DEVELOPMENT OF BLOCKCHAIN BASED GENERAL CONSENT MANAGEMENT SYSTEM

Lappeenranta–Lahti University of Technology LUT

Master’s Programme in DD Software Engineering and Digital Transformation, Master's thesis

2022

Polina Chagina

1st Examiner: Associate Professor A.K.M. Najmul Islam, PhD

2nd Examiner: Bahalul Haque, Junior Researcher

ABSTRACT

Lappeenranta–Lahti University of Technology LUT

LUT School of Engineering Science

Software Engineering and Digital Transformation

Polina Chagina

Development of blockchain-based general consent management system

Master's thesis

2022

67 pages, 36 figures, 9 tables and 1 appendix

Examiner(s): Associate Professor Najmul Islam, PhD, Bahalul Haque, Junior Researcher.

Keywords: consent, consent management, GDPR, blockchain

In today's world majority of communication processes are held through digital space where users without realizing are sharing their personal data which might be used by unworthy services for their own benefits. To impose restrictions on data collection the General Data Protection Regulation (GDPR) stands, which demands user consent requests and informs the user of the collection of personal data. The research goal is to identify how to design and develop a General Consent Management System considering GDPR.

Within the scope of work with the thesis, an analysis of academic literature and proposed systems was conducted. As this research is held as a solution-based approach Design Thinking methodology was chosen. During the research process, consent management was identified in connection with GDPR. The use of blockchain technology allows tracking of the activity of user consent. This thesis proves the consent of a general consent management system with the use of blockchain technology and provides a prototype of the working system.

ACKNOWLEDGEMENTS

I would like to express my gratitude and appreciation to my supervisors professor Najmul Islam and Bahalul Haque. For their research assistance, availability for discussions and ideas generation and help in maintaining productive research spirit.

SYMBOLS AND ABBREVIATIONS

Abbreviations

GDPR	General Data Protection Regulation
EU	European Union

TABLE OF CONTENTS

1 Introduction

This Master Thesis is focused on blockchain-based consent management solution development. The solution proposes a General Data Protection Regulation compliant system that ensures the collection, storage, and processing of informed consent. The proposed also preserves data confidentiality, transparency, and security. Compliance with the (GDPR, 2018) is crucial as it protects the personal data and clearly regulates the data processor's obligations within the processing of data collected in the territory of the EU. The importance of controlling the consent of the data subject comes from the fact that the data subject can regulate the legal basis for collecting personal data, as a record of consent or withdrawal of consent is directly transmitted to the processor and controlled by GDPR regulations. Furthermore the proposed methodology and the system architecture includes smart contract as an assistive technology and enabler to Blockchain based system.

1.1 Research motivation

Industry 4.0 is currently unfolding around the world (A. Ustundag, et al., 2022). Companies, businesses, and service providers are actively moving into the digital space. While being in the digital space, users are forced to imprint an information footprint of personal data, allowing untrustworthy services to exploit users' personal information for their benefit without users' permission. The General Data Protection Regulation (GDPR, 2018) is intended to protect user data and imposes several restrictions on collecting user data, explicitly demanding user consent. User consent should be obtained voluntarily. The purpose foruser consent collections must be obtained must be clearly stated and understood by the user, and user consent must be documented in writing or verbally. An essential part of the regulation of user consent is that personal information can only be stored for a fixed period and then should be deleted. The use of blockchain technology will make it possible to verify whether consent has been given.

1.2 Research gaps and questions

During analyzing publications related to the field of study it could be stated that to the best of my knowledge there is a lack of a general blockchain-based consent management system. Article by (B. Haque, et al., 2021) proposes an architecture for developing a blockchain-based solution for COVID vaccination passport VacciFi in compliance with GDPR. For clinical trials (G. Albanese, et al., 2021) developed the SCoDES approach for decentralized dynamic consent management with the use of blockchain technology was developed. Consent management also takes a considerable place in the ICT business area, (D. Peras, 2016) presents a model for consent and management in compliance with GDRP. Daoudagh et al. developed an architecture of GDRP policy where the processors define access control policies (S. Daoudagh, et al., 2021). Kantos et al. developed a system ADVOCATE for managing consent in e-health and IoT areas (K. Rantos, et al., 2019). GDPR compliance is achieved by a data controller that controls the consent management process. The next proposed development (M. Merlec, et al., 2021) aims to provide consent management for patients where GDPR is considered. (V. Jaiman, et al., 2020) Presents the platform for the exchange of patient medical records. The platform is built on the Ethereum blockchain network and ensures compliance with GDPR allowing authorized third parties to exchange patient data according to Recital 69. Similarly lakhan et al. proposed a system arrchitecture for the Internet of Medical Things enables patients' data process from medical sensors using Blockchain-Enable Smart-Contract Cost-Efficient Scheduling Algorithm Framework schemes (A. Lakhan, et al., 2021).

The summary of the conducted analysis is summarized in Table 1. The proposed analysis might lead to the following research gaps:

1. Lack of general systems, mostly blockchain-based consent management systems specified on one profile, like medicine.
2. Lack of proposed system prototypes, only four papers suggested a prototype of the consent management system.

Table 1 – Research Gaps

Article	GDPR compliance	Blockchain technology	Developed system	Field of study
B. Haque et al., 2021	Yes	Not mentioned	*VacciFi – architecture* of framework for a GDPR-compliant blockchain-based COVID vaccination passport	Medicine
Albanese et al., 2021	Yes	Blockchain as a service	*SCoDES* – consent management application for clinical trials	Medicine
D. Peras, 2016	Yes	No	*Guidelines* for the framework of GDPR compliant Consent and Data Management Model in ICT businesses	Medicine
S. Daoudagh et al., 2021	Yes	No	*Access Control Manager* for consent management	Business
K. Rantos et al., 2019	Yes	Ethereum	*ADVOCATE platform* – personal data manager in IoT ecosystem	E-Health, Internet of Things
M. Merlec et al., 2021	Yes	GoQuorum	Smart-contract-based dynamic *consent management system*	Medicine
V. Jaiman et al., 2020	Yes	Ethereum	*A Consent Model*for Blockchain-based Health Data Sharing Platforms	Medicine
A. Lakhan et al., 2021	No	Ethereum	*Algorithm* for minimal usage price calculation of Client-Fog-Cloud Healthcare System	Medicine

1.3 Structure of thesis

This Master's thesis would consist of 5 parts which are shown in Figure 1. Part 1 would be an Introduction and would cover research questions. Part 2 describes the background, describing which concepts and technologies are applied in the field of the master's thesis. Part 3 will outline the research method, its stages as well as the results to be achieved in the research phases. Part 4 presents the description of the system itself, contains requirements and architecture, and describes the algorithm of the developed system. Part 5 is the final part, which summarises the results of the work and identifies possibilities and potential for further research and development.

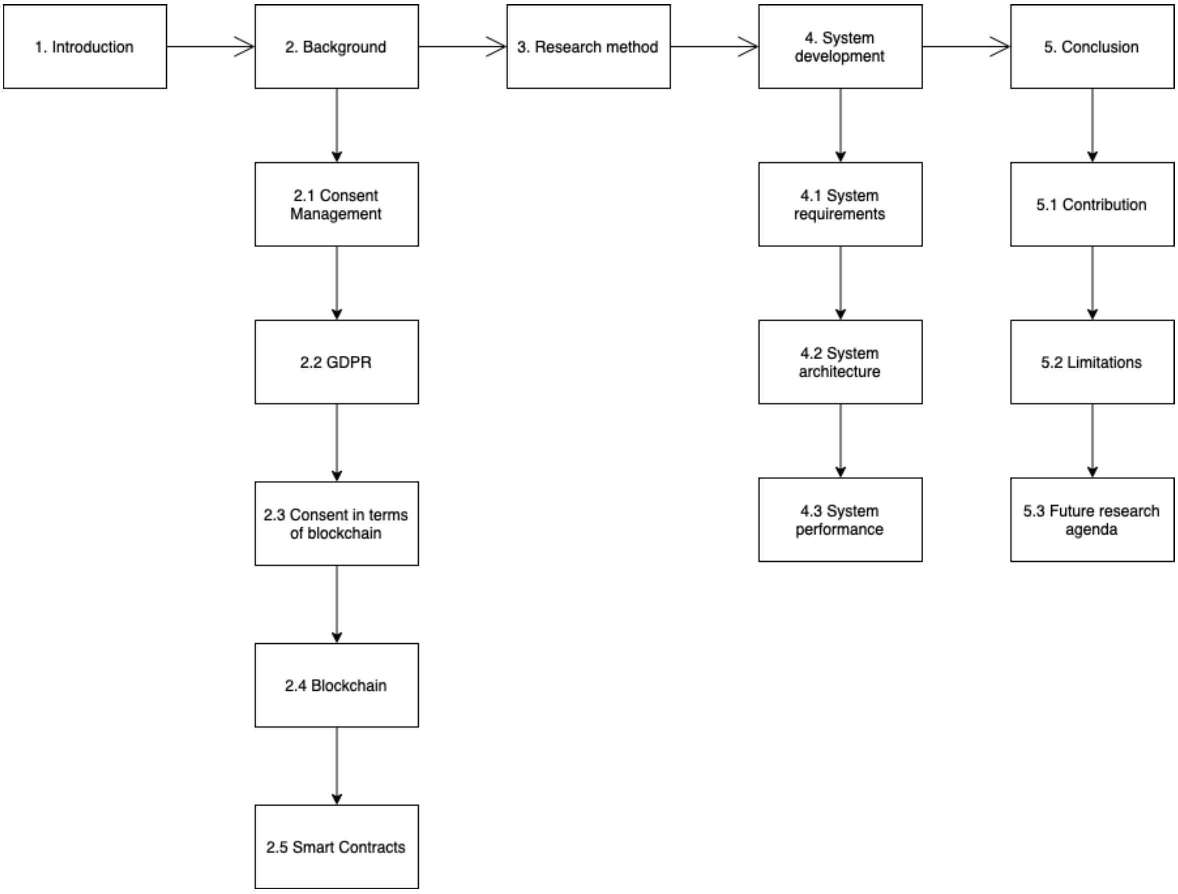


Figure 1 – Thesis structure

2 Background

This section describes consent roots, general definition, the purpose of the consent management itself within providing general information related to the blockchain technology, and conditions for consent collection in terms of GDPR.

2.1 Consent management

Roots of consent belong to social context, law compliance, behavior, and social science, ethical theory. Informed consent includes three criteria: understanding of the agreement, understanding that the agreement is not controlled by any forces and understanding of possible intervention. Compliance with these three criteria leads to informed consent (R. Faden, 1986).

Cambridge dictionary defines consent as agreement on something or permission for something (Cambridge dictionary). Consent is seen in the literature in the fields of health care, analysis, or marketing research. However, it can be noted that consent is intended to protect the personal information of an individual or data subject (IBM, 2021). The method for collecting personal information is called consent management. Consent management also allows the data subject to place restrictions on what personal information they intend to allow to be used. The process of consent management is not holistic, but consists of sequential steps (Gartner, 2022):

- The process of collecting consent
- The process of storing consent
- The process of using consent data

Personal information refers to information that identifies a specific individual or data subject. This information may include (N. Ramirez, 2022):

- name
- ID number
- telephone number
- email
- credit card number and details

- bank account number and details
- address
- location
- IP address
- documents
- written information
- subjective information
- health information
- biometric information
- adherence to a particular religion
- adherence to a particular political opinion
- photo and video

All listed information refers to a natural person. A natural person must have their personal data protected if they have legal capacity (GDPR, Personal data.).

Industry 4.0 is currently taking hold in the world with the digitalization of business processes, which results in an increasing amount of user, customer, and company data entering the Internet (J.Miller, 2019). This leads to the importance of the security of user data in the data processing. Therefore, the data subject should be informed that they have the right to access and delete their data and withdraw consent on demand, knowing that their data will be deleted in a defined period.

Areas where consent is used:

1. Health/ Medical concerns (examination appointment, consent to medical intervention, consent to data processing, consent to appointment)
2. Legal concerns (consent to data processing, consent to sign a contract, consent to process/receive a document)
3. Research/ Science work (consent to participate in the experiment, consent to the experiment procedure, consent to the collection of personal information)
4. Education (consent to data processing, consent to enroll in a training program, consent to a test/exam result)
5. Consumer (consent to the credit card data processing, consent to the client’s data processing)

6. Smart home devices (personal account processing, residential data processing)

2.2 General Data Protection Regulation

The General Data Protection Regulation (GDPR) is a European Union regulation stated in 2018 which aims to safeguard personal data (H. Platner, 2010). GDPR compliance does not only apply to European Union countries. It regulates all organizations, companies, and services that process data within the European Union. The justification for the processing of personal data of EU citizens and residents should be lawful, this applies to institutions regardless of their own location (P. Voigt, 2017). The aim of the GDPR is to ensure rights and liberty security associated with the protection of personal and confidentiality of data of the European Union citizens. The collection of data should directly lead to data subject notification.

GDPR (S. Sicari, 2015) defines conditions for legitimate data processing as:

- consent of the data subject grants data processing
- to fulfil the obligations stated in the contract
- to fulfil an obligation established by law
- to comply with the critical/vital needs of the data subject
- to respond to the public demand
- to respond to the legal basis of the controller profits

Data privacy laws, such as the GDPR, obligate companies to provide users with full information about what they consent to. It is the company's responsibility to show how the users' personal data would be used (V. Kakarlapudi, 2021).

2.3 Consent in General Data Protection Regulation

According to the GDPR, the consent agreement of the data subject must be concrete, freely granted, and unambiguous, and the data subject must be informed that by giving their consent, it approves actions aimed at personal data processing (GDPR, Article 4). The definition of the data subject in (GDPR, Article 4) is described as a natural person who has already been or might be authorized. Article 5 basis for consent processing under Union law or Member State law. On that basis, the controller applies to the conditioning process by law obligation or by representing public or authority interest.

The European GDPR also highlights the following terms for consent (GDPR, Article 7):

- In processing the data subject's consent, the controller must be able to demonstrate the fact that the data subject's consent to the processing of personal data has been provided
- When consent has been provided in writing form and the outlining of other issues, it is implied that consent has been provided separately in the context of giving consent.
- By giving consent, the data subject must be informed that he or she has the right to withdraw the consent at any time. If the consent is withdrawn after the data has been processed, this does not affect the lawfulness of the action taken.

Consent might be required not only from adults but also from children. Therefore (GDPR, Article 8) sets conditions for child consent. A child is a person under 16 years old. Processing of personal data, in that case, requires the consent agreement of the parent or legal representative is obligatory.

As stated in (GDPR, Article 9), ethnic, political, religious, philosophical, generic, biometric, and health data should be processed with the data subject’s consent and with protection. Personal user information should be stored with security and protection. According to (GDPR, Article 39) the time for user data storage should be strictly limited. The company/organization that collects user data oversees limiting the duration of user data storage. Also, there establishes a reasonable period for data processing as part of the consent.

Stored data should also identify the person who gave the consent. If there were a place for the consent of a data transfer to third parties such a transfer is possible (GDPR, Article 49).

Article of GDPR regulations could be divided into categories for who they are related to the data subject, the data controller, and the data processor. All articles related to consent regulation are presented in the table below.

Table 2 – Consent description in General Data Protection Regulation (GDPR, 2018)

Article number and name	Description	Subject of Article
Article 4 GDPR definition	The purpose and definitions of the GDPR are defined. Members and roles of data processing are set.	All
Article 6 Lawfulness of processing	This defines conditions for data processing, the lawful basis of data processing.	All
Article 7 GDPR conditions for consent	Define consent conditions and data controller participation.	Data subject, Data controller
Article 8 Child's consent	States conditions for collection of child consent.	Data subject, Data controller
Article 9 Special personal data processing	Provides a set of limitations for processing ethnic, political, religious, philosophical, generic, biometric, and health data.	All
Article 22 Automatically given consent	Provides a set of limitations for consent giving in terms of automated data processing.	Data subject, Data controller
Article 39 Data protection officer obligations	States tasks of protection of data subjects data.	All
Article 49 Exceptions	State restrictions for providing data subject data to third parties.	Data subject, Data controller

2.4 Blockchain

This subchapter describes the types of blockchain and the technologies that blockchain relies on smart contracts and consensus algorithms. Furthermore, how blockchain is related to consent management systems.

2.4.1 Blockchain technology definition

Blockchain technology is currently attracting significant attention. According to S. Ferdous, 2020, blockchain technology emerges from the intersection of the disciplines represented in Figure 2. These disciplines include software engineering, cryptography, distributive calculations, and game theory (K. Sultan, 2018). The use of these technologies ensures that blockchain contains characteristics such as:

- The system's information security
- A secure network architecture
- High computing speed
- System stability
- The system's openness

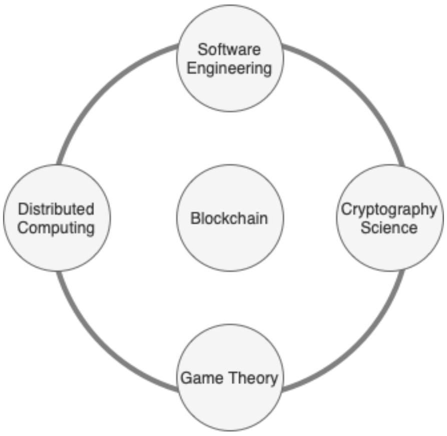


Figure 2 – Foundations of Blockchain

Four basic principles of blockchain can be identified (Merkle Tree):

- The use of cryptography to verify the transaction on the network.

