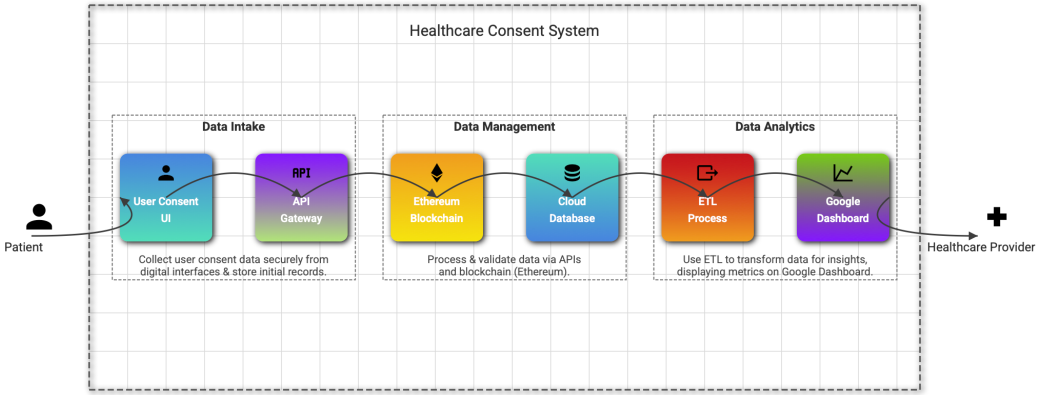
Graphical Abstract

Building Trust in Healthcare with Privacy Techniques: Blockchain in the Cloud

Ferhat Ozgur Catak, Chunming Rong, Øyvind Meinich-Bache, Sara Brunner, Kjersti Engan


Healthcare Consent System
Data Intake
Data Management
Data Analytics
Patient
User Consent UI
API
API Gateway
Ethereum Blockchain
Cloud Database
ETL Process
Google Dashboard
Healthcare Provider
Collect user consent data securely from digital interfaces & store initial records.
Process & validate data via APIs and blockchain (Ethereum).
Use ETL to transform data for insights, displaying metrics on Google Dashboard.

Highlights

Building Trust in Healthcare with Privacy Techniques: Blockchain in the Cloud

Ferhat Ozgur Catak, Chunming Rong, Øyvind Meinich-Bache, Sara Brunner, Kjersti Engan

- **Blockchain-Driven Consent Management:** Developed a novel digital consent platform that leverages Ethereum blockchain and smart contracts to securely record, manage, and audit patient consent in healthcare. This solution ensures immutability, transparency, and tamper-proof recordkeeping.

- **Enhanced Privacy and Data Security:** Integrated advanced encryption techniques and data minimization principles to protect sensitive patient information while complying with privacy regulations such as GDPR. The decentralized architecture reduces the risk associated with centralized data breaches.

- **Cloud-Integrated Architecture:** Combined cloud computing with blockchain technology to enable a scalable infrastructure. The architecture supports secure video data collection and real-time consent verification, vital for projects like NewbornTime that aim to improve newborn care.

- **User-Friendly Analytics Dashboard:** Designed an intuitive, feature-rich dashboard that allows healthcare providers and researchers to monitor consent trends and access actionable insights. This enhances the decision-making process and bridges the gap between complex technologies and everyday clinical practice.

- **Performance and Scalability Evaluation:** Conducted extensive experimental analysis of gas consumption, transaction throughput, and scalability. The insights gained provide a solid foundation for further optimization and larger-scale deployment in healthcare settings.

Building Trust in Healthcare with Privacy Techniques: Blockchain in the Cloud

Ferhat Ozgur Catak[a], Chunming Rong[a], Øyvind Meinich-Bache[a], Sara Brunner[b], Kjersti Engan[a]

[a] *Department of Electrical Engineering and Computer Science, University of Stavanger, Kjell Arholms gate 41, Stavanger, 4021, Rogaland, Norway*
[b] *Laerdal Medical, Tanke Svilands gate 30, Stavanger, 4007, Rogaland, Norway*

Abstract

This study introduces a cutting-edge architecture developed for the NewbornTime project, which uses advanced AI to analyze video data at birth and during newborn resuscitation, with the aim of improving newborn care. The proposed architecture addresses the crucial issues of patient consent, data security, and investing trust in healthcare by integrating Ethereum blockchain with cloud computing. Our blockchain-based consent application simplifies patient consent's secure and transparent management. We explain the smart contract mechanisms and privacy measures employed, ensuring data protection while permitting controlled data sharing among authorized parties. This work demonstrates the potential of combining blockchain and cloud technologies in healthcare, emphasizing their role in maintaining data integrity, with implications for computer science and healthcare innovation.

Keywords:

1. Introduction

The collection of health data is of invaluable importance in medical-related research. While some data is routinely collected and stored, research projects often require the collection and storage of additional data. Informed consent is the general rule when collecting personal data for research [1]. Traditionally, this has been done by signing a paper, which is then stored, and manually assigning a study ID to pseudonymize the data. This process is heavy, and a modern solution would include the digital collection of consent, sometimes called eConsent [2, 3].

The recent European Health Data Space (EHDS) initiative exemplifies the future expectations for sharing health data. For data requiring consent, digital consent through a smart contract is a valuable solution [4], facilitating the giving, changing, and withdrawing of consent throughout the data's lifespan. For such digital consent systems to be widely adopted, they must be trustworthy. Users should be able to trust that personal information, such as names and identification numbers, and the key linking personal identification numbers to study IDs, are not seen or shared. Concerns about unauthorized access, data breaches, and privacy have increased the need for new solutions that protect patient rights and health data.

In this study, we propose a blockchain-based digital consent solution for research data, to be used within the *NewbornTime*[1] project [5]. To ensure trustworthiness, all personal information is encrypted, and the correct consent information is kept together with all consent changes throughout the data's lifespan. The consent information is stored on a blockchain, ensuring tamper-proof consent records.

Globally, 10% of newborns require assistance to start breathing after birth, and approximately 5% need ventilation [6, 7]. *NewbornTime – Improved Newborn Care based on video and artificial intelligence* is a research project that collects thermal video data from the time during labor, right before and after birth, as well as visual light video from the resuscitation tables for newborns needing assistance to start breathing. Using AI for activity recognition, the project aims to create objective timelines of events, such as birth and resuscitation interventions [8, 9]. These timelines can be compared with guidelines and outcomes, supporting knowledge generation, debriefing, and quality improvement [10].

