. 369–70.
- Priya KF, Patil NN. Resolving privacy conflict for maintaining privacy policies in online social networks. *Int J Comput Eng Technol*. 2019;10:94–101. <https://doi.org/10.34218/IJCET.10.3.2019.011>
- Hölbl M, Kompara M, Kamišalić, A, Nemeč Zlatolal L. A systematic review of the use of blockchain in healthcare. *Symmetry*. 2018;10:470. <https://doi.org/10.3390/sym10100470>

31. Agbo CC, Mahmoud QH, Eklund JM. Blockchain technology in healthcare: a systematic review. In: *Proceedings of the health-care. Multidisciplinary Digital Publishing Institute*, 2019; Vol. 7, p. 56.
32. McGhin T, Choo KKR, Liu CZ, He D. Blockchain in health-care applications: research challenges and opportunities. *J Netw Comput Appl.* 2019;135:62–75. <https://doi.org/10.1016/j.jnca.2019.02.027>
33. Swan M. *Blockchain: blueprint for a new economy.* O'Reilly Media, Inc; 2015.
34. Buterin V. *A next generation smart contract & decentralized application platform.* Whitepaper. Ethereum Foundation; 2013.
35. Becker G. Merkle signature schemes, merkle trees and their cryptanalysis. Ruhr-University Bochum, Tech. Rep; 2008.
36. Hevner A, Chatterjee S. Design science research in information systems. *Integrated Series in Information Systems.* 2010; pp. 9–22.
37. Westaway MD, Stratford PW, Binkley JM. The patient-specific functional scale: validation of its use in persons with neck dysfunction. *J Orthop Sports Phys Ther.* 1998;27:331–8. <https://doi.org/10.2519/jospt.1998.27.5.331>
38. Nguyen GT, Kim K. A survey about consensus algorithms used in blockchain. *J Inf Process Syst.* 2018;14:101–28.
39. Bitcoin—Open source P2P money [Internet]. bitcoin.org. [cited 2023 Jun 15]. Available from: <https://bitcoin.org>
40. Home | Ethereum [Internet]. [ethereum.org](https://www.ethereum.org). 2019 [cited 2023 Jun 15]. Available from: <https://www.ethereum.org>
41. Hyperledger Fabric—Hyperledger [Internet]. Hyperledger; 2017 [cited 2023 Jun 15]. Available from: <https://www.hyperledger.org/projects/fabric>
42. Udokwu C, Kormiltsyn A, Thangalimodzi K, Norta A. The state of the art for blockchain-enabled smart-contract applications in the organization. In: *Proceedings of the 2018 Ivannikov Ispras Open Conference (ISPRAS).* IEEE, 2018; pp. 137–44.
43. Weyl EG, Ohlhaber P, Buterin V. *Decentralized society: Finding Web3's soul.* Available at SSRN 4105763 2022.
44. Thematic Report [Internet]. Available from: https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf
45. Damjan M. The interface between blockchain and the real world. In: *Ragion pratica.* 2018; pp. 379–406.
46. Caldarelli G, Ellul J. The blockchain oracle problem in decentralized finance—a multivocal approach. *Appl Sci.* 2021;11:7572. <https://doi.org/10.3390/app11167572>
47. Liu L, Zhou S, Huang H, Zheng Z. From technology to society: an overview of blockchain-based DAO. *IEEE Open J Comput Soc.* 2021.
48. Grefen P, Aberer K, Hoffner Y, Ludwig H. CrossFlow: cross-organizational workflow management in dynamic virtual enterprises. *Comput Syst Sci Eng.* 2000;1:277–90.
49. Rahmani AM, Thanigaivelan NK, Gia TN, Granados J, Negash B, Liljeberg P, et al. Smart e-health gateway: bringing intelligence to internet-of-things based ubiquitous health-care systems. In: *Proceedings of the 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC).* IEEE, 2015; pp. 826–34.
50. Leiding B, (sup) Dieter Hogrefe, Clemens HC, Norta A. *The M2X economy—business interactions, transactions and collaborations among autonomous smart devices.* PhD thesis, Georg-August-Universitaet Goettingen, 2019.
51. Shiang CW, Meyer JJ, Taveter K. Agent-oriented methodology for designing cognitive agents for serious games. *Engineering multi-agent systems.* 2016; p. 39.
52. Barr ET, Harman M, McMinn P, Shahbaz M, Yoo S. The oracle problem in software testing: a survey. *IEEE Trans Softw Eng.* 2014;41:507–25. <https://doi.org/10.1109/TSE.2014.2372785>
53. Norta A, Mahunnah M, Tenso T, Taveter K, Narendra NC. An agent-oriented method for designing large socio-technical service-ecosystems. In: *Proceedings of the 2014 IEEE World Congress on Services.* IEEE, 2014; pp. 242–9.
54. Sherkat M, Mendoza A, Miller T, Burrows R. Emotional attachment framework for people-oriented software. *arXiv preprint arXiv:1803.08171* 2018.
55. Kormiltsyn A. *A systematic approach to define requirements and engineer the ontology for semantically merging data sets for personal-centric healthcare systems.* 2018.
56. Sherkat M. *Emotionalism in software engineering.* PhD thesis, 2019.
57. Mendoza A, Miller T, Pedell S, Sterling L, et al. The role of users' emotions and associated quality goals on appropriation of systems: two case studies. In: *Proceedings of the 24th Australasian Conference on Information Systems.* 2013.
58. Avizienis A, Laprie JC, Randell B, Landwehr C. Basic concepts and taxonomy of dependable and secure computing. *IEEE Trans Dependable Secure Comput.* 2004;1:11–33. <https://doi.org/10.1109/TDSC.2004.2>
59. Abouelmehdi K, Beni-Hessane A, Khaloufi H. Big healthcare data: preserving security and privacy. *J Big Data.* 2018;5:1. <https://doi.org/10.1186/s40537-017-0110-7>
60. Fulpagare Priya K, Patil NN. *Conflict detection techniques for preserving privacy in social media.* 2018.
61. Udokwu C, Norta A. Deriving and formalizing requirements of decentralized applications for inter-organizational collaborations on blockchain. *Arab J Sci Eng.* 2021;46:8397–8414. <https://doi.org/10.1007/s13369-020-05245-4>
62. Jensen K, Kristensen LM. *Coloured Petri nets: modelling and validation of concurrent systems.* Springer Science & Business Media, 2009.
63. Mahunnah M, Norta A, Ma L, Taveter K. Heuristics for designing and evaluating socio-technical agent-oriented behaviour models with coloured petri nets. In: *Proceedings of the Computer Software and Applications Conference Workshops (COMP-SACW), 2014 IEEE 38th International.* IEEE, 2014; pp. 438–43.
64. Norta A, Kormiltsyn A, Udokwu C, Dwivedi V, Aroh S, Nikolajev I. A blockchain implementation for configurable multi-factor challenge-set self-sovereign identity authentication. In: Ezzat SK, Saleh YN, Abdel-Hamid AA (Eds.). *Blockchain Oracles: state-of-the-art and research directions.* IEEE Access; 2022.
65. Riley L. *Universal DLT interoperability is now a practical reality.* Hyperledger Foundation Blog [Internet]. 2021 [cited 2023 Oct 7]. Available from: <https://www.hyperledger.org/blog/2021/05/10/universal-dlt-interoperability-is-now-a-practical-reality>
66. Kormiltsyn A, Norta A. Dynamically integrating electronic-with personal health records for ad-hoc healthcare quality improvements. In: *Proceedings of the International Conference on Digital Transformation and Global Society.* Springer, 2017; pp. 385–99.
67. Norta AH. *Exploring dynamic inter-organizational business process collaboration* [Internet]. 2007 [cited 2023 Oct 7]. Available from: <https://research.tue.nl/files/2003544/200710444.pdf>
68. Kormiltsyn A, Norta A. *Formal evaluation of privacy-conflict resolution for integrating personal-and electronic health records in blockchain-based systems.* Technical report. 2022.