Currently, there is a problem with synchronizing sent data with the recipient, as this operation requires updating the recipient's data ledger. Blockchain technology addresses this problem by using Proof of Work, Proof of Activity, Proof of Stake, and Proof of Weight algorithms.

- Distribution of information about transactions to a large number of participants in the system.

  Distribution of the database among the system participants avoids critical errors. Also, in case of a system failure, it makes it possible to save all copies without losses. The network participants can confirm the addition of new transactions during the check of the comparison with their forces.

  The presence of decentralization.

  The principle of a decentralized network is shown in Figure 3.

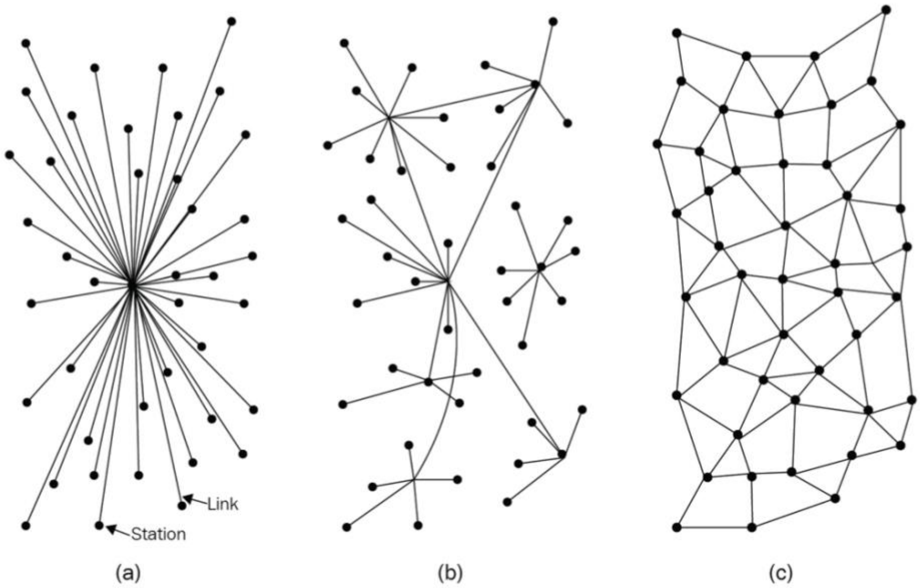


Figure 3 – Centralized (a), decentralized (b), distributed (c) network architecture (T. Swanson, 2015)

- Privacy

  The main unique feature of the technology is that blocks are stored simultaneously by all users of the network and are constantly updated and referenced. Moreover, if someone tries to cheat the system, a mismatch in the structure of the blocks will be detected instantly.

From a technical point of view, blockchain technology is built on the Merkle Tree. The Merkle Tree allows the data structure to be designed to minimize memory usage in proving the data's integrity. (Merkle Tree) Data in Merkle Tree is stored as layers. Merkle Tree uses one-way hash functions. They are responsible for creating the root of the tree, which is a merge of data layers. The Merkle Tree root function can validate all data located on the layers. This architecture is used in peer-to-peer (P2P) networks.

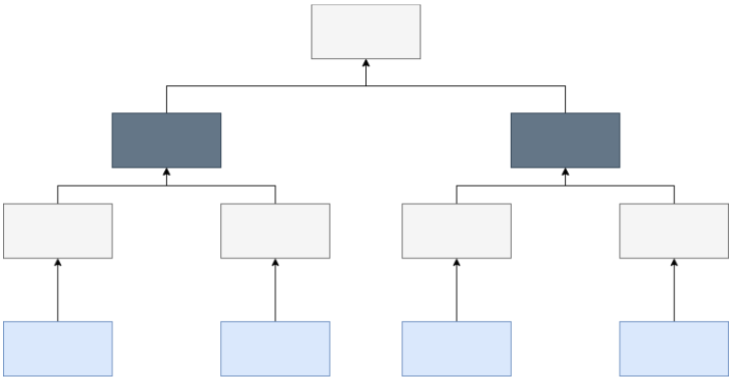


Figure 4 – Merkle Tree

Merkle Tree offers the following benefits (Merkle Tree, Blockchain):

- Rapid data verification. This is achieved due to the arrangement of the data in a layered format.
- Compactivity. The structure of the Tree saves storage space.
- Scalability. When data of one tree is checked, it could be decomposed into layers and then these layers could be checked independently.
- Quick data integrity checks. Also, due to its structure, fast checking of data on the layers can be achieved

The Merkle Tree's deployment in a blockchain network is highly crucial. The configuration of this tree, as mentioned above, reduces the amount and size of data, making it faster and more reliable to use the blockchain network.

Nowadays, blockchain technology is applicable to the software computing and cryptocurrency area. Blockchain technology's application area is much wider, including the internet of things, medicine, banks, insurance, governance, and contract management.

Negotiating their operation with consensus algorithms ensures that blockchain-based applications work consistently and securely (W. Viriyasitavat, 2017). Cryptography in the blockchain is used to verify the transaction on the network. Synchronization of sent data with the recipient is currently a challenge, as this operation requires updating the recipient's data ledger. Blockchain technology can solve this problem by using Proof of Work, Proof of Activity, Proof of Stake, and Proof of Weight algorithms.

Blockchain technology uses consensus algorithms to validate blocks in a chain. Depending on the user case, different blockchains use different consensus principles. (W. Viriyasitavat, 2017) Consensus algorithms such as Proof-based Consensus Algorithms and Voting-based Consensus Algorithms can be divided into two primary classes. (S. Ferdous, 2020)

2.4.2 Consensus algorithms

Blockchain technology combines peer-to-peer networks and distributed consensus algorithms to solve the synchronization problems of traditional distributed databases. Cryptography, algorithms, economic models, mathematics techniques, and their combinations are used in blockchain technology. (J. Garay, 2015) states that consensus algorithms are used to identify if the block in the chain was created.

The use of consensus models helps to maintain data integrity recorded on the blockchain. Three main properties of consensus algorithms can be identified (T. Swanson, 2015):

- Security
  Protocol states rules according to which all nodes must produce the same result. This will ensure the security and consistency of the algorithm
- Survivability
  If a node fails, it is responsible for producing a value and must still produce it.
- Fault tolerance
  In the event of a node failure or malfunction, it must be recovered

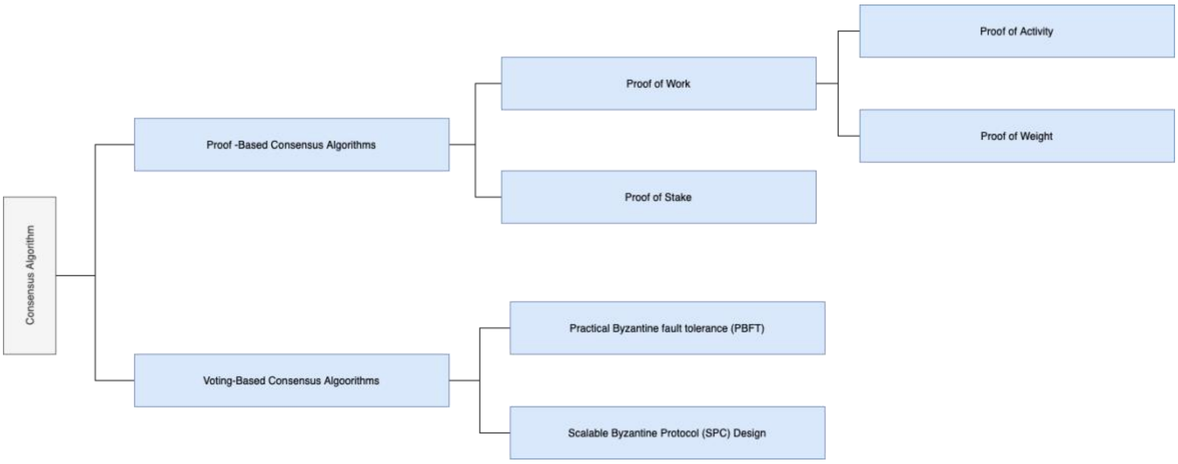

Consensus Algorithm
Proof -Based Consensus Algorithms
Proof of Work
Proof of Activity
Proof of Weight
Proof of Stake
Voting-Based Consensus Algoorithms
Practical Byzantine fault tolerance (PBFT)
Scalable Byzantine Protocol (SPC) Design

Figure 5 – Consensus Algorithms Classification

Proof-based Consensus Algorithms

Consensus Algorithms can be divided into two main categories. The first category refers to proof-based algorithms. These can be highlighted as proof-of-work, proof-of-stake, proof-of-activity, proof-of-weight, and their hybrid variations.

Proof of Work

This consensus algorithm is used to confirm the appearance of a new block in the chain by validating the performance of certain cryptographic calculations. Contributors can use a proof-of-work algorithm to confirm that calculation resources were used. Work of this type of proof-based algorithm can be described as a function that refers to true, or false as a result of verification.

$$F_d(c, x)\{true, false\}$$

where parameters c, x, d are known. (R. Wattenhofer, 2016)

Proof of Stake

This consensus algorithm works by proving that a particular participant's stake representing their ability to create a new block is the same as the participant's stake in cryptocurrency.

Proof of Activity

Within this algorithm, the consensus uses fewer resources to prove the creation of a new block. In Proof of Activity, limits are set on the time it takes to add a block to the chain—restrictions for the maximum speed of adding to the network a new block.

Proof of Weight

Another purpose of using proof-of-work is to control the rate at which blocks appear on the network. By controlling the rate at which blocks appear, a constant level of average blockchain growth rate can be maintained.

Voting-based Consensus Algorithms.

These algorithms operate on the principle of voting for a particular consensus (G. Nguyen, 2018). Typically, such algorithms set a minimum for votes amount or compare the percentage of votes cast for decision making.

Practical Byzantine fault tolerance (PBFT)

The concept of (Byzantine) error comes from the Byzantine General Dilemma. This logical dilemma was outlined in 1982. The dilemma aims to reach a consensus between the generals and find a solution each side supports.

To find a solution, the following should be considered:

- The parties must decide to either attack or retreat.
- The parties must agree on a single decision at a time.
- The decision reached is final.

The main drawback of this dilemma is that the parties do not communicate directly but pass messages through an intermediary. The consequence of this is a delayed, lost, or intentionally deleted message. Messages can also be deliberately misspelled.

(M. Castro, 2001) This dilemma in the blockchain network occurs between nodes that need to come to a consensus. Members of the network must agree to perform a single action. The network should consist of a minimum of ⅔ of the total number of nodes to meet the needs of that consensus algorithm. The advantage of this algorithm is that if 1/3 of the nodes fail, the system will remain operational.

Scalable Byzantine Protocol (SPC) Design

(C. Berger, 2018) Scalable Byzantine Protocols can be classified according to purpose:

- Optimizing the use of many nodes in a network – Algorand
- High operating speed optimizing – FastBFT
- Optimizing for network failures and bad network conditions – HoneyBadgerBFT
- Optimize system capacity – OmniLedger

All protocols are adaptable to the specific needs of the application designer. Also, the scalability can be based on the type of communication chosen in the system used. The types of scalability are depicted in Figure 6.

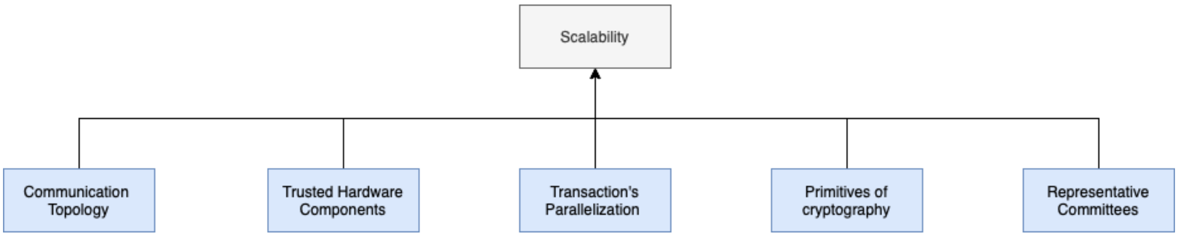

Scalability
Communication Topology
Trusted Hardware Components
Transaction's Parallelization
Primitives of cryptography
Representative Committees

Figure 6 – Types of scalabilities in Byzantine Protocols

2.4.3 Public blockchain

Blockchain can be classified according to the architecture of the network - public, private, or consortium. (A. Prashanth Joshi, 2018) These architectures differ in the degree to which nodes in the network can participate openly.

A public blockchain is the first stage in the development of this technology. (E. Kathleen, 2021) A feature of a public blockchain is that every network user can view the full history of transactions and verify that a particular transaction took place.

However, this approach has the major disadvantage of demanding significant computing power. (B. Haque, 2021)

2.4.4 Private blockchain

A private blockchain responds to a request for user authorization. (T. Tuan, 2017) This means that a blockchain participant must first be authenticated to the network. This prevents free entry and exit into the blockchain network.

2.4.5 Consortium blockchain

Consortium blockchain technology is used in large enterprises for consensus building and is also a public in-network use (W, Yao, 2021). This allows users with access rights to all transactions to inspect them, while others do not have this right.

Table 3 – Comparison of Public, Private, and Consortium blockchain

	Public blockchain	Private blockchain	Consortium blockchain
Centralized	No	Yes	Partial
Transaction verification	All users	Selected users	Predefined users
Who control network security	All users	Selected users	Predefined nodes
Who participate in consensus	All nodes	Selected nodes	Predefined nodes
Nodes participation	Nodes validation	Block validation	Block validation

2.4.6 Smart contracts

Smart contracts could be outlined as class declarations in the object-oriented programming paradigm, consisting of a set of variables used to describe their states and a set of functions whose logic is laid down by the developer of these contracts. (Byzantine Fault Tolerance Explained, 2018)

Security of smart contracts against attacks is critical; smart contracts manage valuable and important resources. Attacks can steal these resources or disable contracts.

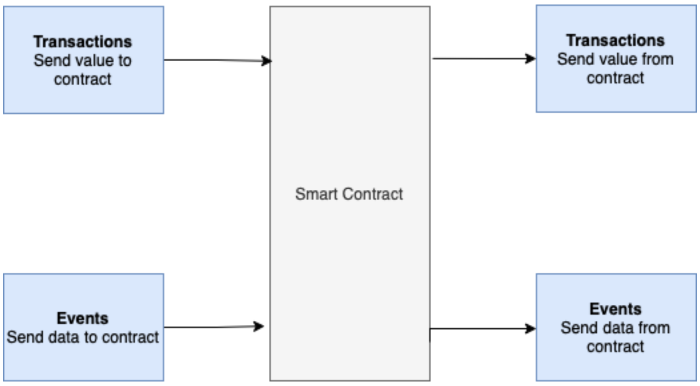


Figure 7 – Smart Contract

Smart contracts can also be described as a software process that received data and delivers the outputs. The key feature of this process is that program code cannot be modified. A contract is signed, i.e. by fulfilling the terms of the contract, the user receives the agreed outcome in return.

2.5 Blockchain-based consent management

According to the GDPR, collecting and informing users of their consent for personal data processing is critical. By decentralizing blockchain technology, information about each transaction is permanently stored in a blockchain. In this way, information about whether the user has given or withdrawn their consent is permanently stored and users can always verify this.

The decentralized storage process of the blockchain ensures transparency so that transactions made on the blockchain network can be traced. A network’s decentralization ensures that there is no single governance authority, nodes and participants in the network manage such networks (S. Medvedeva, 2019). The information does not have a common repository and is also distributed in a decentralized way in blocks of the blockchain network. Users of blockchain networks have the right to see the history of all transactions (J. Garay, 2015), which means that a user's consent can be tracked, and an external party cannot manipulate that consent data. This property of blockchain can be described as immutability. When consent is given or withheld, it is written to the blockchain, and information about it cannot be modified. The user’s personal information remains anonymous. This is achieved with a public key (S. Nakamoto, 2008) that is accessible and can be used to verify the transaction, while at the same time the user can explicitly view data with the private key. Blockchain stores the data in an encrypted form, a hash. If necessary, the hash can be merged into a distributed hash table. (S. Medvedeva, 2019) The application of blockchain technology in consent management is promising. Blockchain technology in consent management can be used to achieve secure storage of user data, transparency of received/stored user data, and control data management.

3 Research method

This section contains a research method description and justification with the following explanation of the research stages.

3.1 Design Thinking

Design Thinking methodology is applied to the industry as it mostly refers to a solution-based approach to problem-solving. The Design Thinking methodology is proposed by Stanfords Hasso-Plattner Institute of Design (H. Platner, 2010). It consists of five steps that guide researchers to build a solution orientated to people's needs. Figure 8 shows five main Design Thinking steps.

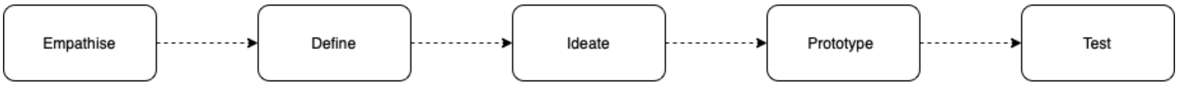


Figure 8 – Design Thinking process

However, depending on the developing solution, iterations between stages might be different for each case. Design Thinking methodology defines five steps that would occur in a problem-solving project. In contrast, the sequence of the steps could be modified based on the developing solution, meaning the flexibility of the developing process.