Collecting and processing sensitive video data raises significant ethical and legal challenges. The NewbornTime project addresses these concerns through data minimization and a secure, multi-layered approach to ethical data handling using a secure cloud platform for video data storage. Strict access control and security protocols ensure compliance with the General Data Protection Regulation (GDPR). To manage patient consent, the project employs a blockchain-based system developed with BitUnitor[2]. This approach ensures transparency, immutability, and traceability of consent records, ac-

[1] `https://www.uis.no/en/research/newborntime`

[2] `https://www.bitunitor.com`

cessible only to authorized parties.

The main contributions of this study highlight significant advancements at the intersection of blockchain technology, cloud computing, and healthcare consent management.

1. **Blockchain-Based Consent Application**: We present a blockchain-driven consent application specifically tailored for healthcare needs. This application securely and transparently manages patient consent, leveraging blockchain's tamper-proof and immutable features within the healthcare ecosystem.
2. **Smart Contract Integration**: A central component of our solution is the use of smart contracts, which ensure secure, decentralized, and automated handling of consent transactions. By employing Ethereum's robust platform, the consent records remain accurate and resilient to unauthorized alterations.
3. **Privacy and Security Measures**: Recognizing the sensitivity of healthcare data, our system incorporates advanced encryption techniques to safeguard personal information. Additionally, data minimization and decentralized storage ensure compliance with privacy regulations like GDPR, reducing vulnerabilities associated with centralized systems.
4. **User-Friendly Dashboard for Consent Management**: To enhance accessibility and usability, we have integrated a consent management dashboard. This dashboard allows users to view, edit, and withdraw consents while providing insightful visualizations of consent trends over time. Its intuitive interface bridges the gap between technical innovations and user experience.
5. **Broader Implications for Healthcare**: Beyond the NewbornTime project, our research demonstrates the transformative potential of combining blockchain and cloud technologies in healthcare. These innovations not only address current challenges in consent management but also pave the way for broader adoption of secure and transparent data-sharing practices across the sector.

Our study represents a crucial step toward addressing the challenges of patient consent, and data security in healthcare. By presenting an integrated solution that combines blockchain, cloud computing, and a user-friendly dashboard within the scope of the NewbornTime project, we demonstrate the system's ability to ensure data integrity, and advance healthcare innovation. These contributions provide a strong foundation for future research and real-world implementation in diverse healthcare settings.

2. Preliminary Information

Before exploring the details of our architectural framework and its use in the NewbornTime project, we need to build a basic understanding of some key concepts that support our research. These concepts, such as blockchain, smart contracts, and Ethereum, provide the foundation for our approach.

2.1. Blockchain

Originally developed as the distributed ledger technology behind cryptocurrencies like Bitcoin, blockchain is a decentralized and unchangeable digital ledger represented as $\mathcal{L}$. It records transactions, where each transaction T_i is a set $\langle S_i, R_i, D_i \rangle$ that includes a sender's address S_i, a recipient's address R_i, and data D_i. The ledger $\mathcal{L}$ is made up of blocks $\mathcal{B}_j$, so $\mathcal{L} = [\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_n]$. Each block $\mathcal{B}_j$ holds a group of transactions and is linked to the previous block using cryptography, ensuring tamper-resistance through a hash function $\mathcal{H} : \mathcal{H}(\mathcal{B}_j) = \mathcal{B}_j(\text{prev hash})$. This transparency and security make blockchain highly valuable in industries that need openness, and data integrity.

2.2. Smart Contracts

Smart contracts are self-executing, predictable programs represented as $\mathcal{C}$ and deployed on blockchain platforms like Ethereum. A smart contract $\mathcal{C}$ contains logic $\mathcal{L}_{\mathcal{C}}$ as code, which sets conditions $\mathcal{C}_{\text{conditions}}$ that, when met, trigger actions $\mathcal{C}_{\text{actions}}$. In a pseudocode representation:

```
Smart Contract C:
    Conditions: C_conditions
    Actions: C_actions
```

Smart contracts remove the need for intermediaries by automating contract execution based on predefined rules, promoting transparency, security, and efficiency. They are suitable for various uses, such as legal agreements, supply chain management, and managing healthcare consent.

2.3. Ethereum

Ethereum, represented as $\mathcal{E}$, is a leading blockchain platform that enhances the capabilities of blockchain technology [11, 12]. It maintains a global state $\mathcal{S}$, made up of accounts $\mathcal{A}$, where each account $\mathcal{A}_i$ is identified by an address $\mathcal{A}_i$address. Ethereum allows developers to create and deploy smart contracts, enabling a wide range of decentralized applications (DApps). Ethereum's Turing-complete scripting language and flexible ecosystem make it a great choice for projects that combine blockchain with innovative contract capabilities across various fields, including healthcare.

With this basic understanding of blockchain, smart contracts, and Ethereum, we are ready to dive into the details of our architectural framework and how it is used in the NewbornTime project. Our approach uses these technologies to tackle the important challenges of patient consent, data security, all supported by a strong theoretical foundation.

3. Web Interface for Users

The web interface of the NewbornTime project has been designed to provide a user-friendly platform for users to give, view, and manage their consent related to participation in the project. Below are the key components of the interface with relevant screenshots.

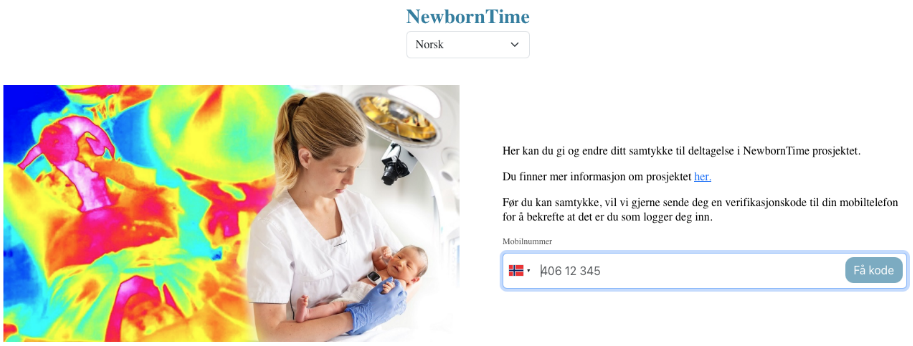
3.1. User Consent Submission

When a user accesses the platform, they are prompted to provide their phone number to receive a verification code, ensuring that the user giving consent is verified (Figure 1). This step is crucial for verifying that the correct individual is interacting with the system.