69. Norta A, Eshuis R. Specification and verification of harmonized business-process collaborations. *Inf Syst Front*. 2010;12:457–79. <https://doi.org/10.1007/s10796-009-9164-1>
70. Zhao F, Xiang D, Liu G, Jiang C. A new method for measuring the behavioral consistency degree of WF-net systems. *IEEE Trans Comput Soc Syst*. 2021;9:480–93. <https://doi.org/10.1109/TCSS.2021.3099475>
71. Weidlich M. Behavioural profiles: a relational approach to behaviour consistency. PhD thesis, Universität Potsdam; 2011.
72. Workflow Nets—ML Wiki [Internet]. mlwiki.org. [cited 2023 Jul 11]. Available from: http://mlwiki.org/index.php/Workflow_Nets
73. Gehlot V, Sloane E, Thalassinidis AE. Personal health technology: CPN based modeling of coordinated neighborhood care environments (hubs) and personal care device ecosystems. 2019.
74. Jensen K, Kristensen LM, Wells L. Coloured Petri Nets and CPN Tools for modelling and validation of concurrent systems. *Int J Softw Tools Technol Transf*. 2007;9:213–54. <https://doi.org/10.1007/s10009-007-0038-x>
75. sanamnisarmalik. sanamnisarmalik/hprivacyconflictresolutionbyblockchain [Internet]. GitHub. 2022 [cited 2023 Sep 25]. Available from: <https://github.com/sanamnisarmalik/hprivacyconflictresolutionbyblockchain>
76. Nisar S. Defining blockchain-based techniques for privacy conflict-resolution in cross-organizational processes for e-health systems. Master's thesis, University of Tartu, Faculty of Science and Technology Institute of Computer Science; 2022.
77. Blockchains for mass adoption [Internet]. polygon.technology. [cited 2023 Jun 15]. Available from: <https://polygon.technology>
78. Polkadot: Web3 Interoperability | Decentralized blockchain [Internet]. Polkadot Network. [cited 2023 Oct 4]. Available from: <https://www.polkadot.network/>
79. Substrate And Polkadot | Substrate_ [Internet]. substrate.io. [cited 2023 Jun 15]. Available from: <https://substrate.io/vision/substrate-and-polkadot/>
80. Stahnke S, Shumaiev K, Cuellar J, Kasinathan P. Enforcing a cross-organizational workflow: an experience report. In: *Proceedings of the Enterprise, Business-Process and Information Systems Modeling: 21st International Conference, BPMDS 2020, 25th International Conference, EMMSAD 2020, Held at CAiSE 2020, Grenoble, France, June 8–9, 2020, Proceedings 21*. Springer, 2020; pp. 85–98.
81. Park G, van der Aalst WM. Towards reliable business process simulation: a framework to integrate ERP systems. In *Proceedings of the Enterprise, Business-Process and Information Systems Modeling: 22nd International Conference, BPMDS 2021, and 26th International Conference, EMMSAD 2021, Held at CAiSE 2021, Melbourne, VIC, Australia, June 28–29, 2021, Proceedings*. Springer, 2021; pp. 112–27.
82. Jadav D, Jadav NK, Gupta R, Tanwar S, Alfarraj O, Tolba A, et al. A trustworthy healthcare management framework using amalgamation of AI and blockchain network. *Mathematics*. 2023;11:637. <https://doi.org/10.3390/math11030637>
83. Kim J, Kim M. DeepBlockShield: blockchain agent-based secured clinical data management model from the deep web environment. *Mathematics*. 2021;9:1069. <https://doi.org/10.3390/math9091069>
84. Abbas A, Alroobaea R, Krichen M, Rubaiee S, Vimal S, Almansour FM. Blockchain-assisted secured data management framework for health information analysis.