Current research will be held as presented in Figure 9. This combination of Prototype-Define, Test- Prototype and Test-Ideate loops allows using practical experience to improve project functionality and practical use. Therefore, the solution would fit user needs and be properly developed.

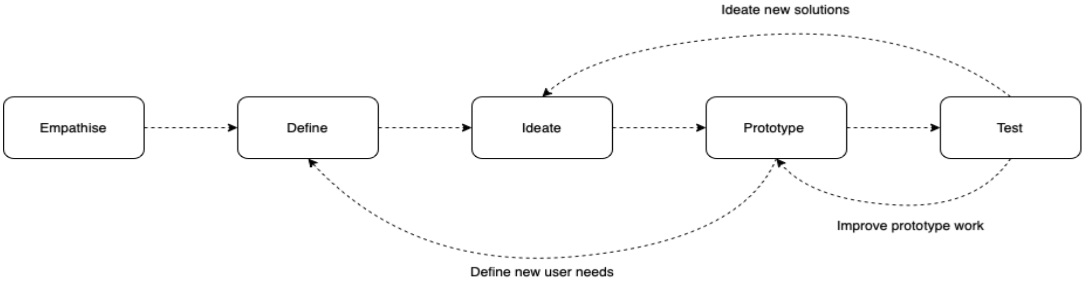


Figure 9 – Research method

3.1.1 Empathise

The aim of empathizing is to understand people's emotional and physical needs. By understanding and predicting people's needs, it is easy to suggest useful decisions which would fulfill their needs. The real value of communication is to understand people's values and to think processes that might help to develop or improve solutions regarding discussing issues. The observer, in discussing the processes of daily life, can highlight patterns or areas that need to be improved. Allocating such patterns makes it possible to provide the user with the desired product and to widespread it. Key elements of the empathizing process are:

- To observe
- To engage
- To watch and listen

After following these steps, the conclusions can be drawn, and the process would move to the Define step where all results would be analyzed.

3.1.2 Define

Define step is a process of analyzing collected information and synthesis in logical order. As a result of the conducted analysis, a statement and the following arguments would be concluded. This step answers the question “What should be done?”.

3.1.3 Ideate

Ideate step answers the question “How?”. The aim of this step is to know how the problem would be solved and to generate solution ideas. There are some techniques for idea generation (A. Bureau, 2022):

- Mind Mapping
- Brainstorm
- Reverse thinking
- Worst Possible Idea
- SCAMPER
- The 5 W's (Who, What, Where, When, Why)

And also, tools such as Pinterest, Mindmaster, Mindomo would be helpful to complete this step.

3.1.4 Prototype

This step aims to evaluate and investigate the efficiency of proposed ideas and define the best solution. As a result of this stage, the product limitations and possibilities would become apparent as a better understanding of users’ behavior.

3.1.5 Test

Testing step clearly shows the actual behavior of the system therefore this step could be connected to each previous step to redefine the problem statement or improve the existing prototype.

3.2 Conducted research activities to identify requirements

To detect system requirements the following work was done. As presented in Figure 10 main sources of requirements were conducted in academic literature analysis, which is located in Appendix section table 8, together with the General Data Protection Regulation study and analysis of existing solutions (Appendix section table 9). All results and conclusions reached during the research work were discussed with two blockchain experts.

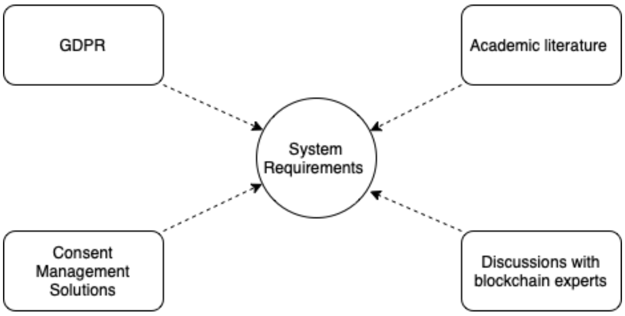

GDPR
Academic literature
System Requirements
Consent Management Solutions
Discussions with blockchain experts

Figure 10 – Sources of requirements

4 System development

In developing a blockchain-based general consent management system, it is important to highlight the essential requirements that the system should meet, namely integrity, verifiability, trust in versions, and system design. All listed requirements are achievable through a decentralized blockchain network.

(GDPR, Article 4) define the following types of personal data:

1. Personal data
   That type of data consists of personal information which can point to one specific individual.

2. Genetic data
   That type of data contains genetic information which can point to one specific individual.

3. Biometric data
   That type of data is collected physiological or behavioral characteristics from the data subject which can point to one specific individual.

4. Data concerning health
   That type of data contains information about data subject to physical or mental health that can point to one specific individual.

Development tools:

The system should consist of two parts both the frontend and backend. The frontend would have a user interface with minimal features. The backend of the system should have the implementation of algorithm logic using solidity.

Tools for frontend development are listed below:

- JavaScript – for providing logic of the user interface.
- Vue.js – JavaScript framework for user interface creation.
- MetaMask – crypto wallet which allows users to collaborate with the Ethereum network.

Backend development was performed with the following tools.

- Solidity – programming language which allows performing smart contracts development.
- RemixIDE – an online IDE for Solidity programming. This IDE allows the programming, deploying, and testing of developed smart contracts in the Ethereum network.
- Python/FastAPI – programing language for creating logic for database and frontend connection in FasiAPI framework.
- PostgreSQL – object-relational database for storing user information.

4.1 System requirements

Based on observed academic literature placed in Table 8 and Table 9, GDPR requirements which are stated in Part 2.2 following main system requirements were indicated and described:

1. Consent states

   Consent should apply to be clearly stated, determined, and freely collected. The data subject decides whether to give consent based on the conditions stated in the consent form
2. Consent collection

   Consent should be provided in text or verbal statements. This means that whenever there is a need for a data subject to give consent there should be a form either digital or paper for collecting consent.
3. Consent aim

   Consent given by the data subject should fulfill all stated purposes only.
4. Consent request

   Consent request should contain a short description of its purpose. The consent form should not interfere with the review of the service/product for which consent is required
5. The data subject rights

   Data subjects legally can give or withdraw consent within their will.
6. The data storage

This requirement means that the data of the data subject, i.e. the user, should be stored off-chain (in traditional storage). This type of data storage will not cause a collision if the data subject requests data removal.

7. The controller duty

   Controllers can manage user consent only under GDPR regulation and should always be able to prove a legal basis for user data processing. To ensure consistency with GDPR, smart contracts will be used in this developing system. Smart contracts allow tracking of consent because a record of it can be traced back to the user

General personal data for collection:

1. username (optional)
2. name
3. contact information (e-mail, phone number)
4. ID details
5. Consent (Y/N)

4.2 System architecture

The system contains three main roles, these are Data Subject, Data Controller, and Data Processor (GDPR, Article 4).

1. Data Subject is a natural or legal person in relation to whom data protection and processing are structured. Data Subjects have two main functions which they can perform on consent to provide and to withdraw their consent. These functions control the processing of their data by the data subject side. Data Subjects should also be able to access consent history and be able to check under what conditions and for what purposes their data is collected

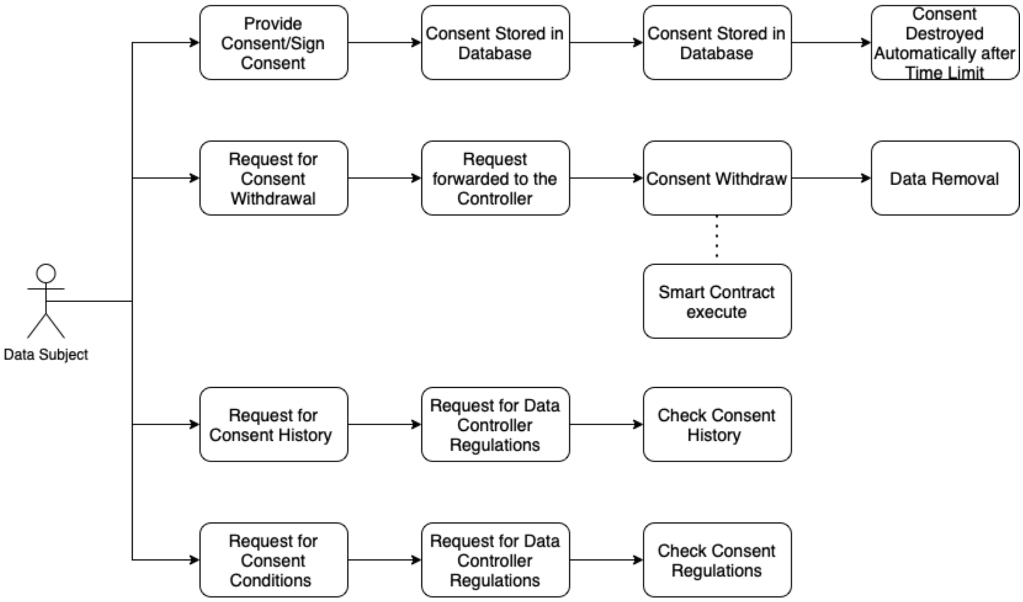

Provide Consent/Sign Consent
Consent Stored in Database
Consent Stored in Database
Consent Destroyed Automatically after Time Limit
Request for Consent Withdrawal
Request forwarded to the Controller
Consent Withdraw
Data Removal
Smart Contract execute
Data Subject
Request for Consent History
Request for Data Controller Regulations
Check Consent History
Request for Consent Conditions
Request for Data Controller Regulations
Check Consent Regulations

Figure 11 – Data Subject

2. Data Controller is a natural or legal person who oversees personal data processing.

The data controller provides context, and scope and defines the purpose for which data should be processed, updated, and deleted.

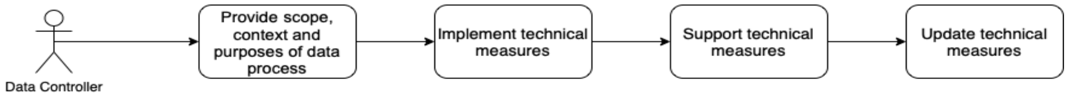

Data Controller
Provide scope, context and purposes of data process
Implement technical measures
Support technical measures
Update technical measures

Figure 12 – Data Controller

3. Data Processor is a natural or legal person or authority whose responsibilities are to ensure data process compliance with controller regulations.

The Data Processor acts directly to present Data controller regulations, whose mission is to ensure that all the rules and regulations that the Data controller has established. The Data Processor is processing data according to Data Controller.

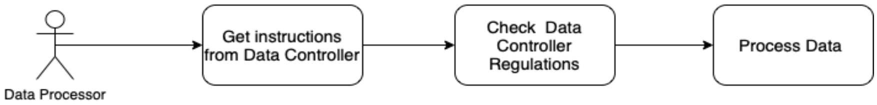

Data Processor
Get instructions from Data Controller
Check Data Controller Regulations
Process Data

Figure 13 – Data Processor

The system should have a user interface that allows users to interact with the system. As well as perform such actions as login, send consent, withdraw consent, view consent terms, and view consent history.

The system under development should have several types of storage. According to the GDPR, the consent of a data subject has the property of deleting data, so data about the data subject must be stored in the Database. Consent management is conveniently implemented by blockchain technology, so that user consents will be stored in the blockchain.

The system must have User Consent Management, User Profile Management, and GDPR Complains. User Consent Management controls Data Processor based on Data Controller regulations. User Profile Management is controlled by the Data Controller, it sets regulations to handle user consent. The GDPR Complains module is needed to verify that user consent regulations are compliant with GDPR regulations.

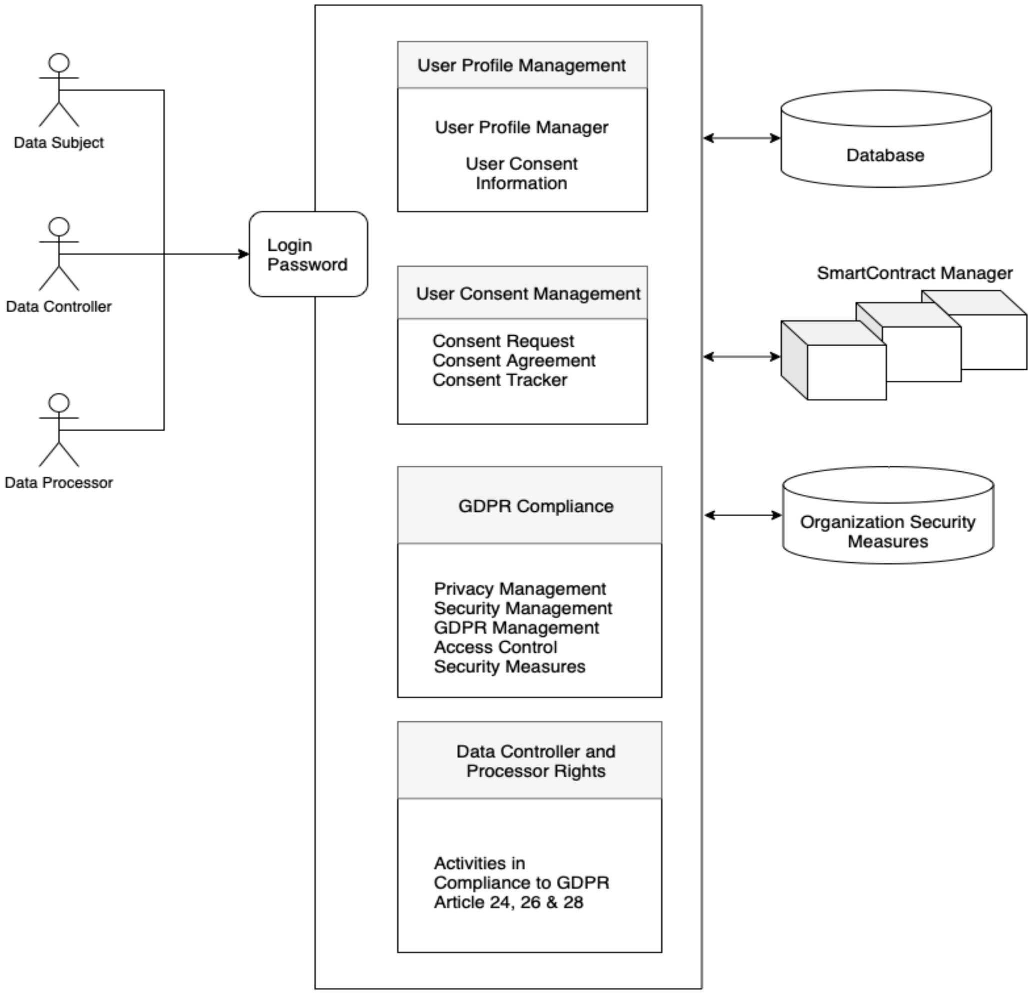


Figure 14 – System Architecture

The aim of the system is to store user data, especially consent information securely. Algorithm 1 work is to save user consent in the blockchain and memorizing the timestamp of each consent.

Table 4 – Algorithm 1

Algorithm 1: Save user consent
Input: Consent hash
Output: Consent saved

if Consent status != confirmed **then**
    save Consent and set a creation timestamp of Consent
else do nothing

User consent could have three statuses: confirmed, withdrawn, expired. Condition for confirmed status is providing consent, for withdrawn status is fulfilled request for consent withdrawn by the user, and for expired status is consent to be given over a 90 days period. The second algorithm is aimed to show a current consent status.

Table 5 – Algorithm 2

```
Algorithm 2: Get user consent status
Input: User address
Output: Consent status
if Consent was withdrawn then
    Consent status is Withdrawn
if Consent timestamp was created more than 90 days ago then
    Consent status is Expired
else Consent status is Confirmed
```

In the system controller has a responsibility of withdrawn user consent as it is shown in algorithm 3.

Table 6 – Algorithm 3

```
Algorithm 3: Withdraw user consent
Input: User address
Output: Consent status Withdrawn
if caller == owner then
    if Consent status != withdrawn and Consent status != Expired then
Consent status == Withdrawn
```

4.3 System performance

Figure 15 contains attributes, functions, struct and modifier that Consent smart contract holds and processes.