The system also supports the entry of paper-signed consents by research staff, ensuring that all consent records, whether digital or paper-based, are centralized and accessible for verification. This feature accommodates scenarios where paper signing is more practical, such as during initial participant recruitment.

3.2. User Dashboard

After verification, users are presented with a dashboard where they can give consent, view or edit existing consents, and modify personal information (Figure 2). The options are straightforward and designed to allow users to quickly navigate the platform.



Her kan du gi og endre ditt samtykke til deltagelse i NewbornTime prosjektet.

Du finner mer informasjon om prosjektet her.

Før du kan samtykke, vil vi gjerne sende deg en verifikasjonskode til din mobiltelefon for å bekrefte at det er du som logger deg inn.

Mobilnummer: 406 12 345

Figure 1: Initial screen for user consent submission, requiring phone number verification.

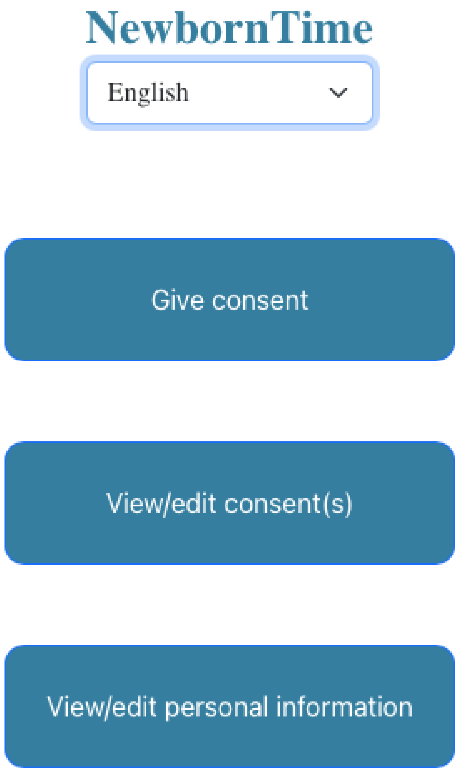
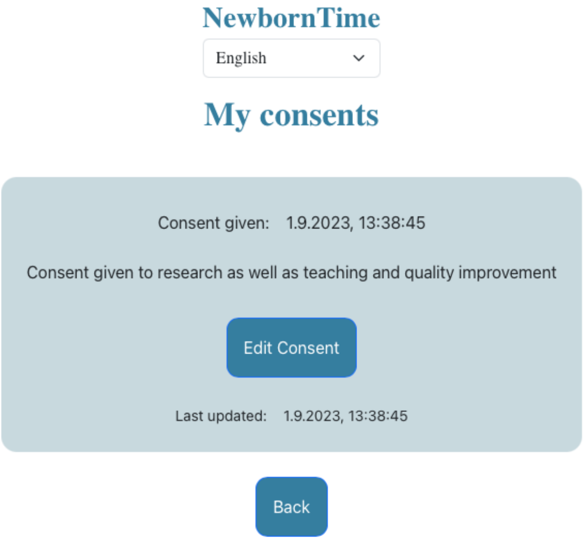


Figure 2: User dashboard offering options to give consent, view/edit consents, or modify personal information.

3.3. Consent Overview

In the consent overview section (Figure 3), users can view the details of their current consent, including the type of consent given and the time and date the consent was submitted. The interface allows the user to edit or withdraw consent as needed.



NewbornTime

English

My consents

Consent given: 1.9.2023, 13:38:45

Consent given to research as well as teaching and quality improvement

Last updated: 1.9.2023, 13:38:45

Figure 3: Overview of the user's given consent with options to edit or withdraw consent.

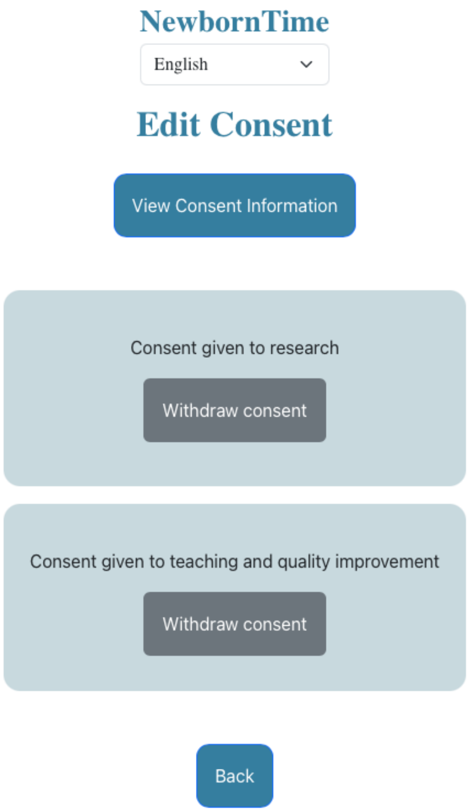
3.4. Consent Editing

Users can withdraw specific consent through the consent editing interface (Figure 4). This feature allows flexibility, giving users control over their consent at any time. The interface provides clear options to withdraw consent for different purposes, such as research or teaching.

The web interface has been developed with a focus on ease of use, security, and transparency, ensuring that users can efficiently manage their consent and personal information in line with the project's ethical standards.

3.5. Consent Statistics Dashboard

The Consent Statistics Dashboard is an integral feature of the NewbornTime web interface, designed to provide both administrators and researchers



Consent given to research

Consent given to teaching and quality improvement

Figure 4: Consent editing interface where users can withdraw their consent for specific purposes.

with valuable insights into consent trends over time. This interactive dashboard visualizes key metrics, allowing stakeholders to monitor and analyze consent data effectively (Figure 5).

The dashboard includes the following features:

- **Consent Trends Over Time**: A line graph displays the number of consents given for different purposes, such as research or education, over a selected time range. This feature helps to track consent activity and identify patterns.
- **Weekly Distribution of Consents**: A pie chart illustrates the distribution of consents across days of the week, providing insights into user behavior and engagement patterns.
- **Summary Metrics**: Key statistics, such as the total number of consents for education and research, appear to offer a quick overview of the current consent status.
- **Detailed Consent Records**: A tabular view lists individual consent records, including registration date, number of participants, and types of consent given. This granular data supports in-depth analysis and reporting.