Copyright Ownership: This is an open-access article distributed in accordance with the Creative Commons Attribution Non-Commercial (CC BY-NC 4.0) license, which permits others to distribute, adapt, enhance this work non-commercially, and license their derivative works on different terms, provided the original work is properly cited, and the use is non-commercial. See: <http://creativecommons.org/licenses/by-nc/4.0>.

Appendix

3-tuple N: A tuple is a finite sequence or ordered list of numbers or, more generally, mathematical objects, which are called the elements of the tuple. A 3-tuple is called a triple (or triplet). The number n can be any non-negative integer.

Agent-oriented modeling (AOM): Used in organization and information system modeling for providing intentional descriptions of processes as a network of relationships among actors. As such, they capture and represent goals, dependencies, intentions, beliefs, alternatives, etc.

Algorithmic decision systems (ADS): The delegation of decision-making and implementation to machines.

Bipartite graph: A graph where the vertices can be divided into two disjoint sets such that all edges connect a vertex in one set to a vertex in another set.

Business Process Model and Notation (BPMN): A graphical representation for specifying business processes in a business process model.

Colored Petri Net (CPN)⁶⁹ Model: Backward-compatible extension of the mathematical concept of Petri nets.

Colored Petri Nets (CPNs): Extend the vocabulary of ordinary Petri Nets and add features that make them suitable for modeling large systems.

Copyright Ownership: This is an open-access article distributed in accordance with the Creative Commons Attribution Non-Commercial (CC BY-NC 4.0) license, which permits others to distribute, adapt, and enhance this work non-commercially, and license their derivative works on different terms, provided the original work is properly cited, and the use is non-commercial. See: <http://creativecommons.org/licenses/by-nc/4.0>.

Decentralized Autonomous Organizations (DAOs): An entity in which all members participate in decision-making because there is no central authority.

Article 7 in the Charter of Fundamental Rights of the European Union: As defined in the Charter of Fundamental Rights of the European Union,¹³ Article 7 is the right of any individual to respect their private and family life, home, and correspondence.

DeepBlockShield: A model that implements secure sharing of clinical data. It adopts a two-way user verification and asynchronous information provision methodology to enhance the security of clinical data.