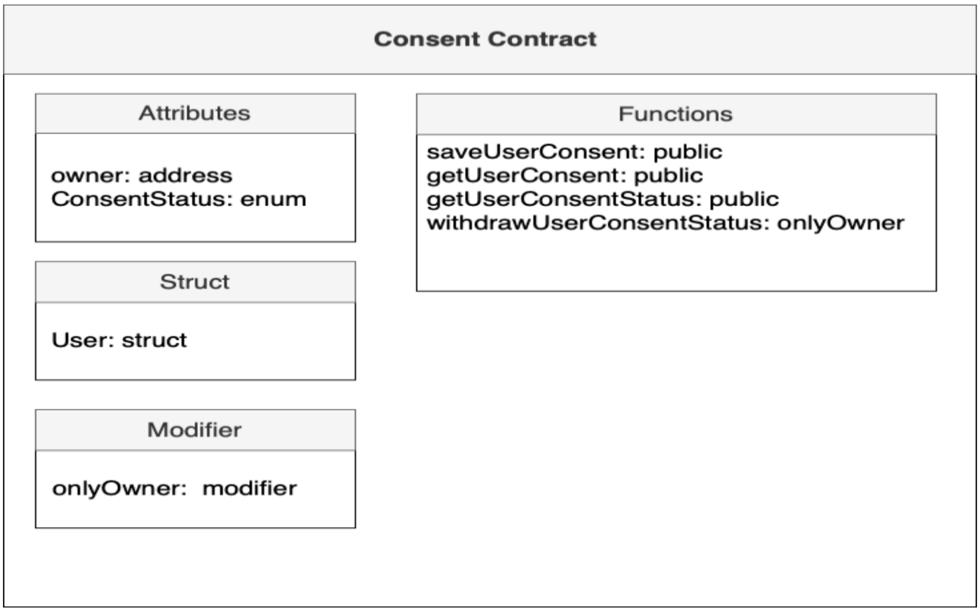
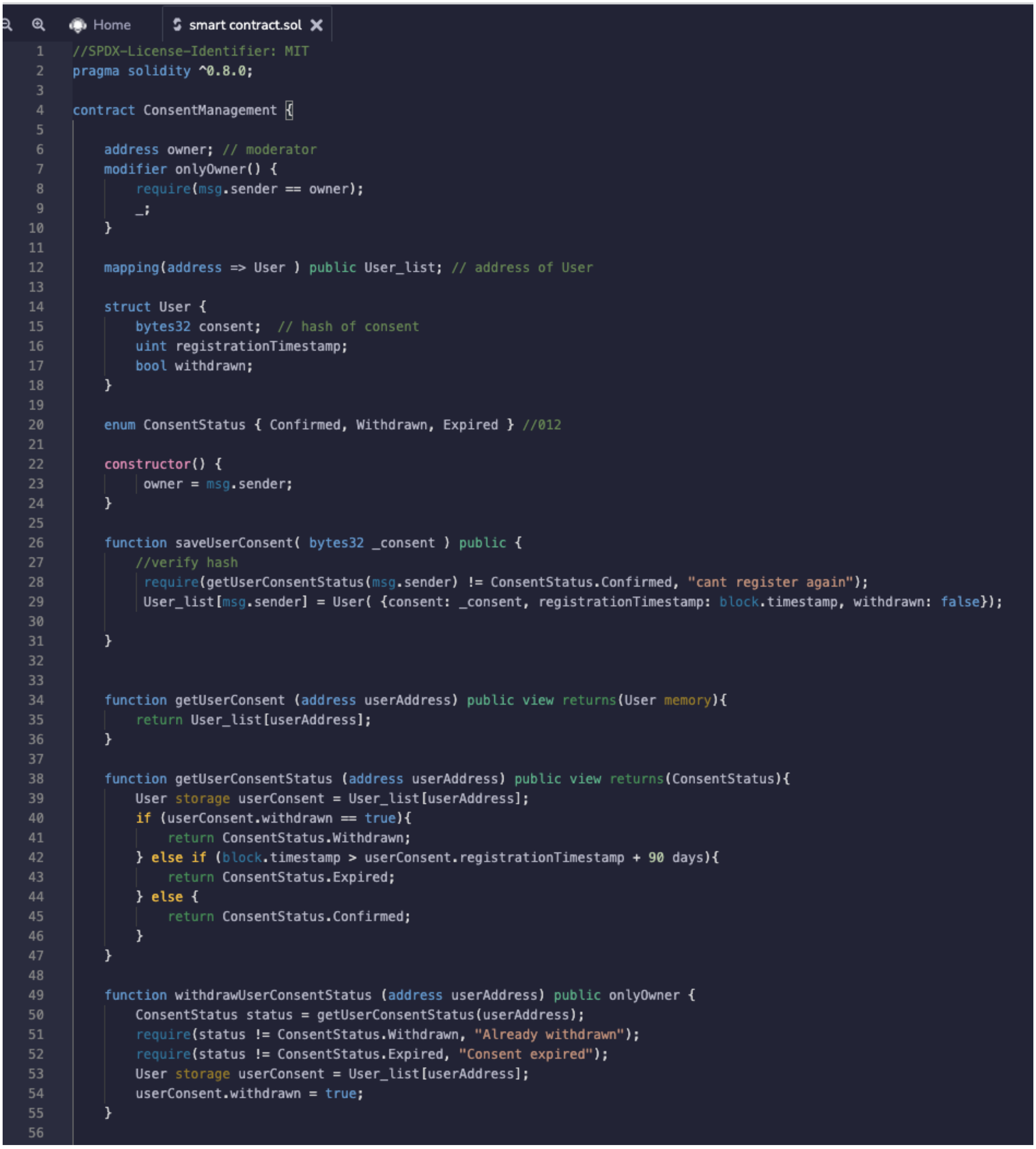


Figure 15 – Smart Contract

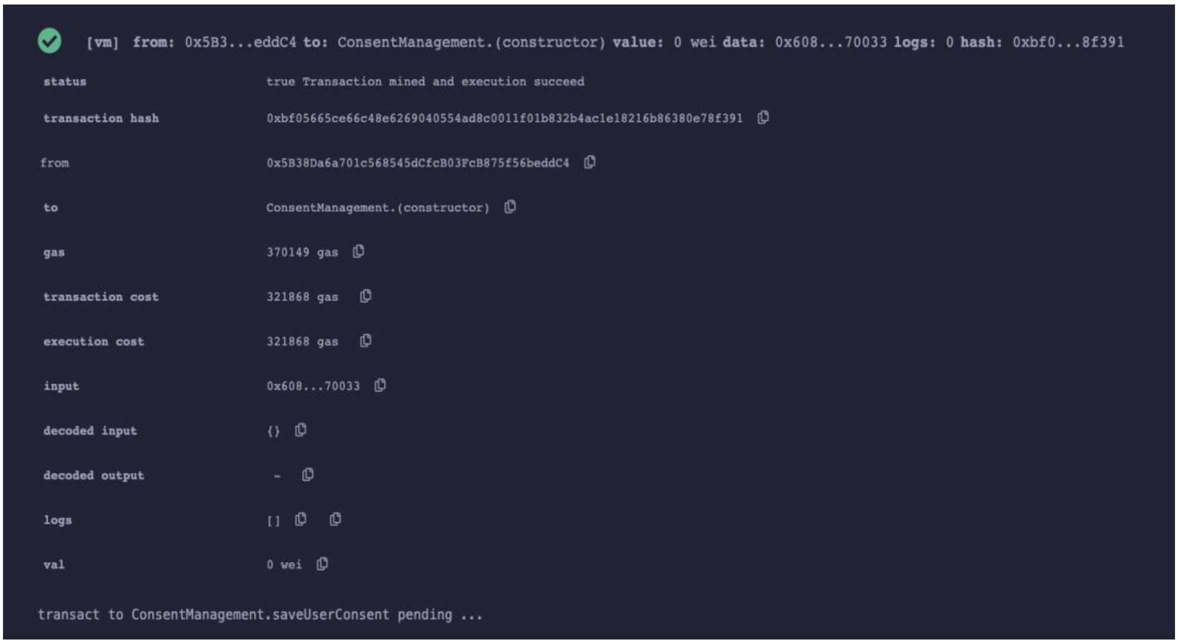
Figure 16 shows the code of the executed smart contract. Smart contract algorithms were described in tables: Table 4 – Algorithm 1, Table 5 – Algorithm 2, Table 6– Algorithm 3. Smart Contract execution was held in Remix IDE and the development language was Solidity.



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

contract ConsentManagement {

    address owner; // moderator
    modifier onlyOwner() {
        require(msg.sender == owner);
        _;
    }

    mapping(address => User ) public User_list; // address of User

    struct User {
        bytes32 consent;  // hash of consent
        uint registrationTimestamp;
        bool withdrawn;
    }

    enum ConsentStatus { Confirmed, Withdrawn, Expired } //012

    constructor() {
         owner = msg.sender;
    }

    function saveUserConsent( bytes32 _consent ) public {
        //verify hash
         require(getUserConsentStatus(msg.sender) != ConsentStatus.Confirmed, "cant register again");
         User_list[msg.sender] = User( {consent: _consent, registrationTimestamp: block.timestamp, withdrawn: false});

    }


    function getUserConsent (address userAddress) public view returns(User memory){
        return User_list[userAddress];
    }

    function getUserConsentStatus (address userAddress) public view returns(ConsentStatus){
        User storage userConsent = User_list[userAddress];
        if (userConsent.withdrawn == true){
            return ConsentStatus.Withdrawn;
        } else if (block.timestamp > userConsent.registrationTimestamp + 90 days){
            return ConsentStatus.Expired;
        } else {
            return ConsentStatus.Confirmed;
        }
    }

    function withdrawUserConsentStatus (address userAddress) public onlyOwner {
        ConsentStatus status = getUserConsentStatus(userAddress);
        require(status != ConsentStatus.Withdrawn, "Already withdrawn");
        require(status != ConsentStatus.Expired, "Consent expired");
        User storage userConsent = User_list[userAddress];
        userConsent.withdrawn = true;
    }

```

Figure 16 – Executed Smart Contract

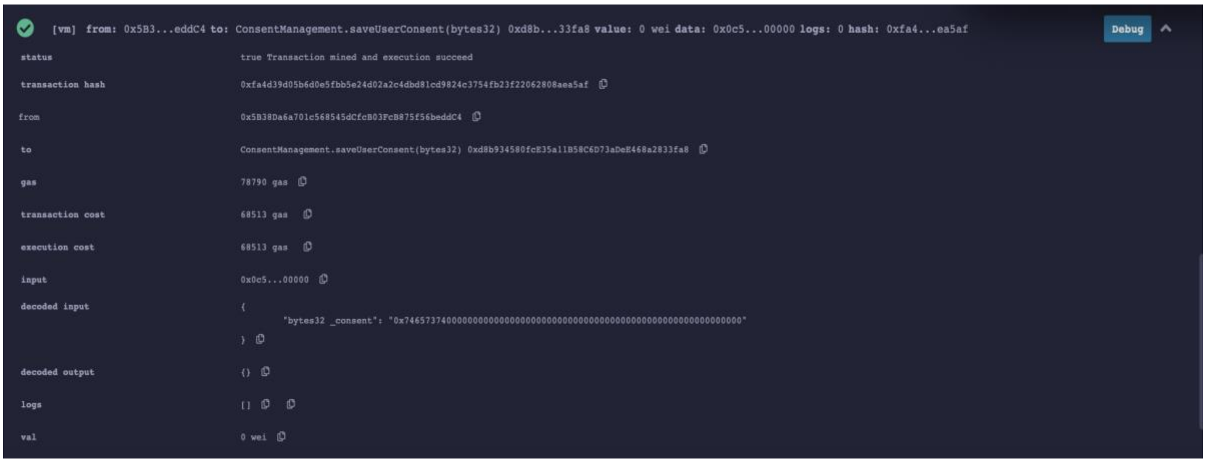
After a smart contract gets a hash of the user wallet crypto signature it saves with saveUserConsent( ) function in a list of users with a tame stamp. To work with user consent, getUserConsent( ), getUserConsentStatus( ) and withdrawUserConsentStatus( ) functions were developed. Function getUserConsent( ) is used for further work with user data. Function getUserConsentStatus( ) can be called by the user to check consent status. According to the GDPR data controller who is represented as onlyOwner can only withdraw user consent; that is why withdrawUserConsentStatus( ) function can be called by onlyOwner.



```
[vm]  from: 0x5B3...eddC4 to: ConsentManagement.(constructor) value: 0 wei data: 0x608...70033 logs: 0 hash: 0xbf0...8f391
status                  true Transaction mined and execution succeed
transaction hash        0xbf05665ce66c48e6269040554ad8c0011f01b832b4ac1e18216b86380e78f391
from                    0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to                      ConsentManagement.(constructor)
gas                     370149 gas
transaction cost        321868 gas
execution cost          321868 gas
input                   0x608...70033
decoded input           {}
decoded output           -
logs                    []
val                     0 wei
transact to ConsentManagement.saveUserConsent pending ...
```

Figure 17 – Contract Deployment gas cost

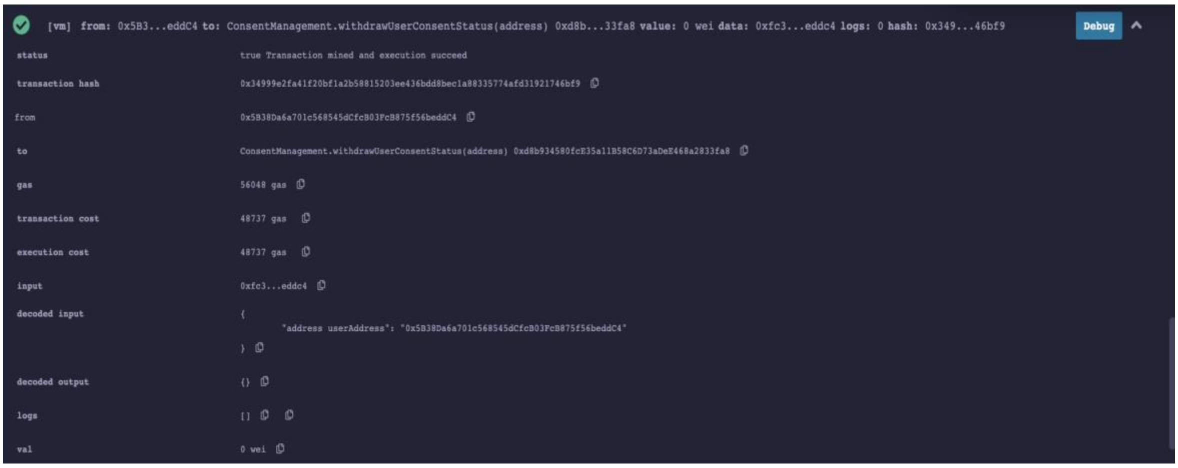
All transactions in the Ethereum network require computational effort for example for smart contract execution. To measure computational effort Gas is calculated which also could be described as a network fee for transaction conducting. In Ethereum Network native currency is Ether (ETH) with which Gas is paid. However, Gas prices are calculated in Gwei which is equal to 0.000000001 ETH.



```
[vm]  from: 0x5B3...eddC4 to: ConsentManagement.saveUserConsent(bytes32) 0xd8b...33fa8 value: 0 wei data: 0x0c5...00000 logs: 0 hash: 0xfa4...ea5af
status                  true Transaction mined and execution succeed
transaction hash        0xfa4d39d05b6d0e5fbb5e24d02a2c4dbd81cd9824c3754fb23f22062808aea5af
from                    0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to                      ConsentManagement.saveUserConsent(bytes32) 0xd8b934580fcE35a11B58C6D73aDeE468a2833fa8
gas                     78790 gas
transaction cost        68513 gas
execution cost          68513 gas
input                   0x0c5...00000
decoded input           {
                              "bytes32 _consent": "0x7465737400000000000000000000000000000000000000000000000000000000"
                        }
decoded output          {}
logs                    []
val                     0 wei
```

Figure 18 – saveUserConsent( ) gas cost

Calling saveUserConsent( ) and withdrawUserConsentStatus( ) functions would have a Gas price for users each time they interact with those functions. The gas cost would be validated in terms of network and miner’s workload.