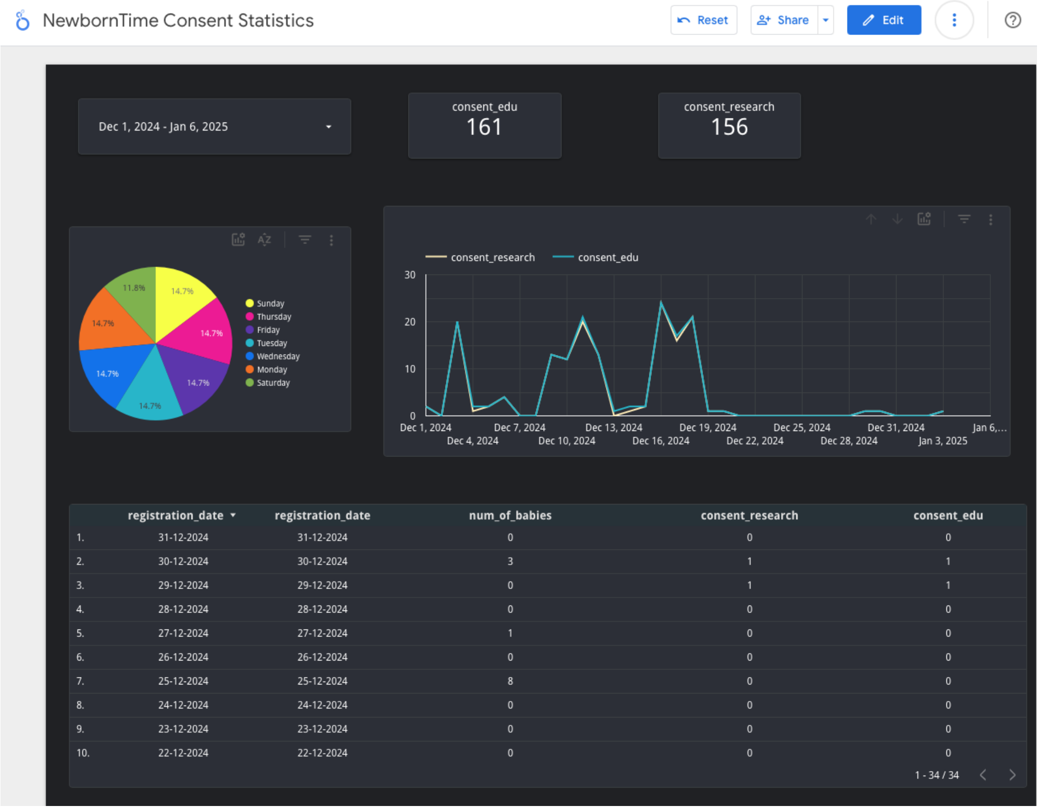
4. Consent Management Smart Contract

This section provides a detailed look at the architecture behind the NewbornTime project, with a specific focus on the Ethereum-based healthcare consent management system.

4.1. System Overview

Figure 6 illustrates the end-to-end architecture of the consent management system implemented for the NewbornTime project. This modular design seamlessly integrates blockchain technology, cloud-based infrastructure, and user-friendly interfaces to address critical challenges in healthcare consent management. The system is composed of the following main components:

- **Consent Portal:** Mothers submit their consent through an intuitive web interface, which securely logs all actions. The portal also allows for modifications, withdrawals, and updates to consent records.



consent_edu
161

consent_research
156

	registration_date ▾	registration_date	num_of_babies	consent_research	consent_edu
1.	31-12-2024	31-12-2024	0	0	0
2.	30-12-2024	30-12-2024	3	1	1
3.	29-12-2024	29-12-2024	0	1	1
4.	28-12-2024	28-12-2024	0	0	0
5.	27-12-2024	27-12-2024	1	0	0
6.	26-12-2024	26-12-2024	0	0	0
7.	25-12-2024	25-12-2024	8	0	0
8.	24-12-2024	24-12-2024	0	0	0
9.	23-12-2024	23-12-2024	0	0	0
10.	22-12-2024	22-12-2024	0	0	0

1 - 34 / 34

Figure 5: Consent Statistics Dashboard displaying trends, distributions, and detailed records for consent management.

- **Cloud System for Blockchain:** Consent data is managed by smart contracts deployed on the Ethereum blockchain. These contracts ensure secure and immutable storage of consent records, handling all submissions, withdrawals, and updates while providing tamper-proof event logs.
- **Cloud System for Reporting:** This component includes an Extract-Transform-Load (ETL) process that aggregates and anonymizes data from the blockchain. The data is then visualized through an interactive dashboard, providing healthcare professionals and researchers with actionable insights into consent trends, compliance rates, and distribution patterns.
- **Consent Verification for Delivery Room:** The system ensures real-time verification of consent during critical moments such as video recordings in the delivery room. Healthcare staff can generate unique study IDs linked to the consent records, ensuring compliance and ethical data handling.

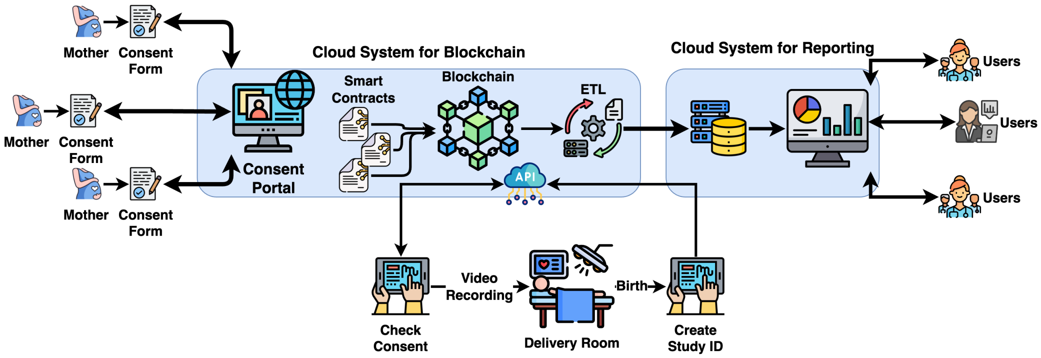


Figure 6: System overview of the NewbornTime consent management system, showcasing the integration of the consent portal, blockchain, cloud reporting, and real-time consent verification processes.