Design Science Research Cycles: The process that includes six steps: problem identification and motivation, objectives for a solution, design and development, evaluation, and communication.

Design-science research (DSR): Research that invents a new purposeful artifact to address a generalized type of problem and evaluates its utility for solving problems of that type.

Electronic Health (EHR): A patient's data created by healthcare professionals and stored digitally.

Enterprise Resource Planning (ERP): A type of software that organizations use to manage their day-to-day activities and streamline business processes. ERP systems integrate various functions across different departments, such as finance, human resources, procurement, manufacturing, supply chain management, and more, into a single unified platform.

Ethereum mainnet: The primary public Ethereum production blockchain, where actual-value transactions occur on the distributed ledger. Ethereum uses a proof-of-stake (PoS) where validation is based not on the resources spent on mathematical problem-solving but on a node's reputation.

European Data Protection Board (EDPB): European Union independent body with juridical personality whose purpose is to ensure consistent application of the General Data Protection Regulation and to promote cooperation among the EU's data protection authorities.

Graph Model for Conflict Resolution (GMCR): A flexible tool for use in strategic management within a competitive environment.

Health Level Seven International (HL7): A clinical result reporting standard that is now ubiquitous in healthcare systems around the world.

Hidden Markov Models (HMM): Sequence models. That is, given a sequence of inputs, such as words, an HMM will compute a sequence of outputs of the same length. An HMM model is a graph where nodes are probability distributions over labels and edges, giving the probability of transitioning from one node to the other.

Internet of Things (IoT): The collective network of connected devices and the technology that facilitates communication between devices and the cloud, as well as between the devices themselves.

Logical Observation Identifiers Names and Codes (LOINC®): Clinical terminology that is important for laboratory test orders and results and is one of a suite of designated standards for use in U.S. Federal Government systems for the electronic exchange of clinical health information.

Merkle tree or hash tree: Ensures that the transactions stored on a blockchain are correlated through mathematical hashes.

Metamask wallet: Software cryptocurrency wallet used to interact with the Ethereum blockchain.

Multi-agent systems (MAS): A computerized system composed of multiple interacting intelligent agents. Multiagent systems can solve problems that are difficult or impossible for an individual agent or a monolithic system to solve.

Multifactor challenge-set self-sovereign identity authentication (MFSSIA): Enables cross-blockchain interoperability by utilizing blockchain oracles.

Parachains: Blockchains connected to the relay chain of Polkadot or Kusama. They are application-specific data structures that validate transactions using the relay chain, an underlying structure that supports secure communication between all connected blockchains, also known as parachains.

Personal health record (PHR): An individual's electronic health-related information.

Personal Health Token (PHT): A utility token for the decentralized person-centric e-health system.

Polkadot: Enables cross-blockchain transfers of any type of data or asset, not just tokens. Connecting to Polkadot gives the ability to interoperate with a wide variety of blockchains in the Polkadot network.

Proof-of-concept (PoC): Also known as proof of principle, it is a realization of a certain method or idea in order to demonstrate its feasibility or a demonstration in principle with the aim of verifying that some concept or theory has practical potential. A proof of concept is usually small and may or may not be complete.

Proof-of-work (PoW) consensus algorithm: A decentralized consensus mechanism that requires network members to expend effort in solving an encrypted hexadecimal number. Proof of work is also called mining, in reference to receiving a reward for work done.

SNOMED CT or SNOMED: A systematically organized computer-processable collection of medical terms providing codes, terms, synonyms, and definitions used in clinical documentation and reporting.

Software Development Lifecycle (SDLC): The cost-effective and time-efficient process that development teams use to design and build high-quality software. The goal of SDLC is to minimize project risks through forward planning so that software meets customer expectations during production and beyond.

“Soulbound” tokens (SBT): A type of token that can only be owned and transferred by a specific address. This means that once a Soulbound token is created and assigned to an address, it cannot be transferred or owned by any other address.

Spanish Data Protection Authority (AEPD): An independent agency of the government of Spain that oversees the compliance with the legal provisions on the protection of personal data.

Standard Contractual Clauses (SCC): Documentation by the EC; this update is a significant step in ensuring robust and up-to-date data protection measures in cross-border data transfers.

Test Data Management (TDM): The process for providing controlled data access to modern teams throughout the Software Development Lifecycle (SDLC).

Utility- and non-transferable “soulbound” tokens (SBT): Also called “a non-transferable token,” it is a type of NFT that cannot be transferred or sold to another wallet. These types of tokens are often used to represent credentials, affiliations, achievements, or memberships.

WF-nets: A formalization for describing process models in parallel and distributed systems.