```
[vm] from: 0x5B3...eddC4 to: ConsentManagement.withdrawUserConsentStatus(address) 0xd8b...33fa8 value: 0 wei data: 0xfc3...eddc4 logs: 0 hash: 0x349...46bf9
status                  true Transaction mined and execution succeed
transaction hash        0x34999e2fa41f20bf1a2b58815203ee436bdd8bec1a88335774afd31921746bf9
from                    0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to                      ConsentManagement.withdrawUserConsentStatus(address) 0xd8b934580fcE35a11B58C6D73aDeE468a2833fa8
gas                     56048 gas
transaction cost        48737 gas
execution cost          48737 gas
input                   0xfc3...eddc4
decoded input           {
                              "address userAddress": "0x5B38Da6a701c568545dCfcB03FcB875f56beddC4"
                        }
decoded output          {}
logs                    []
val                     0 wei
```

Figure 19 – withdrawUserConsentStatus( ) gas cost

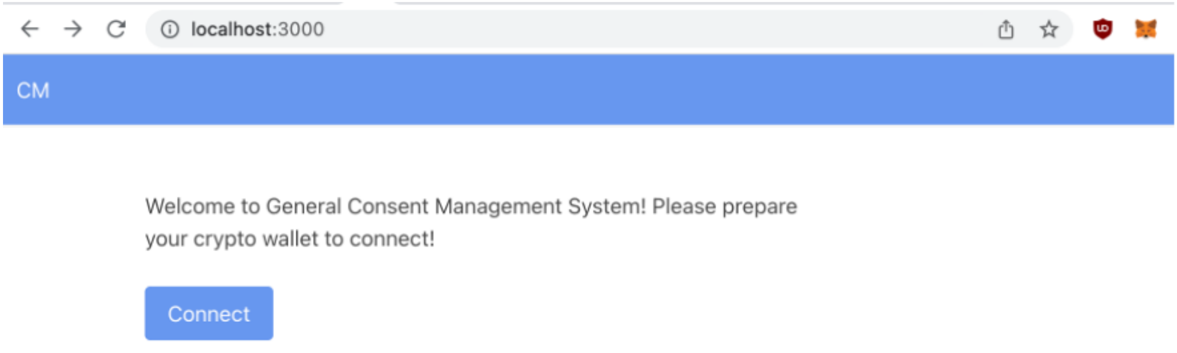
In the table below gas prices of saveUserConsent( ) and withdrawUserConsentStatus( ) functions with smart contract deployment cost are summed up. Cost of functions getUserConsent( ) and getUserConsentStatus( ) are view functions Cost only apply when called by a contract.

Table 7 – Gas price of transactions

Task	Transaction cost	Execution cost
Contract Deployment	321868	321868
saveUserConsent( )	68513	68513
withdrawUserConsentStatus( )	48537	48537

Figures 20-35 shows system behavior and interface for user and administrator. The system administrator performs data processor and data controller functions.

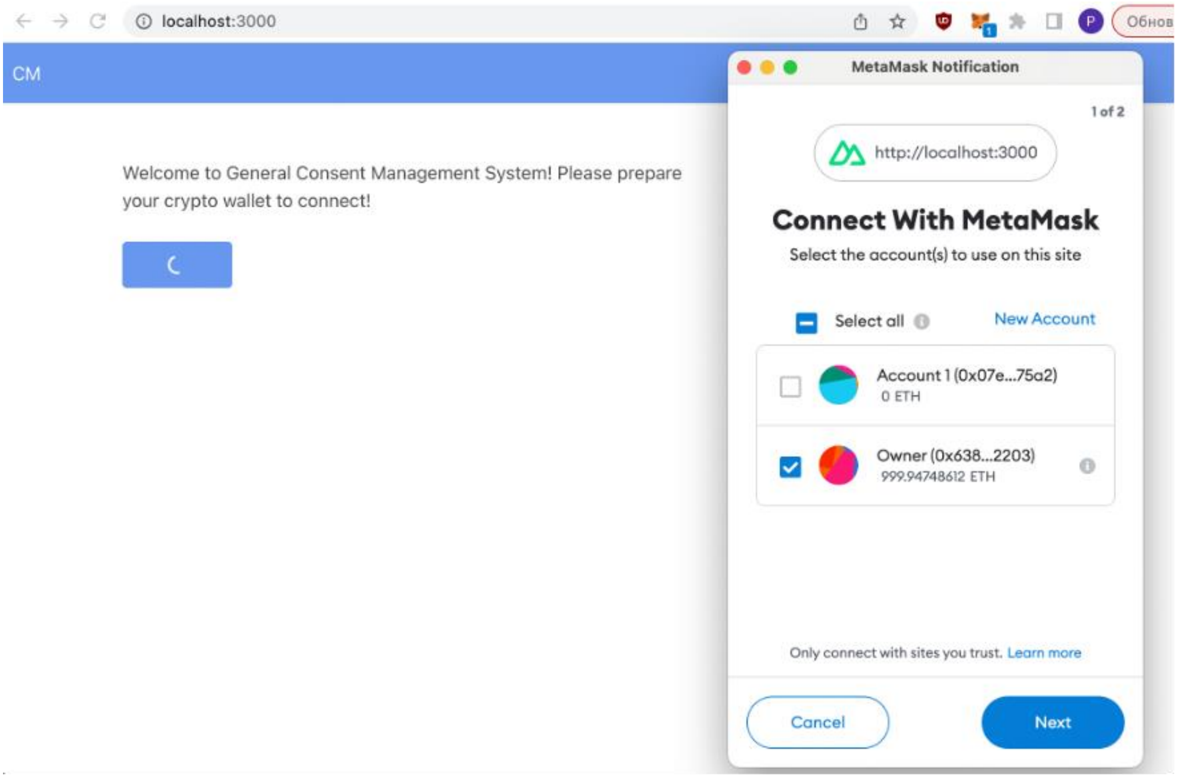
Figure 20 represents the main screen of the system. To use the General Consent Management System user should own a crypto wallet. The system was tested with MetaMask wallet.



Welcome to General Consent Management System! Please prepare your crypto wallet to connect!

Figure 20 – Main screen

Process of wallet connection is shown in Figure 21. The user connects to the MetaMask wallet and chooses an account for further use. After connecting to the crypto wallet user is redirected to the registration page which is shown in Figure 22 below.



Welcome to General Consent Management System! Please prepare your crypto wallet to connect!

Connect With MetaMask

Select the account(s) to use on this site

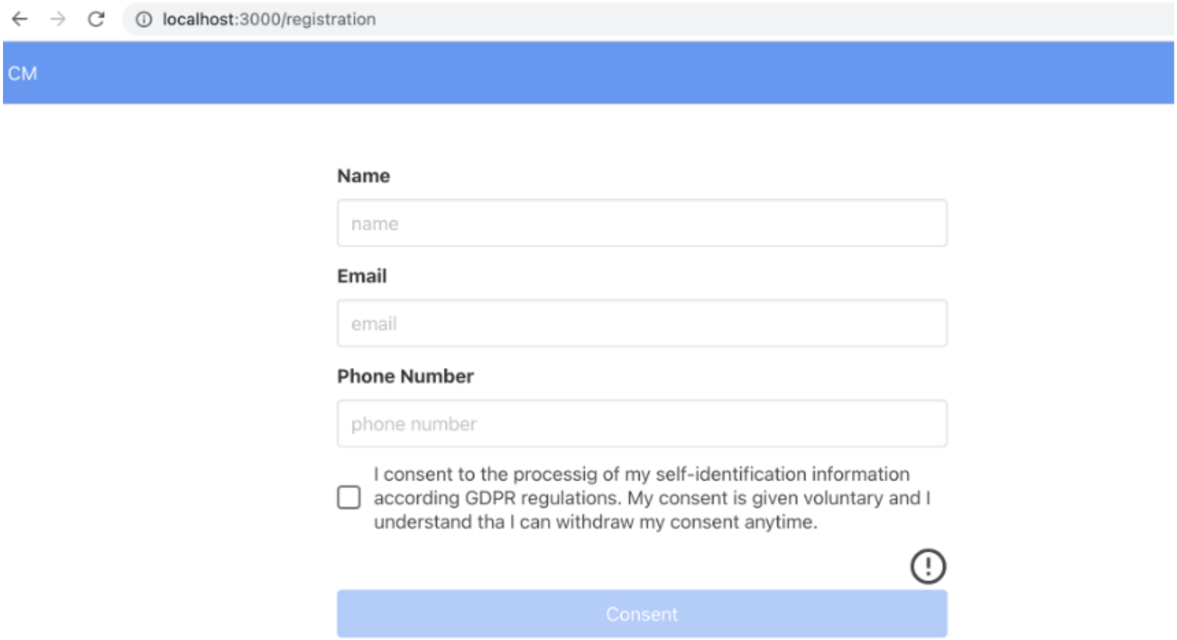
□ Account 1 (0x07e...75a2) 0 ETH

☑ Owner (0x638...2203) 999.94748612 ETH

Only connect with sites you trust. Learn more

Figure 21 – Connecting Crypto Wallet

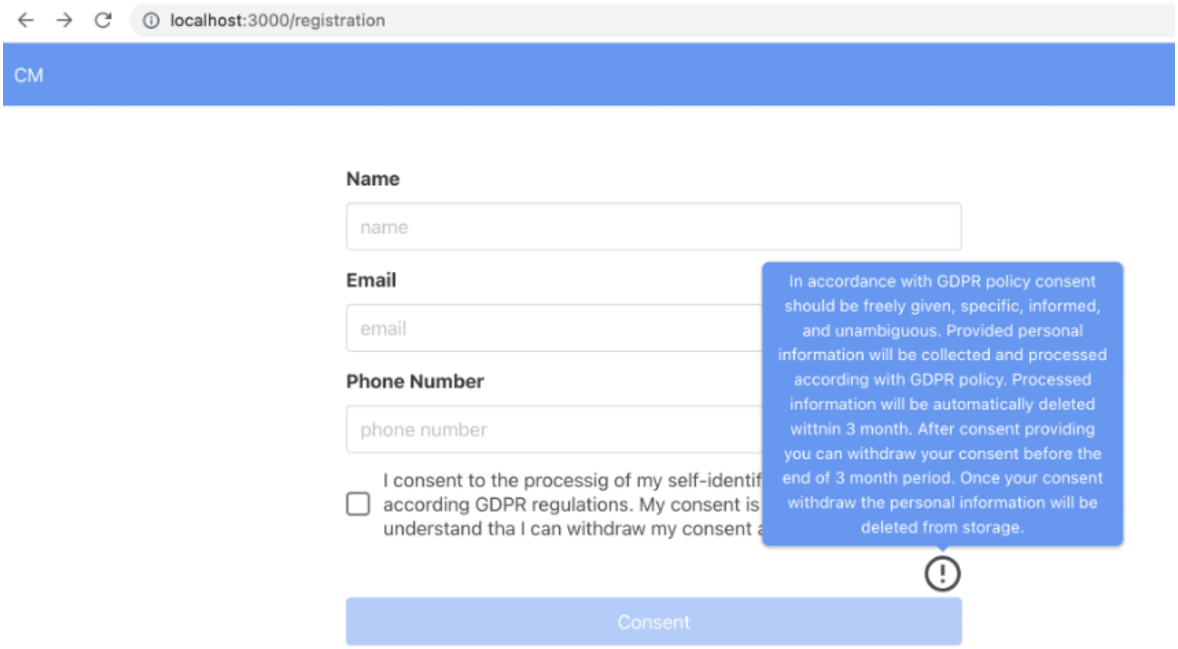
Fields Name, Email, Phone number which are presented in Figure 22 are obligatory to fill. The name field requires information about user’s name. The email field should contain relevant user email along with Phone number information. A checkbox for consent is described next to it and connects with the blockchain.



□ I consent to the processig of my self-identification information according GDPR regulations. My consent is given voluntary and I understand tha I can withdraw my consent anytime.

Figure 22 – Registration

In order to inform users of their rights to process their consent as withdrawal or display information about the consent policy. Figure 23 shows a system tooltip that provides users with an explanation under which regulation, and with which rules their consent would be processed and stored.



localhost:3000/registration

CM

Name

name

Email

email

Phone Number

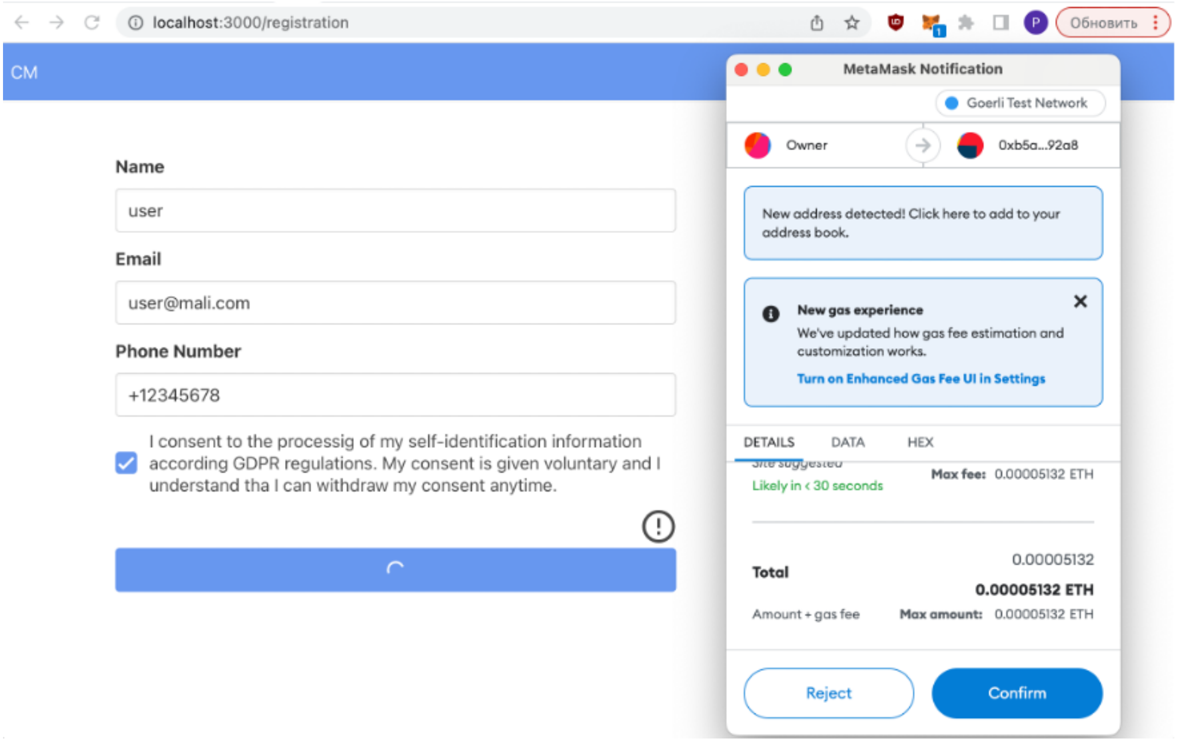
phone number

□ I consent to the processig of my self-identif
according GDPR regulations. My consent is
understand tha I can withdraw my consent a

In accordance with GDPR policy consent should be freely given, specific, informed, and unambiguous. Provided personal information will be collected and processed according with GDPR policy. Processed information will be automatically deleted wittnin 3 month. After consent providing you can withdraw your consent before the end of 3 month period. Once your consent withdraw the personal information will be deleted from storage.

Figure 23 – System consent policy information

After filling all registration fields user consent should be confirmed with the crypto wallet. In Figure 24 a window for confirmation in the crypto wallet is presented.



localhost:3000/registration

CM

Name

user

Email

user@mali.com

Phone Number

+12345678

☑ I consent to the processig of my self-identification information according GDPR regulations. My consent is given voluntary and I understand tha I can withdraw my consent anytime.

MetaMask Notification

Goerli Test Network

Owner → 0xb5a...92a8

New address detected! Click here to add to your address book.

New gas experience

We've updated how gas fee estimation and customization works.

Turn on Enhanced Gas Fee UI in Settings

Site suggested

Likely in < 30 seconds

Max fee: 0.00005132 ETH

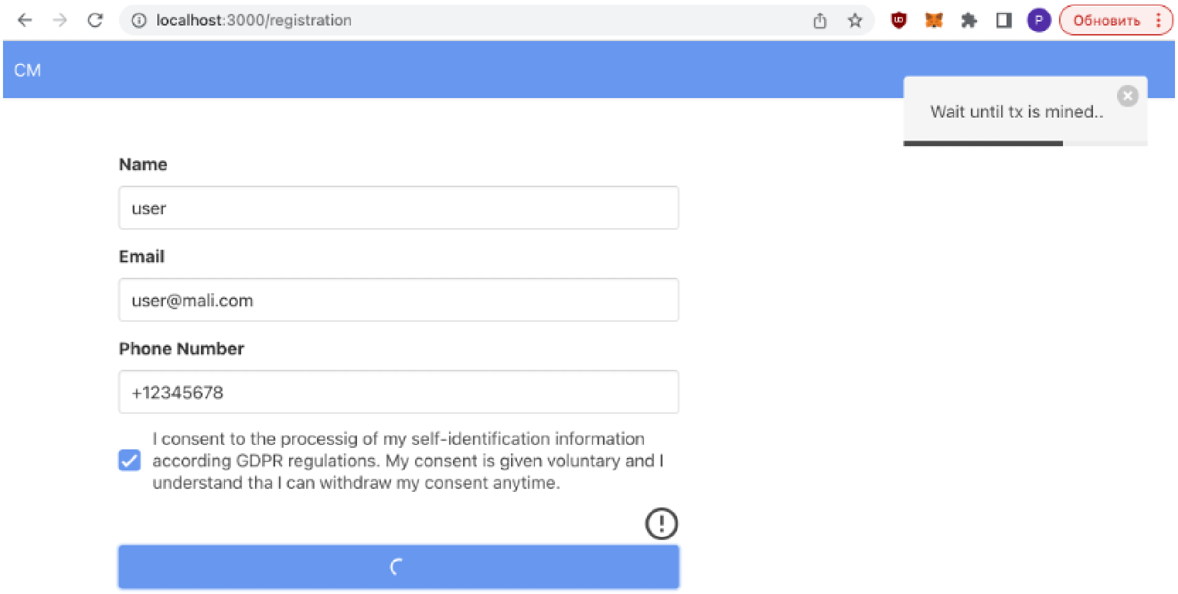
Total 0.00005132

0.00005132 ETH

Amount + gas fee Max amount: 0.00005132 ETH

Figure 24 – Confirm Consent

System shows a notification to the user to inform of ongoing processes as shown in Figures 25 and 26.



Wait until tx is mined..

Name

user

Email

user@mali.com

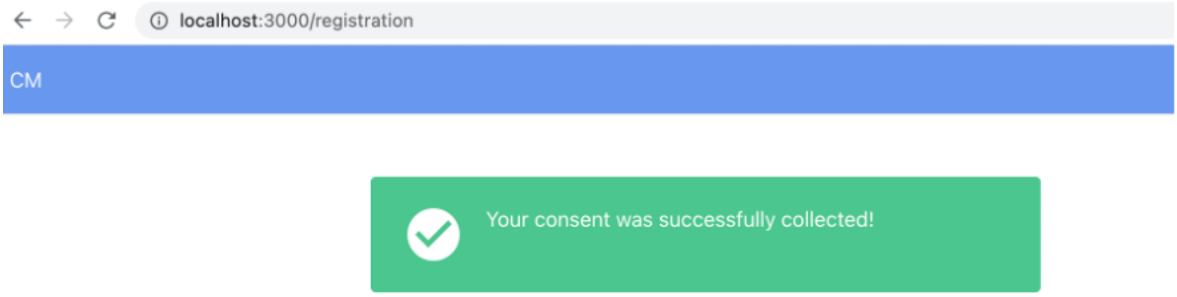
Phone Number

+12345678

☑ I consent to the processig of my self-identification information according GDPR regulations. My consent is given voluntary and I understand tha I can withdraw my consent anytime.

Figure 25 – Waiting notification

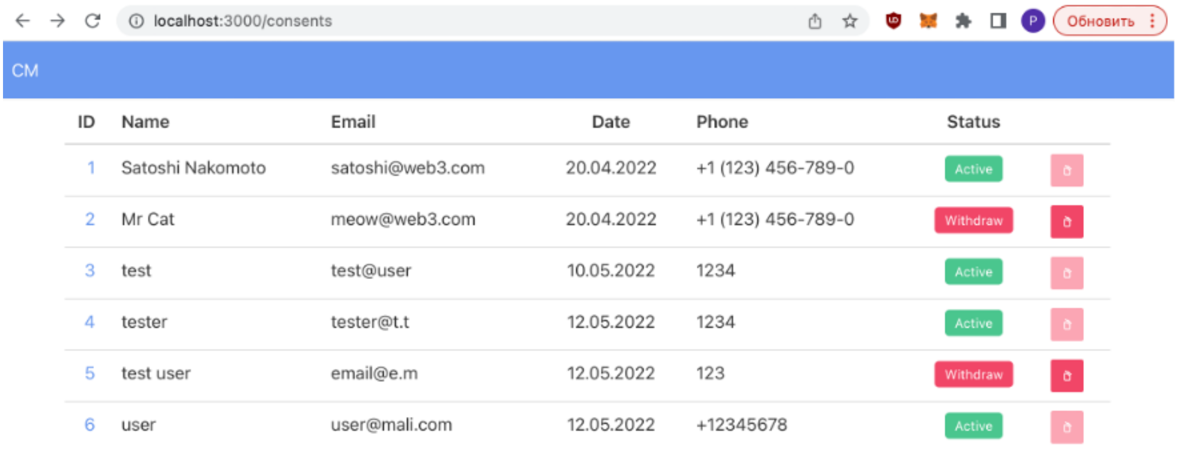
After filling out the Registration form all information sends to the system administrator and user profile and the user can see a notification about successful registration as shown in the picture below.



Your consent was successfully collected!

Figure 26 – Registration notification

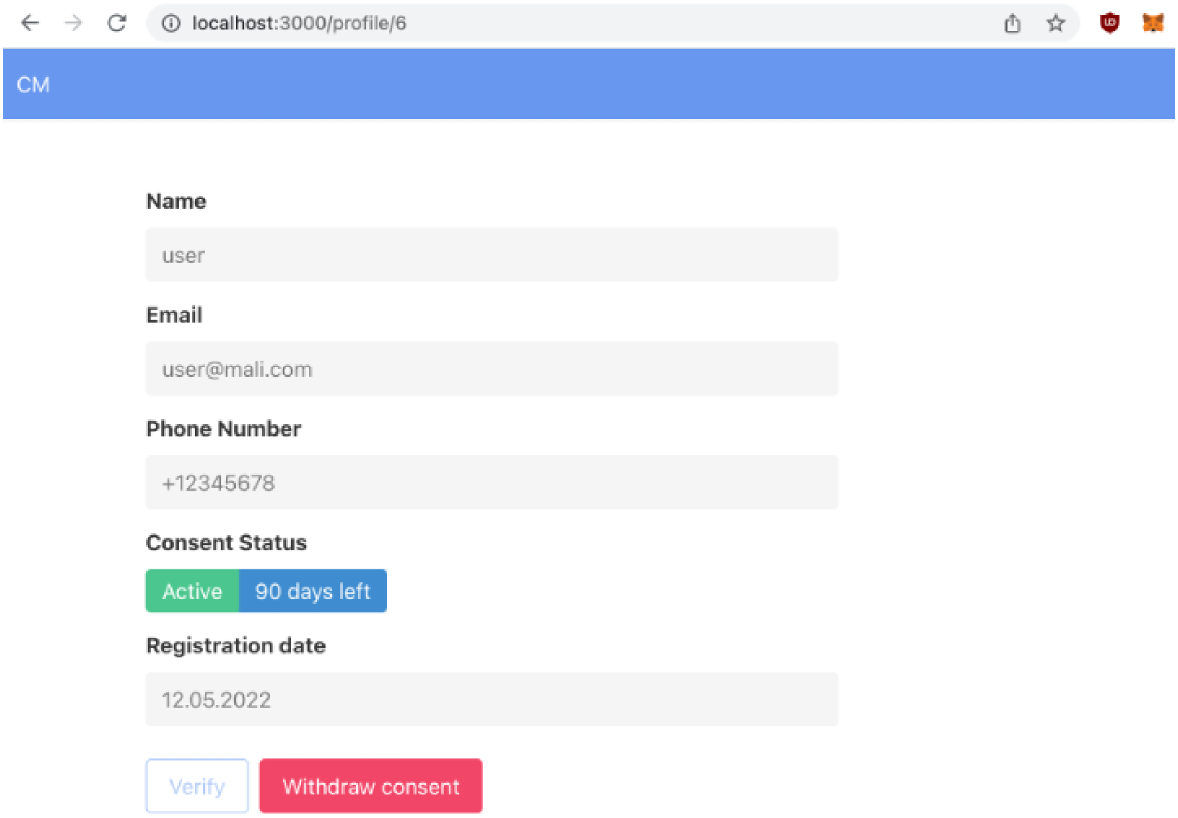
All user information displays on the Administrator screen and includes consent status (Active or Withdraw) which is presented in Figure 27. Administrators can check users' profiles and Withdraw user information with the following removal.



ID	Name	Email	Date	Phone	Status	
1	Satoshi Nakomoto	satoshi@web3.com	20.04.2022	+1 (123) 456-789-0	Active	🗑
2	Mr Cat	meow@web3.com	20.04.2022	+1 (123) 456-789-0	Withdraw	🗑
3	test	test@user	10.05.2022	1234	Active	🗑
4	tester	tester@t.t	12.05.2022	1234	Active	🗑
5	test user	email@e.m	12.05.2022	123	Withdraw	🗑
6	user	user@mali.com	12.05.2022	+12345678	Active	🗑

Figure 27 – Administrator

All information which was provided by the user is displayed on their profile. Figure 28 displays all sections of the user profile. Users can see their consent status, date of registration, and how many days are left for consent storage. Users can check their information or withdraw their consent.



Name

user

Email

user@mali.com

Phone Number

+12345678

Consent Status

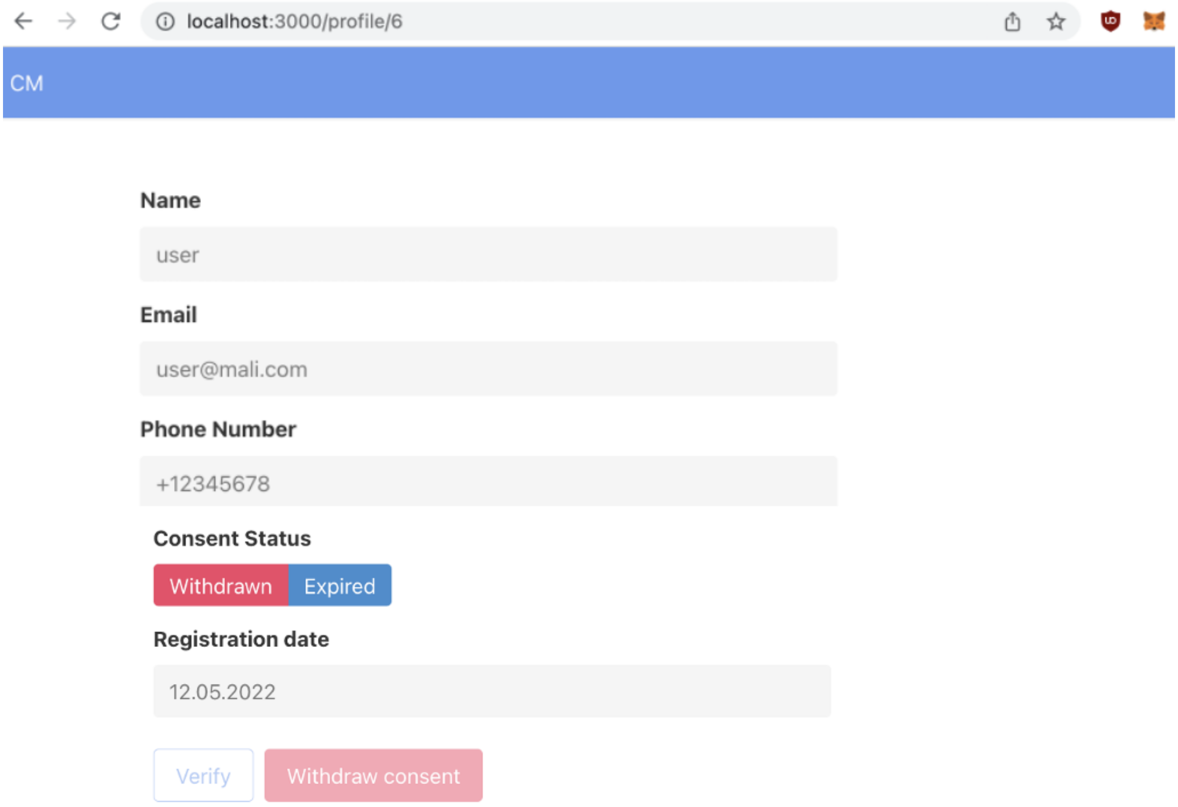
Active 90 days left

Registration date

12.05.2022

Figure 28 – User profile

User can send the request to the administrator to delete personal information after withdrawing consent. Figure 29 shows the user profile after the user clicks to withdraw consent.



Name: user

Email: user@mali.com

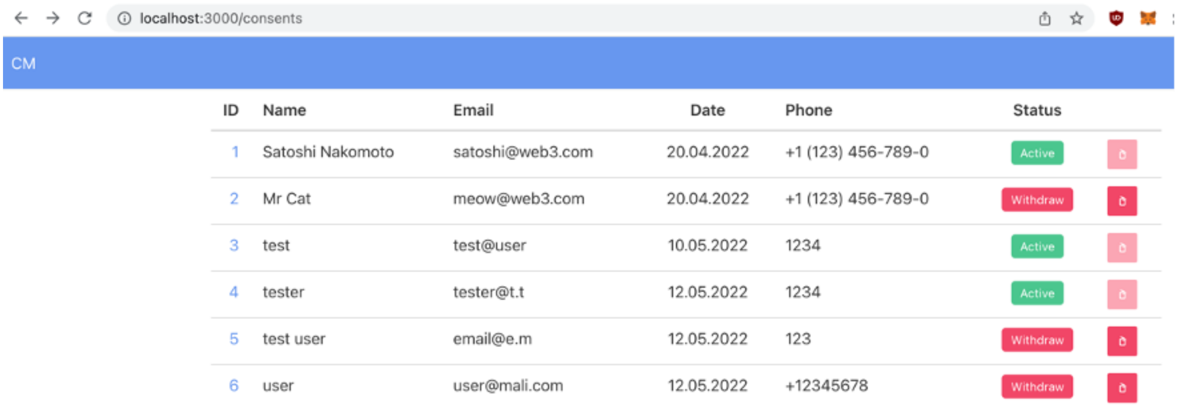
Phone Number: +12345678

Consent Status: Withdrawn Expired

Registration date: 12.05.2022

Figure 29 – Withdrawn consent

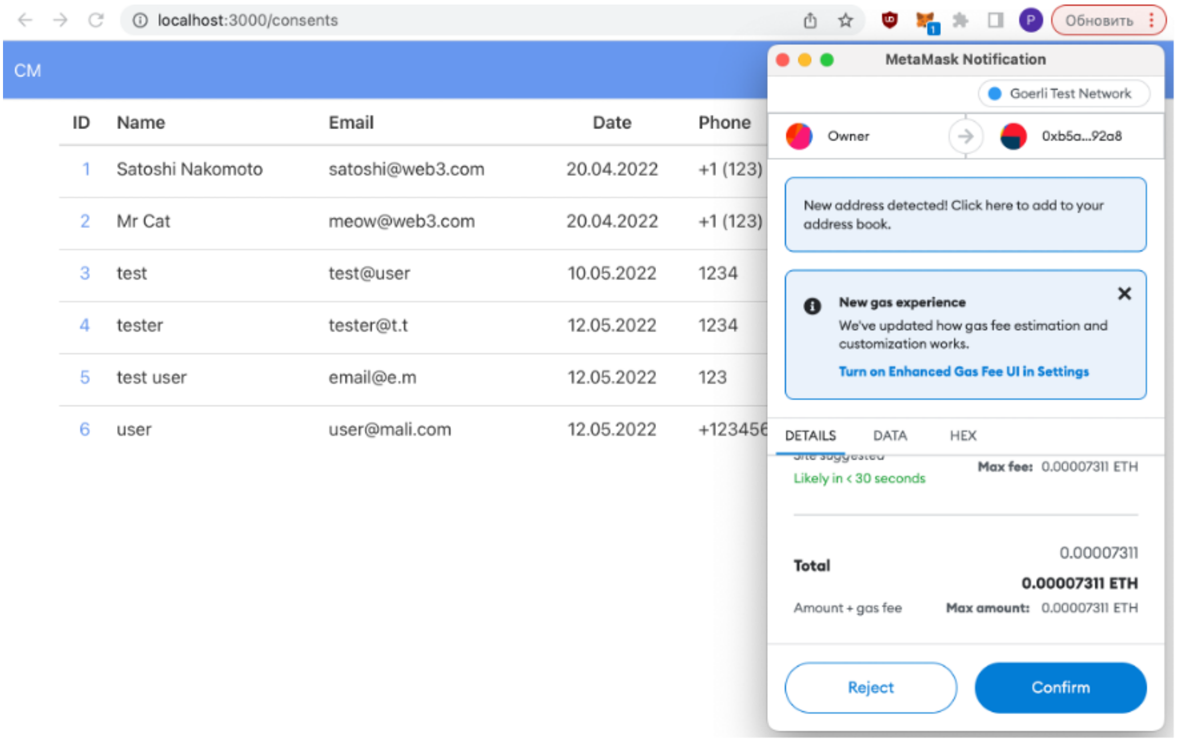
In administrator profile request for withdrawing performed as red Withdraw button as it indicated for users with id number 2, 5, 6 on Figure 30. After consent status changes from active to withdrawn, the delete function is activated.



ID	Name	Email	Date	Phone	Status	
1	Satoshi Nakomoto	satoshi@web3.com	20.04.2022	+1 (123) 456-789-0	Active	🗑
2	Mr Cat	meow@web3.com	20.04.2022	+1 (123) 456-789-0	Withdraw	🗑
3	test	test@user	10.05.2022	1234	Active	🗑
4	tester	tester@t.t	12.05.2022	1234	Active	🗑
5	test user	email@e.m	12.05.2022	123	Withdraw	🗑
6	user	user@mali.com	12.05.2022	+12345678	Withdraw	🗑

Figure 30 – Request for Withdrawn

To delete user profile administrator should be confirmed delete action with crypto wallet. Confirmation window of deleting the user profile is presented on Figure 31.



ID	Name	Email	Date	Phone
1	Satoshi Nakomoto	satoshi@web3.com	20.04.2022	+1 (123)
2	Mr Cat	meow@web3.com	20.04.2022	+1 (123)
3	test	test@user	10.05.2022	1234
4	tester	tester@t.t	12.05.2022	1234
5	test user	email@e.m	12.05.2022	123
6	user	user@mali.com	12.05.2022	+123456

MetaMask Notification

Goerli Test Network

Owner → 0xb5a...92a8

New address detected! Click here to add to your address book.

New gas experience

We've updated how gas fee estimation and customization works.

Turn on Enhanced Gas Fee UI in Settings

Site suggested

Likely in < 30 seconds

Max fee: 0.00007311 ETH

Total 0.00007311

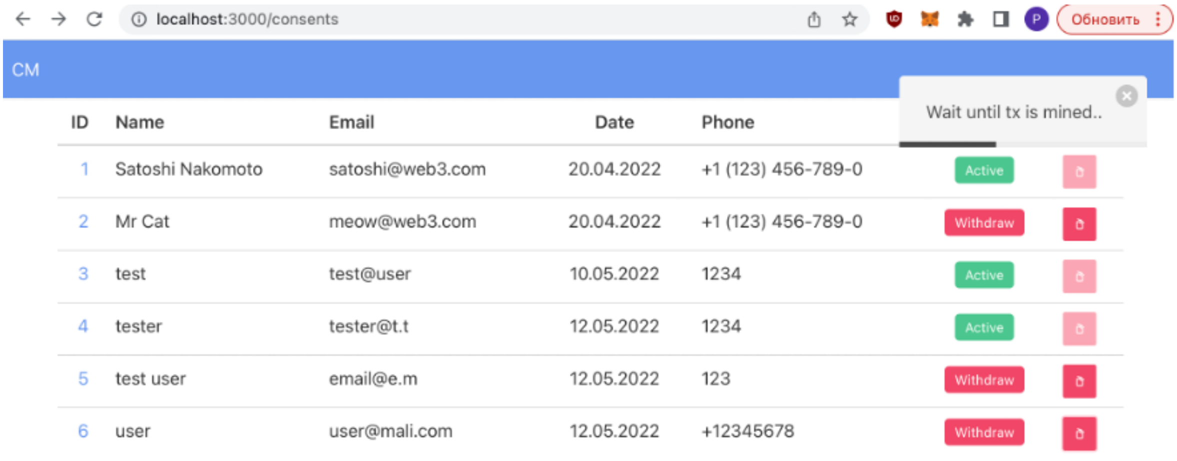
0.00007311 ETH

Amount + gas fee

Max amount: 0.00007311 ETH

Figure 31 – Delete confirmation

Process of deleting user information might take time and in order to inform the user about the process status Waiting notification is shown in Figure 32.