The consent management system is tailored for research purposes, facilitating the collection and management of consent for research data, distinct from clinical healthcare data. Currently, the system is implemented for the NewbornTime research project, managing consent for video data analysis during birth and resuscitation. Its architecture, however, allows for potential future applications in broader healthcare settings, pending additional regulatory and usability assessments [13]. The system integrates both digital and paper-based consent processes, allowing for flexibility in how consents are obtained and recorded. The system integrates with the NewbornTime project by verifying consent before uploading video data to the cloud storage. The process involves: 1) Recording births and consents in the Liveborn Observation app, 2) Generating study IDs via the BitYoga system, 3) Periodically checking for valid consents and uploading corresponding videos to Azure if consent is active.

4.2. Architectural Formalization

The consent management system employs a robust, decentralized architecture designed to enhance newborn care by seamlessly integrating advanced AI algorithms for video analysis during childbirth and postpartum. The architecture also facilitates the secure and traceable management of patient consent, including the generation of unique Study IDs to link maternal and neonatal data.

The blockchain-based consent management algorithm presented in Algorithm 1 outlines the core processes involved in submitting, querying, creating Study IDs, and withdrawing consent on the Ethereum blockchain.

The `SubmitConsent` procedure is initiated when a mother accesses the consent management platform. The process begins with user verification, where a verification code is sent to the mother's phone, and the user is required to submit this code to confirm their identity. If the verification is successful, the mother selects the type of consent they wish to provide (e.g., for research or education purposes). The consent record is encrypted using the mother's public key to ensure confidentiality before being sent to the smart contract on the Ethereum blockchain. The smart contract stores the consent and emits a `ConsentGiven` event, signaling that the consent has been successfully recorded. At this stage, only a Mother ID is generated by the system, and no Baby ID is assigned yet.

The `QueryConsent` procedure enables to verify whether a mother has given consent. The provider (e.g. Laerdal Medical) uses the mother's personal number as a key parameter to query the blockchain for the consent record. The smart contract retrieves the encrypted consent record. The consent information is made available to the provider. This step is critical during childbirth when video recordings or other data collection processes require immediate consent verification.

The `CreateStudyID` procedure is executed post-birth. If valid consent is confirmed for the mother, the research assistant can invoke an API call to generate a unique Study ID that links the Mother ID and the newly assigned Baby ID. The Study ID serves as a pseudonymized identifier for securely associating consent records with data collected during and after birth. The smart contract records the Study ID creation and emits a `StudyIDCreated` event for transparency.

The `WithdrawConsent` procedure allows the user to revoke specific consents through the platform. The smart contract updates the consent record on the blockchain to reflect withdrawal and emits a `ConsentWithdrawn` event, ensuring that the revoked consent is no longer valid for future use.

The algorithm ensures the security and privacy of user data through encryption and access control mechanisms. All consent records are encrypted before being sent to the blockchain, ensuring that only authorized entities can access and view the records. The smart contract acts as a gatekeeper, enforcing strict authorization protocols while maintaining transparency through event emissions.

4.3. Ethereum Smart Contract

In the ensuing discussion, we present the Ethereum smart contract titled `HealthcareConsent.sol`. This contract occupies a pivotal role within the project, empowering the secure administration of patient consents via the Ethereum blockchain.

Listing 1: HealthcareConsent.sol Smart Contract

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract HealthcareConsent {
    address public owner;
```

Starting with a SPDX-License-Identifier comment, this contract sets the licensing terms under which the code runs, following the MIT license.

Named `HealthcareConsent`, this contract includes a state variable, `owner`, which is used to store the Ethereum address of the contract's owner.

```
    // Struct to represent a consent record
    struct Consent {
        address patient;
        address healthcareProvider;
        bool isConsentGiven;
```

Algorithm 1: Blockchain-Based Consent Management Algorithm

```
Input: User data (phone number, personal number), consent type
Output: Consent record stored on the blockchain, Study ID generated
SubmitConsent:
Mother accesses platform and submits verification code
if verification successful then
    Mother selects consent type
    Encrypt consent record and send to smart contract
    Smart Contract: Store consent, generate Mother ID, and emit
     ConsentGiven event
else
    Terminate process
QueryConsent:
Healthcare provider submits mother's personal number
if authorized then
    Retrieve and decrypt consent record
else
    Deny access
CreateStudyID:
Provider queries consent status using mother's personal number
if consent valid then
    Generate unique Study ID by combining Mother ID and Baby ID
    Smart Contract: Record Study ID and emit StudyIDCreated event
else
    Deny Study ID creation
WithdrawConsent:
User selects consent to withdraw
Smart Contract: Mark consent as withdrawn and emit ConsentWithdrawn
 event
```

```
        string motherName;
        uint256 nationalID;
        string phoneNumber;
        uint256 timestamp;
    }
```

- A `Consent` struct is introduced to hold individual consent records. This structure includes various attributes, such as the patient's Ethereum address, the healthcare provider's address, the consent status (`isConsentGiven`), the mother's name (`motherName`), the national identification number (`nationalID`), the phone number (`phoneNumber`), and a timestamp (`timestamp`).

```
    // Mapping from patient's address to their consents
    mapping(address => Consent[]) public patientConsents;
```

- A mapping named `patientConsents` is leveraged to aggregate arrays of `Consent` records, categorizing them under the Ethereum addresses of respective patients. In this structure, the Ethereum address of the patient serves as the mapping's key, while the value corresponds to an array of `Consent` records.

```
    // Event to log consent changes
    event ConsentChanged(address indexed patient, address
       indexed healthcareProvider, bool isConsentGiven,
       uint256 timestamp);
```

- The contract incorporates an `event` termed `ConsentChanged`, intended to record alterations in consent statuses. This event is distinguished by indexed parameters, namely `patient`, `healthcareProvider`, `isConsentGiven`, and `timestamp`, serving as pivotal transparency and audit trail mechanisms.

```
    constructor() {
        owner = msg.sender;
    }
```

- The contract's constructor initializes the `owner` variable, assigning it the Ethereum address of the contract deployer, represented by `msg.sender`. This address designates the contract's owner.