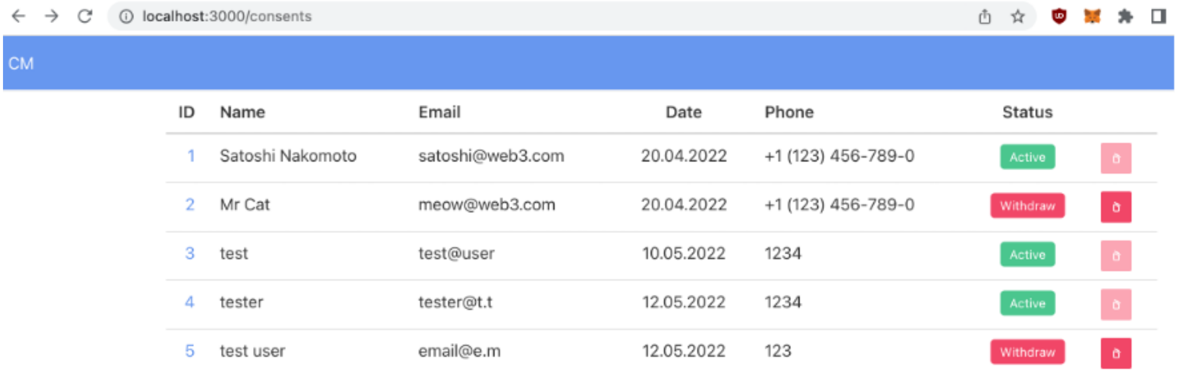


Wait until tx is mined..

ID	Name	Email	Date	Phone		
1	Satoshi Nakomoto	satoshi@web3.com	20.04.2022	+1 (123) 456-789-0	Active	
2	Mr Cat	meow@web3.com	20.04.2022	+1 (123) 456-789-0	Withdraw	
3	test	test@user	10.05.2022	1234	Active	
4	tester	tester@t.t	12.05.2022	1234	Active	
5	test user	email@e.m	12.05.2022	123	Withdraw	
6	user	user@mali.com	12.05.2022	+12345678	Withdraw	

Figure 32 – Waiting notification

Administrator should delete user after request for consent is withdrawn. After user was deleted, information is removed from the database. As it presented in Figure 33 user with id number 6 was deleted.



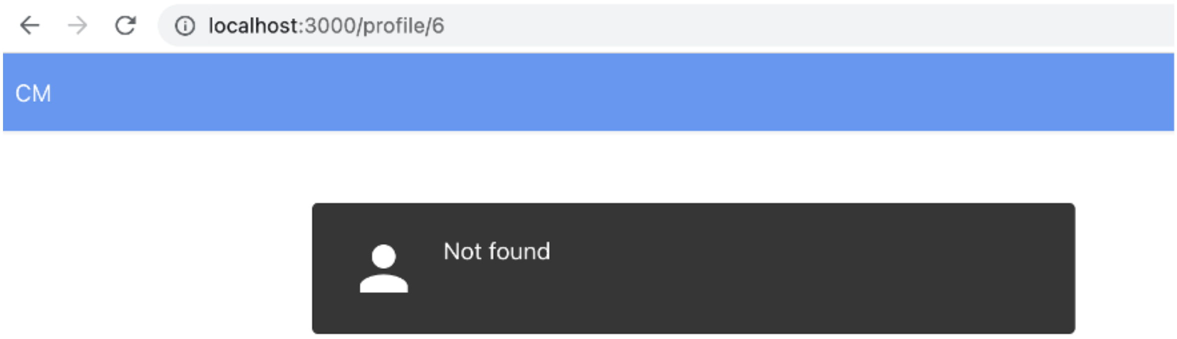
localhost:3000/consents

CM

ID	Name	Email	Date	Phone	Status
1	Satoshi Nakomoto	satoshi@web3.com	20.04.2022	+1 (123) 456-789-0	Active
2	Mr Cat	meow@web3.com	20.04.2022	+1 (123) 456-789-0	Withdraw
3	test	test@user	10.05.2022	1234	Active
4	tester	tester@t.t	12.05.2022	1234	Active
5	test user	email@e.m	12.05.2022	123	Withdraw

Figure 33 – User 6 was deleted

Once the administrator deleted user data, the user profile is also removed. Figure 34 shows updated information about user profiles.



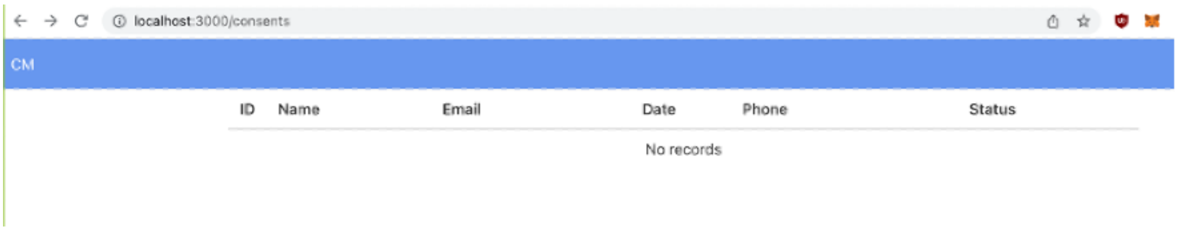
localhost:3000/profile/6

CM

Not found

Figure 34 – Deleted User

Figure 35 shows the case if there is no user registered or no active consent user database is empty.



localhost:3000/consents

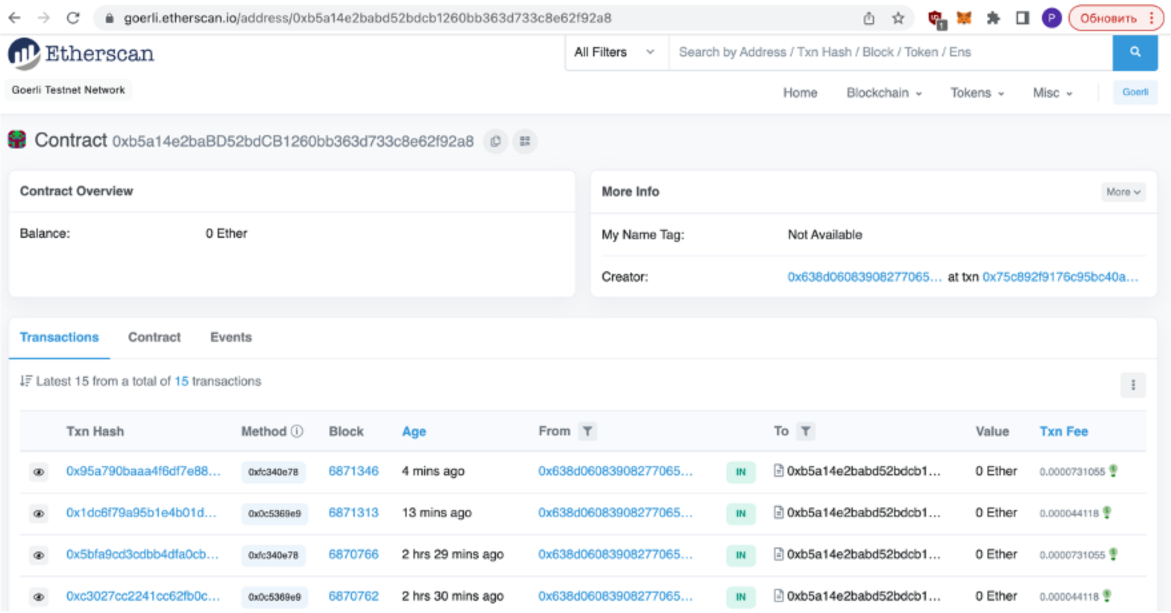
CM

ID	Name	Email	Date	Phone	Status

No records

Figure 35 – Empty Database

All transaction history is easy to check on Etherscan by contract hash. On Figure 36 the value “0xb5a14e2baBD52bdCB1260bb363d733c8e62f92a8” is hash of consent management contract. Therefore, all transactions such as signing the contract by user or deleting user information by the administrator are recorded.



goerli.etherscan.io/address/0xb5a14e2babd52bdcb1260bb363d733c8e62f92a8

Contract 0xb5a14e2baBD52bdCB1260bb363d733c8e62f92a8

Contract Overview

Balance: 0 Ether

More Info

My Name Tag: Not Available

Creator: 0x638d06083908277065… at txn 0x75c892f9176c95bc40a…

Latest 15 from a total of 15 transactions

Txn Hash	Method	Block	Age	From		To	Value	Txn Fee
0x95a790baaa4f6df7e88…	0xfc340e78	6871346	4 mins ago	0x638d06083908277065…	IN	0xb5a14e2babd52bdcb1…	0 Ether	0.0000731055
0x1dc6f79a95b1e4b01d…	0x0c5369e9	6871313	13 mins ago	0x638d06083908277065…	IN	0xb5a14e2babd52bdcb1…	0 Ether	0.000044118
0x5bfa9cd3cdbb4dfa0cb…	0xfc340e78	6870766	2 hrs 29 mins ago	0x638d06083908277065…	IN	0xb5a14e2babd52bdcb1…	0 Ether	0.0000731055
0xc3027cc2241cc62fb0c…	0x0c5369e9	6870762	2 hrs 30 mins ago	0x638d06083908277065…	IN	0xb5a14e2babd52bdcb1…	0 Ether	0.000044118

Figure 36 – Transaction history

5 Conclusions

The proposed system is analyzed according to the scope of the thesis. Among the reviewed materials, no system that would be suitable for a broad, general area of application was identified. As part of the development of the system, the requirements for the system were summarized. Based on the summarized requirements, the architecture of the proposed system was designed. The architecture contains smart contracts to interface with blockchain technology. This part of the architecture allows user consent to be stored securely and to track the consent history - whether it has been deleted after the storage period has expired.

Furthermore, the thesis outlines that a prototype of the General Blockchain-based Consent Management System is probable and can be used, which proves the idea of developing consent management systems as per GDPR and blockchain technology applications.

5.1 Contribution

The proposed system allows the following functions for consent management: collecting and saving user consent and withdrawing user consent. By interacting with the user interface, the data subject provides personal data and consent for the data collection and processing. Once the user consent is collected, its record is made in the Ethereum blockchain. Users have their own profile to check the current consent status and to withdraw the given consent by their wish. The process of withdrawing consent can be performed by users themselves. Upon user consent, the system administrator deletes the personal data. Otherwise, if the consent is just stored in the system after 90 days, the consent would be automatically withdrawn. All user data would be deleted by the system administrator who performs the data processing functions. Besides, all the records of the users personal data removal are recorded in the blockchain.

As the GDPR regulates the process of data collection and processing, it assures users of the legality of data collection and storage. All processing stages are stated and seen to the user before consent collection, allowing users to be aware of the whole process and their rights. The authorities benefit as there is a general law for the data processing. Unified regulation of data collection and processing provides the same competitiveness among all institutions requiring personal data collection.

5.2 Limitations

Major limitations of this study includes scalability, lack of a comprehensive framework and time limitation. The proposed system is helpful for a small-scale system. The system is tested in a local environment as well. Before implementing in the real world, the system needs to be developed and tested in a large-scale global environment. In addition, as mentioned in the background section, it is very tough to design a standardized consent management framework because it is different in various application domains. However, longitudinal research can reveal useful insights regarding a more standardized framework. Furthermore, the system will also have to be tested by domain experts and companies.

5.3 Future Research Agenda

Further system development involves seeking investors and development team expansion. That allows the creation of a plan for further integration with websites of systems that should provide a consent collection under the GDPR. Further development involves improving the user experience and extending the administrator's functions. Additionally, it is crucial to study the legal basis for data transferring to third parties. To achieve that, it is necessary to establish the rules, the algorithm of data transfer, and data deletion after consent expires. With the increasing a number of user system should be scalable to perform smoothly for new users.

References

R. Faden, T. Beaucham, N. King, 1986, A history and theory of informed consent. New York: Oxford University Press. pp. 53-55

GDPR document Personal data. [website]. [sited 28.02.2022]. Available: https://gdpr-info.eu/issues/consent/

Cambridge dictionary [website]. [sited 01.03.2022]. Available: https://dictionary.cambridge.org/us/dictionary/english/consent

GDPR document, Article 4 [website]. [sited 01.03.2022]. Available: https://gdpr-info.eu/art-4-gdpr/

GDPR document, Article7 [website]. [sited 01.03.2022]. Available: https://gdpr-info.eu/art-7-gdpr/

J.Miller, 2019, Moving towards Industry 4.0: The Internet of Things and Cyber Technology [electronic journal]. [sited 02.03.2022]. Available: http://www.worximity.com/en/blog/moving-towards-industry-4-iiot-and-cyber-technology

S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in internet of things: the road ahead,” Computer Networks, vol. 76, pp. 146–164, 2015.

P. Voigt, V. Bussche, 2017 The Eu General Data Protection Regulation (GDPR): A Practical Guide, 1st ed.; Springer International Publishing: Cham, Switzerland.

IBM, 2021, Overview of Consent Management, [website]. [sited 01.03.2022]. Available: https://www.ibm.com/support/knowledgecenter/SSWSR9_11.6.0/com.ibm.mdmhs.overview.doc/consentmanagementoverview.html

Gartner, Consent Management. [website]. [sited 01.03.2022]. Available: https://www.gartner.com/en/information-technology/glossary/consent-management

V. Kakarlapudi, H. Mahmoud, 2021, A Systematic Review of Blockchain for Consent Management [electronic journal]. [sited 02.03.2022]. Available: https://www.researchgate.net/publication/348941302_A_Systematic_Review_of_Blockchain_for_Consent_Management

GDPR document Article 5 [website]. [sited 07.03.2022]. Available: https://gdpr-info.eu/art-5-gdpr/

K. Sultan, U. Ruhi, R. Lakhani, 2018, Conceptualizing Blockchains: characteristics & applications, [electronic journal]. [sited 17.03.2022]. Available: https://arxiv.org/pdf/1806.03693.pdf

W. Viriyasitavat, D. Hoonsopon, 2017, Blockchain characteristics and consensus in modern business processes, [electronic journal]. [sited 20.03.2022]. Available: https://www.sciencedirect.com/science/article/abs/pii/S2452414X18300815

S. Ferdous, M. Chowdhury, A. Hoque, A. Colman, 2020, Blockchain Consensus Algorithms: A Survey, [electronic journal]. [sited 20.03.2022]. Available: https://arxiv.org/abs/2001.07091

T. Nguyen, K. Kim, 2018 A survey about consensus algorithms used in Blockchain, [electronic journal]. [sited 20.03.2022]. Available: https://www.researchgate.net/publication/323704818_A_survey_about_consensus_algorithms_used_in_Blockchain

Merkle Trees and Merkle Roots Help Make Blockchains Possible, 2021. [website]. [sited 20.03.2022]. Available: https://www.gemini.com/cryptopedia/merkle-tree-blockchain-merkle-root

Merkle Tree in Blockchain: What is it, How does it work and Benefits, 2021, [website]. [sited 20.03.2022] Available: https://arxiv.org/pdf/1908.01738.pdf

A. Prashanth Joshi, M. Han, Y. Wang, 2018, A SURVEY ON SECURITY AND PRIVACY ISSUES OF BLOCKCHAIN TECHNOLOGY, [electronic journal]. [sited 20.03.2022]. Available: https://www.researchgate.net/publication/325173502_A_survey_on_security_and_privacy_issues_of_blockchain_technology

G. Nguyen, K. Kim A Survey about Consensus Algorithms Used in Blockchain, 2018, pp 37-42

R. Wattenhofer, The Science of the Blockchain, 2016, pp. 23–24

J. Garay, A. Kiayias, N. Leonardos, 2015, The Bitcoin Backbone Protocol: Analysis and Applications, [electronic journal]. [sited 01.04.2022]. Available: https://link.springer.com/chapter/10.1007/978-3-662-46803-6_10

T. Swanson, 2015, Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems, [electronic journal]. [sited 01.04.2022]. Available: http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf

M. Castro, 2001, Practical Byzantine Fault Tolerance, [electronic journal]. [sited 01.04.2022]. Available: https://www.researchgate.net/publication/2516268_Practical_Byzantine_Fault_Tolerance

Byzantine Fault Tolerance Explained. [website]. [sited 13.04.2022]. Available: https://academy.binance.com/en/articles/byzantine-fault-tolerance-explained

S. Medvedeva, D.Malovanyi, 2019, BASIC PRINCIPLES OF THE BLOCKCHAIN THECHNOLOGY AND ITS APPLICATION. [electronic journal]. [sited 11.04.2022]. Available: https://core.ac.uk/download/199457858.pdf

C. Berger, H. Reiser, 2018, Scaling Byzantine Consensus: A Broad Analysis, [electronic journal]. [sited 05.04.2022]. Available: https://d-nb.info/1199607843/34

J. Garay, A. Kiayias, N. Leonardos, 2015, Design and Implementation of a Blockchain-based Consent Management System, [electronic journal]. [sited 01.04.2022]. Available: https://link.springer.com/chapter/10.1007/978-3-662-46803-6_10

S. Nakamoto, 2008, Bitcoin: A peer-to-peer electronic cash system, [electronic journal]. [sited 01.04.2022]. Available: https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf

E. Kathleen, E. Wegrzyn, 2021, Types of Blockchain: Public, Private, or Something in Between, [electronic journal]. [sited 21.04.2022]. Available: https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between

B. Haque, B. Naqvi, N. Islam, S. Hyrynsalmi, 2021, Towards a GDPR-Compliant Blockchain-Based COVID Vaccination Passport [electronic journal]. [sited 28.02.2022]

T. Tuan, A. Ji, W. Chen, R. Beng, C. Ooi, K. Tan, 2017, BLOCKBENCH: A Framework for Analyzing Private Blockchains, [electronic journal]. [sited 27.02.2022]. Available: https://arxiv.org/pdf/1703.04057.pdf

W. Yao, J. Ye, R. Murimi, G. Wang, 2021, A Survey on Consortium Blockchain Consensus Mechanisms, [electronic journal]. [sited 27.02.2022]. Available: https://arxiv.org/pdf/2102.12058.pdf

A. Ustundag, E. Cevikcan, 2018, Maturity and Readiness Model for Industry 4.0., [electronic journal]. [sited 28.02.2022]. Available: https://www.researchgate.net/publication/319862859_Maturity_and_Readiness_Model_for_Industry_40_Strategy

M. Hussain, A. Shafie, A. Latiff, M. Madni, 2019, Concept of Blockchain Technology, [electronic journal]. [sited 01.04.2022]. Available: https://www.researchgate.net/publication/337904696_Concept_of_Blockchain_Technology (sited 25.02.2022)

G. Albanese, J. Calbimonte, M. Schumacher, D. Calvaresi, 2021, Dynamic consent management for clinical trials via private blockchain technology [electronic journal]. [sited 28.02.2022]

D. Peras, 2016, Guidelines for GDPR Compliant Consent and Data Management Model in ICT Businesses [electronic journal]. [sited 28.02.2022]. Available: https://www.bib.irb.hr/980604/download/980604.ETICT-3.pdf

S. Daoudagh, E. Marchetti, V. Savarino, R. Di Bernardo, 2021, How to Improve the GDPR Compliance through Consent Management and Access Control. [electronic journal]. [sited 28.02.2022]. Available: https://www.scitepress.org/Papers/2021/102602/102602.pdf

K. Rantos, G. Drosatos , A. Kritsas , C. Ilioudis , Al. Papanikolaou, A. Filippidis, 2019, A Blockchain-Based Platform for Consent Management of Personal Data Processing in the IoT Ecosystem [electronic journal]. [sited 28.02.2022]. Available: https://www.researchgate.net/publication/336649345_A_Blockchain-Based_Platform_for_Consent_Management_of_Personal_Data_Processing_in_the_IoT_Ecosystem

M. Merlec, Y. Lee, S. Hong, H. In, 2021, A Smart Contract-Based Dynamic Consent Management System for Personal Data Usage under GDPR [electronic journal]. [sited 25.03.2022]. Available: https://www.mdpi.com/1424-8220/21/23/7994

V. Jaiman, V. Urovi, 2020, A Consent Model for Blockchain-Based Health Data Sharing Platforms, [electronic journal]. [sited 25.03.2022]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9159120

A. Lakhan, M. Mohammed, A. Rashid, S. Kadry, T. Panityakul, K. Abdulkareem, O. Thinnukool, 2021, Smart-Contract Aware Ethereum and Client-Fog-Cloud Healthcare System, [electronic journal]. [sited 25.02.2022]. Available: https://www.mdpi.com/1424-8220/21/12/4093

GDPR document, What is GDPR, the EU’s data protection law? [website]. [sited 25.02.2022]. Available: https://gdpr.eu/what-is-gdpr/

N. Ramirez, 2022, The ultimate guide to personal data [electronic journal]. [sited 25.03.2022]. Available: https://www.osano.com/articles/the-ultimate-guide-to-personal-data

H. Platner, 2010, An Introduction to design thinking [electronic journal]. [sited 25.04.2022]. Available: https://web.stanford.edu/~mshanks/MichaelShanks/files/509554.pdf

A. Bureau, 2022, Idea Generation – Techniques, Tools, Examples, Sources And Activities, [electronic journal]. [sited 02.04.2022]. Available: https://alcorfund.com/insight/idea-generation-2/

GDPR document Article 6 [website]. [sited 28.03.2022]. Available: https://gdpr-info.eu/art-6-gdpr/

GDPR document Article 7 [website]. [sited 28.03.2022]. Available: https://gdpr-info.eu/art-7-gdpr/

GDPR document Article 8 [website]. [sited 28.03.2022]. Available: https://gdpr-info.eu/art-8-gdpr/

GDPR document Article 9 [website]. [sited 28.03.2022]. Available: https://gdpr-info.eu/art-9-gdpr/

GDPR document Article 22 [website]. [sited 28.03.2022]. Available: https://gdpr-info.eu/art-22-gdpr/

GDPR document Article 39 [website]. [sited 28.03.2022]. Available: https://gdpr-info.eu/art-39-gdpr/

GDPR document Article 49 [website]. [sited 28.03.2022]. Available: https://gdpr-info.eu/art-49-gdpr/

CodeAcademy official website. [website]. [sited 28.04.2022]. Available: https://www.codecademy.com/learn/introduction-to-javascript

Official Vue website. [website]. [sited 10.04.2022]. Available: https://vuejs.org

MetaMask official website. [website]. [sited 10.04.2022]. Available: https://metamask.io

Solidity official website. [website]. [sited 01.05.2022]. Available: https://docs.soliditylang.org/en/v0.8.13/

Remix official website. [website]. [sited 01.05.2022]. Available: https://remix-ide.readthedocs.io/en/latest/

Coursera, What Is Python Used For? A Beginner's Guide, 2022. [website]. [sited 01.05.2022]. Available: https://www.coursera.org/articles/what-is-python-used-for-a-beginners-guide-to-using-python

FastApi official website. [website]. [sited 02.05.2022]. Available: https://fastapi.tiangolo.com

PostgeSQL official website. [website]. [sited 01.05.2022]. Available: https://www.postgresql.org

Ethereum documentation. Gas and Fees, 2022. [website]. [sited 28.04.2022]. Available: https://ethereum.org/en/developers/docs/gas/

Appendix 1. Tables

Table 8 Requirements of existing Consent Management Applications (B. Haque, 2021), (G. Albanese, 2021), (D. Peras, 2016), (S. Daoudagh, 2021), (K. Rantos, 2019), (M. Merlec, 2021)

Author and article	Requirements	System features	Source of requirements
Towards a GDPR-Compliant Blockchain-Based COVID Vaccination Passport *B. Haque, Bilal Naqvi , A. K. M. Najmul Islam and Sami Hyrynsalmi*	1. Monitoring of data base access. 2. Smart contracts are used for data subject consent collection. 3. Data on blockchain should be modified or delete once there is such a request. 4. All data controllers and processors must be aurhorized. .	Main system management functions: ● Create, ● Read, ● Update, ● Delete	GDPR based on article: **Realizing Edge Marketplaces: Challenges and Opportunities** *Blesson Varghese; Massimo Villari; Omer Rana; Philip James; Tejal Shah; Maria Fazio; Rajiv Ranjan*
Dynamic consent management for clinical trials via private blockchain technology *Giuseppe Albanese1 · Jean-Paul Calbimonte1*	1. To improve the current CTs consent management. 2. To ensure patient confidentiality in data-transfer between medical platforms 3. All patient's data and consent should be authorised. 4. To ensure confidentiality and transparency in management of data and patient consent	Main system management functions: ● Authentication ● Access management ● Transactions validation	Article: **Blockchain applications in the biomedical domain: a scoping review. Comput Struct Biotechnol J** Drosatos G, Kaldoudi E (2019)