```
    // Modifier to restrict access to the contract owner
    modifier onlyOwner() {
        require(msg.sender == owner, "Only the contract owner
            can call this function");
        _;
    }
```

- The contract includes a `modifier` called `onlyOwner`, which is used to limit access to certain functions. Functions with this modifier can only be called by the contract owner. This access control works by checking that the sender's Ethereum address (`msg.sender`) matches the contract owner's address.

4.4. Patient Consent Record

Each consent record housed within the `HealthcareConsent.sol` contract is distinguished by the following attributes:

- Patient's Ethereum address

- Educational and research consent status (either granted or revoked)
- Mother's name
- National identification number
- Phone number
- Timestamp
- Study ID

These attributes together enable the careful tracking and management of patient consents, ensuring their integrity and accessibility.

4.5. Security Considerations

4.5.1. Access Control Mechanisms

Access to important functions within the smart contract is controlled by the `onlyOwner` modifier, written as `onlyOwner()`. This modifier restricts access, allowing only the contract owner (`msg.sender` = `owner`) to execute these functions, usually a trusted entity in the healthcare system. Additionally, each patient is given a unique Ethereum address which improves identity verification.

4.5.2. Auditability and Transparency

To support auditing and maintain transparency, the system uses the `ConsentChanged` event. This event logs all changes in consent status, creating a clear and auditable record of the consent history. It helps ensure accountability and assists in identifying any unauthorized or suspicious activities.

4.6. Privacy Safeguards

Protecting patient privacy is a top priority in healthcare systems [14, 15]. The Ethereum-based consent management system used in the NewbornTime project includes strong privacy protections, as summarized in Table 2:

4.6.1. Encryption

Sensitive patient information, like mother's names, national identification numbers, and phone numbers, is encrypted before being stored on the blockchain. This encryption makes sure that even if unauthorized access happens, the data stays confidential and cannot be read without the correct decryption keys.

4.6.2. Data Minimization

The system follows the principle of data minimization, where only the essential information needed for consent management is collected and stored. This approach lowers the risk linked to storing and handling sensitive information, reducing potential weaknesses.

4.6.3. Decentralization

The decentralized structure of the Ethereum blockchain makes sure that patient data is not kept in a single, vulnerable location prone to data breaches. Instead, the data is spread across multiple nodes, which improves protection against attacks and strengthens data security [16].

Incorporating these security measures and privacy protections together creates a strong foundation for the Ethereum-based healthcare consent management system, building data integrity, and patient confidence within the NewbornTime project.

The consent management system incorporates a comprehensive set of security measures and privacy safeguards to ensure the confidentiality, integrity, and availability of patient data. These measures are critical and maintaining compliance with healthcare data protection regulations.

Table 1 summarizes the key security considerations implemented in the system. These include robust access control mechanisms, secure data storage leveraging the tamper-resistant blockchain, and transparent audit trails that log all consent-related changes. Together, these measures prevent unauthorized access, ensure data integrity, and enhance accountability.

Table 1: Summary of Security Considerations

Security Aspect	**Description**
Access Control Mechanisms	Control access to critical functions through the `onlyOwner` modifier, ensuring only authorized entities can execute them.
Secure Data Storage	Utilize the tamper-resistant and immutable nature of the blockchain for secure patient data storage, employing cryptographic techniques for confidentiality.
Auditability and Transparency	Log consent status changes using the `ConsentChanged` event, enhancing accountability and detection of unauthorized activities.

Table 2 outlines the privacy safeguards integrated into the system. These include the encryption of sensitive patient data, adherence to the principle of data minimization, and the decentralized architecture of the Ethereum blockchain. By applying these principles, the system minimizes vulnerabilities and ensures compliance with privacy standards, protecting user data at all times.

Table 2: Summary of Privacy Safeguards

Privacy Aspect	**Description**
Encryption	Apply encryption to sensitive patient information before storage, ensuring confidentiality and data security.
Data Minimization	Collect and store only essential information required for consent management, reducing the risk associated with sensitive data.
Decentralization	Leverage the decentralized Ethereum blockchain to distribute patient data across multiple nodes, enhancing data security and resilience.

Personal identifiable information (PII) is not stored on the blockchain; instead, the blockchain records only consent-related metadata, ensuring privacy while maintaining transparency. Upon withdrawal of consent, a new transaction is recorded on the blockchain to indicate revocation, and the associated personal data is promptly deleted from off-chain storage systems, ensuring compliance with data protection regulations such as GDPR.

5. Experimental Results

Let H be the set of all healthcare providers, P be the set of all patients, and $\mathcal{C}$ be the set of all consent records. For each patient $p \in P$, $\mathcal{C}_p$ represents the set of consent records linked to patient p. Each consent record $c \in \mathcal{C}_p$ is formally defined as follows:

$$c = (p, h, g, m, n, ph, t)$$

where:

- p is the patient's Ethereum address,

- h is the healthcare provider's Ethereum address,
- g denotes the consent status (1 for granted, 0 for revoked),
- m is the mother's name (a string),
- n is the national identification number (an integer),
- ph is the phone number (a string), and
- t is the timestamp (a Unix timestamp).

The `HealthcareConsent.sol` contract manages consent status changes within $\mathcal{C}$. Access control is enforced by the `onlyOwner` modifier, which allows only the contract owner to call certain functions. Additionally, the contract includes an `event`, `ConsentChanged`(p, h, g, t), which records consent changes, providing a permanent and clear audit trail.

5.1. Gas Costs

The gas costs [17] associated with various operations of the `HealthcareConsent.sol` smart contract were measured. Gas costs represent the computational resources required to execute operations on the Ethereum blockchain. Each operation, such as adding, querying, or revoking consent, consumes a specific amount of gas, which translates to transaction fees paid to miners for processing and securing these actions. Table 3 shows the gas used for adding, querying, and revoking consent records.