Author and article	Requirements	System features	Source of requirements
· *Michael Schumacher1* · *Davide Calvaresi*			(study about the application of BCT in the biomedical domain.) Studied projects: ● REDCap (free cross-platform electronic data capture (EDC)3 system for designing clinical and translational research databases) ● OpenClinica (open-source clinical data management system) ● Phoenix CTMS (a custom Java web application)
How to Improve the GDPR Compliance through Consent Management and Access Control *Said Daoudagh, Eda Marchetti1 b, Vincenzo Savarino3 c, Roberto Di Bernardo*	1. Purposes, i.e., to process data only under agreed purposes. 2. Accuracy, i.e., to update regularly. 3. Retention, i.e., processed data should be stored for fixed time period. 4. Subject explicit consent, i.e., only consent ensures data processing.	Main system management functions: ● Consent Manager. To present structured consent. ● Access Control Manager. To ensure ompliance with the policies set by the manager	The General Data Protec tion Regulation (GDPR) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union, L119:1–88.
Guidelines for GDPR Compliant Consent and Data	1. To collect informed and unambiguous consent, 2. To get an oral or written consent confirmation,	Main system management functions: a) User Interface	The General Data Protection Regulation (GDPR)

Author and article	Requirements	System features	Source of requirements
Management Model in ICT Businesses *Dijana Peras*	3. To provide a description for consent use, 4. To inform data subject about consent process and its motive, 5. Consent request should not be destructive, 6. System should provide a choice for the data subject whether to give a consent for data collection or not, 7. Information about users' rights and data processors should be provided, 8. System should allow users to check, modify or delete their personal data, 9. The data controller upon request should provide proves of its ability to process user information.	b) Consent manager c) Data manager	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union, L119:1–88. On the Management of Consent and Revocation in Enterprises: Setting the Context. HP Laboratories, Technical Report HPL-2009-49: 11. Mont, Marco Casassa, Siani Pearson, Gina Kounga, Yun Shen, and Pete Bramhall, (2009). **Discovered models:** A Conceptual Model for Privacy Policies with Consent and Revocation Requirements. In Privacy and Identity Management for Life. Simone Fischer-Hübner, Penny Duquenoy, Marit Hansen, Ronald Leenes, and Ge Zhang, eds. Pp. 258–270. Berlin, Heidelberg: Springer Berlin Heidelberg. http://link.springer.com/10.1007/978-3-642- 20769-3_21, accessed March 21, 2018. Casassa Mont, Marco, Siani Pearson, Sadie Creese, Michael Goldsmith, and Nick Papanikolaou, (2011).

Author and article	Requirements	System features	Source of requirements
			Privacy Constraint Processing in a Privacy-Enhanced Database Management System. Data & Knowledge Engineering 55(2): 159–188. Thuraisingham, Bhavani (2005). Cookies and Web Browser Design: Toward Realizing Informed Consent Online. In Pp. 46–52. ACM Press. http://portal.acm.org/citation.cfm?doid=365024.3 6 5034, accessed March 21, 2018. Millett, Lynette I., Batya Friedman, and Edward Felten (2001). Public Online Services at the Age of MyData: A New Approach to Personal Data Management in Finland: 12. Rissanen, Teemu (2016). Compliance through Informed Consent: Semantic Based Consent Permission and Data Management Model. In 5th Workshop on Society, Privacy and the Semantic Web–Policy and Technology (PrivOn2017), C. Brewster, M. Cheatham, M. d'Aquin, S. Decker and S. Kirrane, Eds, CEUR Workshop Proceedings, Aachen Pp. 1613–0073.

Author and article	Requirements	System features	Source of requirements
			Fatema, Kaniz, Ensar Hadziselimovic, H. J. Pandit, et al. (2017).
A Blockchain-Based Platform for Consent Management of Personal Data Processing in the IoT Ecosystem *Konstantinos Rantos ,1 George Drosatos ,2 Antonios Kritsas ,1 Christos Ilioudis ,3 Alexandros Papanikolaou,3 and Adam P. Filippidis*	1. System should list all the personal data which it would process 2. System should list all data processors which would be process data 3. System should list all personal data which would be collected 4. System should state grounds and time limits of consent storge and personal data storage 5. To allow automatic data processing.		The General Data Protec- tion Regulation (GDPR) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union, L119:1–88. “Security, privacy and trust in internet of things: the road ahead,” Computer Networks, vol. 76, pp. 146–164, 2015. . Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “On the features and challenges of security and privacy in distributed internet of things,” Computer Networks, vol. 57, no. 10, pp. 2266–2279, 2013. R. Roman, J. Zhou, and J. Lopez,

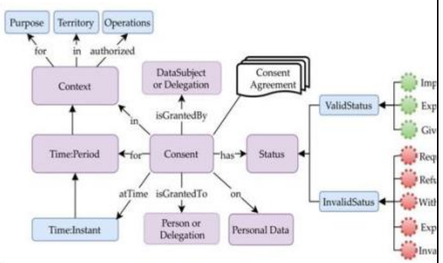
Author and article	Requirements	System features	Source of requirements
A Smart Contract-Based Dynamic Consent Management System for Personal Data Usage under GDPR *Mpyana Mwamba Merlec 1* *, Youn Kyu Lee 2,* , Seng-Phil Hong 3 and Hoh Peter In*	1. Consent should be provided by data subject or their legal representor 2. The data controller should store valid consents 3. The consent should state purposes of data process, should list required data and provide data controller information	 Purpose Territory Operations for in authorized Context DataSubject or Delegation Consent Agreement in isGrantedBy ValidStatus Imp Exp Giv Time:Period for Consent has Status Req Refu With Exp Inva atTime isGrantedTo on InvalidSatus Time:Instant Person or Delegation Personal Data	Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. J. Cybersecur. 2018, Politou, E.; Alepis, E.; Patsakis, C. Pandit, H.J.; Debruyne, C.; O'Sullivan, D.; Lewis, D. GConsent-a Consent Ontology Based on the GDPR. In European Semantic Web Conference; Springer: Cham, Switzerland, 2019.

Table 9 Developed Consent Management Applications (B. Haque, 2021), (G. Albanese, 2021), (D. Peras, 2016), (S. Daoudagh, 2021), (K. Rantos, 2019), (M. Merlec, 2021), (V. Jaiman, 2020), (A. Lakhan, 2021)

Author and article	Objective	What they developed
Towards a GDPR-Compliant Blockchain-Based COVID Vaccination Passport	Vaccination passport would display information about COVID vaccination. Further modifications would allow to add information for other vaccines: polio, tuberculosis, measles, etc. Proposed architecture complies with GDPR and proposes use of blockchain.	*VacciFi– architecture* of framework for a GDPR-compliant blockchain-based COVID vaccination passport

Author and article	Objective	What they developed
B. Haque, Bilal Naqvi , A. K. M. Najmul Islam and Sami Hyrynsalmi		
Dynamic consent management for clinical trials via private blockchain technology *Giuseppe Albanese1 · Jean-Paul Calbimonte1 · Michael Schumacher1 · Davide Calvaresi*	This article presents SCoDES, an approach for trusted and decentralized management of dynamic consent in clinical trials, based on blockchain technology.	*SCoDES* – consent management application for clinical trials and was integrated with REDCap
How to Improve the GDPR Compliance through Consent Management and Access Control *Said Daoudagh, Eda Marchetti1 b, Vincenzo Savarino3 c, Roberto Di Bernardo*	Privacy-by-design solution based on Consent Manager and Access Control to aid organizations to comply with the GDPR	Access Control Manager for consent management
Guidelines for GDPR Compliant Consent and Data Management Model in ICT Businesses	This article proposes guidelines for GDPR complaint consent management and data management.	*Guidelines* for the framework of GDPR compliant Consent and Data Management Model in ICT businesses

Author and article	Objective	What they developed
Dijana Peras		
A Blockchain-Based Platform for Consent Management of Personal Data Processing in the IoT Ecosystem *Konstantinos Rantos ,1 George Drosatos ,2 Antonios Kritsas ,1 Christos Ilioudis ,3 Alexandros Papanikolaou,3 and Adam P. Filippidis*	Researchers developed a platform for consent management which allows personal data control by data subjects. This platform aims to simplify communication between the data controller and the data subject.	*ADVOCATE platform* – personal data manager in Internet of Things ecosystem**.**
A Smart Contract-Based Dynamic Consent Management System for Personal Data Usage under GDPR *Mpyana Mwamba Merlec, Youn Kyu Lee,, Seng-Phil Hong, Hoh Peter In*	Researchers propose a system for smart contract-based consent management system in medicine field. The article proposes design requirements, implementation and rules for consent collection under GDPR regulation.	Smart-contract-based dynamic *consent management system*