The gas cost for adding a consent record was observed to be significantly higher than querying or revoking a consent. Query operations do not require gas as they are read-only, while revoking a consent incurs a cost due to state modification.

5.2. Transaction Throughput

To assess the system's ability to handle multiple transactions, we measured the time taken to add batches of consent records. Figure 7 shows the transaction throughput as the number of records increases.

Table 3: Gas Costs for Different Operations

Operation	**Gas Used**	**Execution Time (ms)**
Add Consent	175719	155.850887
	160719	129.161119
	160719	136.569977
	160719	169.187069
	160719	133.695841
Query Consent	0	105.110168
Revoke Consent	37035	69.026947
	41601	97.961903
	46167	74.846983
	50733	73.647261
	55299	72.370768

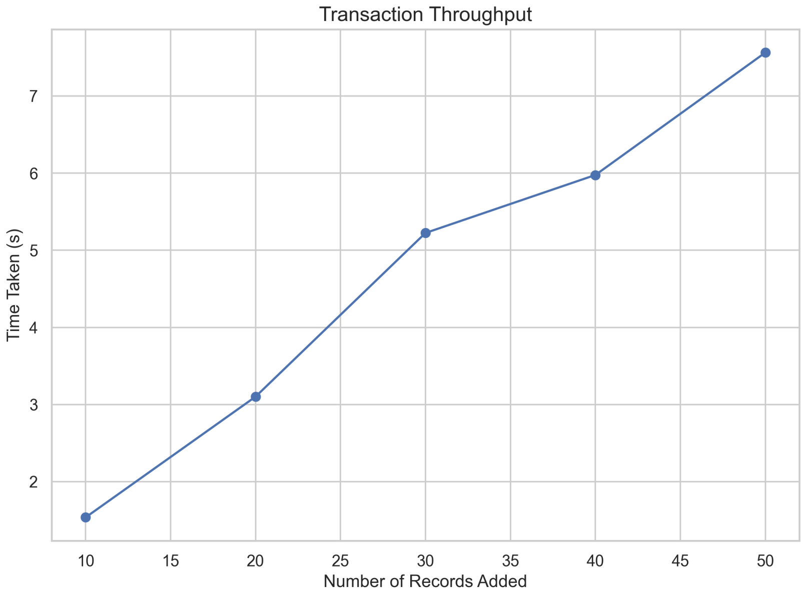


Figure 7: Transaction Throughput Over Time

The system was able to handle up to 50 records within a reasonable time frame, with a noticeable increase in transaction time as the batch size increased. This suggests the system is capable of handling moderate loads but may require optimization for larger-scale operations.

5.3. Scalability Analysis

To test the scalability of the system, we measured the gas used and time taken to add increasingly larger batches of consent records. Table 4 summarizes the scalability results.

Table 4: Scalability Test Results

Records Added	**Gas Used**	**Time Taken (ms)**
10	1606870	183.220911
50	8034350	182.528577
100	16068700	192.539830
500	80343476	207.127324

The results indicate that gas consumption and time scale with the number of records. This behavior is expected due to the immutable and decentralized nature of the Ethereum blockchain.

5.4. Privacy and Data Minimization

To evaluate the impact of data minimization on privacy and system performance, we compared the gas costs of storing full consent records versus minimal consent records. Table 5 summarizes the gas usage and execution time for these two types of records.

The results indicate that storing minimal consent data significantly reduces gas costs (102,437 gas units compared to 160,747 gas units for full data) and execution time (144.618 ms versus 164.344 ms). These findings highlight the efficiency benefits of storing only essential information, such as anonymized or minimal data, while supporting the principle of data minimization.

Table 5: Gas Costs for Minimal vs Full Consent Records

Data Type	**Gas Used**	**Execution Time (ms)**
Full Data	160747	164.344788
Minimal Data	102437	144.618034

The results show that storing minimal consent data significantly reduces gas costs, which supports the principle of data minimization. This ensures that only necessary data is stored on-chain, reducing storage overhead and enhancing privacy.

6. Discussion

The experimental results demonstrate the effectiveness of the Ethereum-based healthcare consent management system in balancing security, privacy, and scalability, with certain limitations. In this section, we discuss the key findings and their broader implications for healthcare and blockchain-based consent management systems.

6.1. Data Privacy and Security

The system's privacy safeguards, particularly encryption and data minimization, were validated through the experiments. Encryption ensures that even if unauthorized access occurs, sensitive patient information such as national IDs and phone numbers remains confidential. The principle of data minimization reduces the amount of sensitive data stored on-chain, thus decreasing the risk of data breaches.

The decentralized nature of the Ethereum network ensures that patient data is not stored in a single centralized repository, reducing the risk of breaches and enhancing overall data security.

The system ensures that personal data is not stored on the blockchain, minimizing privacy risks. The consent withdrawal mechanism triggers immediate deletion of associated data from off-chain storage, demonstrating the system's commitment to data protection. In the context of the Newborn-Time project, the system ensures that sensitive video data is only accessed and processed with valid participant consent, thereby protecting participant privacy and maintaining research integrity.

6.2. Scalability and Performance

The scalability experiments revealed that the system performs well under moderate loads but faces challenges when scaling to handle large volumes of consent records [18]. As shown in Table 6, gas costs increase with the number of consent records, presenting a limitation for large-scale healthcare environments.

The transaction throughput remains sufficient for moderate-scale healthcare settings, but for larger-scale systems, optimization strategies such as Layer 2 scaling solutions (e.g., rollups) could be employed to improve scalability and reduce transaction costs [19].

Table 6 shows the summary of experimental results.

Table 6: Summary of Experimental Results

Aspect	**Key Findings**
Transparency	Blockchain immutability and audit trails enhance trust between patients and healthcare providers.
Data Privacy and Security	Encryption and data minimization ensure confidentiality of sensitive patient information, while decentralization improves data security.
Scalability	System performs well under moderate loads; however, gas costs and time increase linearly with the number of records, limiting scalability.
Trade-offs	High gas costs and slower transaction times in large-scale settings. Optimization needed for scalability.

6.3. Trade-offs and Future Work

While the system successfully addresses the key challenges of security, and privacy, there are trade-offs between security, scalability, and cost. The decentralized nature of the blockchain provides security but results in higher gas costs and slower transaction times, particularly as the system scales.

Future work should focus on optimizing gas usage, exploring alternative blockchain platforms, or integrating more efficient consensus mechanisms. Moreover, the development of user-friendly interfaces for patients and healthcare providers would enhance usability and adoption in real-world healthcare settings.

Future research should include user studies to assess the level of trust and acceptance among participants, especially mothers-to-be, to ensure the system meets their needs and expectations [20]. While the current focus is on research consent management, future work could explore adapting the system for clinical healthcare applications, addressing the specific needs and regulations of patient care environments[21]. A limitation of the current implementation is the low usage of the digital portal for consent management, with participants preferring direct contact with research staff. Future improvements could focus on enhancing user education, simplifying the interface, and providing targeted training to increase engagement with the digital platform [22].

7. Conclusion

This study has presented a complete consent management system developed for the NewbornTime project, which focuses on solving key challenges related to patient consent, and data security in healthcare. The system is built around the `HealthcareConsent.sol` smart contract on the Ethereum blockchain, which ensures transparency, data integrity, and privacy when handling patient consent.

The modular design of the system, shown in the system overview figure, includes the Consent Portal, the Cloud System for Blockchain, the Cloud System for Reporting, and real-time Consent Verification in the delivery room. This setup allows mothers to provide consent securely and enables healthcare professionals to verify consent and generate a Study ID that links the mother's and newborn's data for research purposes.

A major part of the system is the `Consent Statistics Dashboard`, which gives healthcare providers and researchers with clear and useful information about consent trends, status, and records. This feature improves the management of consent processes and supports better decision-making through real-time data analysis.

To protect sensitive data, the system uses strong security and privacy measures, such as data encryption, access control, and tamper-proof storage of the blockchain. These measures ensure that only authorized users can access patient data and that the system meets data protection standards like GDPR.

The system has shown promising performance in managing consent records, but some challenges remain. High gas costs and scalability issues with Ethereum need to be addressed. Future work will focus on making the system more efficient and scalable, possibly by exploring alternative blockchain solutions or optimization methods.

The proposed system offers a secure and reliable solution for managing patient consent in healthcare. It combines blockchain technology, a user-friendly dashboard, and secure data handling to improve efficiency. Future developments will aim to expand the system's use in other healthcare and research projects while improving performance and lowering costs.

References

[1] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, T. Hayajneh, Healthcare blockchain system using smart contracts for secure automated remote patient monitoring, Journal of medical systems 42 (2018) 1–7.

[2] P. Shah, I. Thornton, D. Turrin, et al., Informed consent, StatPearls (2024).

[3] H. Obaidi, Y. Elkhyatt, M. Alzubaidi, M. Househ, Use of e-consent in healthcare settings: A scoping review, Stud Health Technol Inform 316 (2024) 1064–1068.

[4] Z. Zheng, S. Xie, H. Dai, et al., An overview on smart contracts: Challenges, advances, and platforms, Future Generation Computer Systems 105 (2020) 475–491.

[5] K. Engan, S. I. Rettedal, et al., Newborn time - improved newborn care based on video and artificial intelligence - study protocol, BMC Digital Health 1 (2023) 10.

[6] P. A. Bjorland, K. Øymar, H. L. Ersdal, S. I. Rettedal, Incidence of newborn resuscitative interventions at birth and short-term outcomes: a regional population-based study, BMJ paediatrics open 3 (2019).

[7] M. H. Wyckoff, J. Wyllie, K. Aziz, M. F. de Almeida, J. Fabres, J. Fawke, R. Guinsburg, S. Hosono, T. Isayama, V. S. Kapadia, et al., Neonatal life support: 2020 international consensus on cardiopulmonary resuscitation and emergency cardiovascular care science with treatment recommendations, Circulation 142 (2020) S185–S221.

[8] J. García-Torres, Ø. Meinich-Bache, S. Brunner, A. Johannessen, S. Rettedal, K. Engan, Towards using thermal cameras in birth detection, in: 2022 IEEE 14th Image, Video, and Multidimensional Signal Processing Workshop (IVMSP), IEEE, 2022, pp. 1–5.

[9] J. García-Torres, Ø. Meinich-Bache, S. I. Rettedal, A. Kibsgaard, S. Brunner, K. Engan, Comparative analysis of binary and multiclass activity recognition in high-quality newborn resuscitation videos, in: Northern Lights Deep Learning Conference 2024, 2024.

[10] V. Kolstad, J. García-Torres, S. Brunner, A. Johannessen, E. Foglia, H. Ersdal, Ø. Meinich-Bache, S. Rettedal, Detection of time of birth and cord clamping using thermal video in the delivery room, Frontiers in Pediatrics 12 (2024) 1342415.

[11] N. Szabo, Formalizing and securing relationships on public networks, First monday (1997).

[12] V. Buterin, et al., A next-generation smart contract and decentralized application platform, white paper 3 (2014) 2–1.

[13] G. Albanese, J.-P. Calbimonte, M. Schumacher, D. Calvaresi, Dynamic consent management for clinical trials via private blockchain technology, Journal of ambient intelligence and humanized computing 11 (2020) 4909–4926.

[14] C. Cheng, B. Yan, G. Wang, The blockchain based access control scheme for the internet of things, Procedia Computer Science 202 (2022) 342–347. URL: `https://www.sciencedirect.com/science/article/pii/S1877050922005804`. doi:`https://doi.org/10.1016/j.procs.2022.04.046`, international Conference on Identification, Information and Knowledge in the internet of Things, 2021.

[15] F. Albalwy, A. Brass, A. Davies, et al., A blockchain-based dynamic consent architecture to support clinical genomic data sharing (consentchain): Proof-of-concept study, JMIR medical informatics 9 (2021) e27816.

[16] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, M. Guizani, Medshare: Trust-less medical data sharing among cloud service providers via blockchain, IEEE Access 5 (2017) 14757–14767. doi:`10.1109/ACCESS.2017.2730843`.

[17] S. Pongnumkul, C. Siripanpornchana, S. Thajchayapong, Performance analysis of private blockchain platforms in varying workloads, in: 2017 26th International Conference on Computer Communication and Networks (ICCCN), 2017, pp. 1–6. doi:`10.1109/ICCCN.2017.8038517`.

[18] A. E. Gencer, S. Basu, I. Eyal, R. van Renesse, E. G. Sirer, Decentralization in bitcoin and ethereum networks, in: Financial Cryptography and Data Security: 22nd International Conference, FC

2018, Nieuwpoort, Curaçao, February 26 – March 2, 2018, Revised Selected Papers, Springer-Verlag, Berlin, Heidelberg, 2018, p. 439–457. URL: https://doi.org/10.1007/978-3-662-58387-6_24. doi:10.1007/978-3-662-58387-6_24.

[19] M. Zamani, M. Movahedi, M. Raykova, Rapidchain: Scaling blockchain via full sharding, in: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS '18, Association for Computing Machinery, New York, NY, USA, 2018, p. 931–948. URL: https://doi.org/10.1145/3243734.3243853. doi:10.1145/3243734.3243853.

[20] W. M. Charles, M. B. van der Waal, J. Flach, A. Bisschop, R. X. van der Waal, H. Es-Sbai, C. J. McLeod, Blockchain-based dynamic consent and its applications for patient-centric research and health information sharing: Protocol for an integrative review, JMIR Res Protoc 13 (2024) e50339. URL: https://www.researchprotocols.org/2024/1/e50339. doi:10.2196/50339.

[21] A. Khatoon, A blockchain-based smart contract system for healthcare management, Electronics 9 (2020). URL: https://www.mdpi.com/2079-9292/9/1/94. doi:10.3390/electronics9010094.

[22] P. E. Velmovitsky, P. A. D. S. E. S. Miranda, H. Vaillancourt, T. Donovska, J. Teague, P. P. Morita, A blockchain-based consent platform for active assisted living: modeling study and conceptual framework, Journal of medical Internet research 22 (2020) e20832.