Chapter 8
Leveraging Management of Customers' Consent Exploiting the Benefits of Blockchain Technology Towards Secure Data Sharing

Dimitris Miltiadou, Stamatis Pitsios, Spyros Kasdaglis, Dimitrios Spyropoulos, Georgios Misiakoulis, Fotis Kossiaras, Inna Skarbovsky, Fabiana Fournier, Nikolaos Kapsoulis, John Soldatos, and Konstantinos Perakis

1 Introduction

The banking sector is currently undergoing a major transformation driven by the new revised payment service directive (PSD2) which could act as a catalyst for the innovation in the new wave of financial services. It is clear that the introduction of PSD2 is reshaping the banking sector in a way that has not been seen before in the specific sector posing challenges to the banks that are seeking for solutions to abide by this new regulation while at the same time to leverage the opportunities offered to strengthen their position.

PSD2 was initially introduced in 2017 and entered into force in December 2020. It was introduced as an amendment of the previously established in 2007 payment service directive (PSD) and is a European legislation composed of a set of laws

D. Miltiadou (✉) · S. Pitsios · S. Kasdaglis · D. Spyropoulos · G. Misiakoulis · F. Kossiaras
K. Perakis
UBITECH, Chalandri, Greece
e-mail: dmiltiadou@ubitech.eu; spitsios@ubitech.eu; skasdaglis@ubitech.eu; dspyropoulos@ubitech.eu; gmisiakoulis@ubitech.eu; fkossiaras@ubitech.eu; kperakis@ubitech.eu

I. Skarbovsky · F. Fournier
IBM ISRAEL – SCIENCE AND TECHNOLOGY LTD, Haifa, Israel
e-mail: INNA@il.ibm.com; fabiana@il.ibm.com

N. Kapsoulis
INNOV-ACTS Limited, Nicosia, Cyprus
e-mail: nkapsoulis@innov-acts.com

J. Soldatos
IINNOV-ACTS LIMITED, Nicosia, Cyprus

University of Glasgow, Glasgow, UK
e-mail: jsoldat@innov-acts.com

J. Soldatos, D. Kyriazis (eds.), *Big Data and Artificial Intelligence in Digital Finance*,
https://doi.org/10.1007/978-3-030-94590-9_8

and regulations for electronic payment services in the European Union (EU) and the European Economic Area (EEA) [1]. The main objectives of PSD2 are built around the following main pillars: (a) the establishment of a single, more integrated and efficient payment market across the European Union, (b) the establishment of more secure and safe electronic payments, (c) the protection of the customers of the electronic payment services against possible financial frauds and (d) the boost of innovation in the banking services with the adaptation of new novel technologies.

One of the fundamental changes introduced by PSD2 [2], along with the employment of strong customer authentications and the requirement of the authorised and registered by the European Banking Authority (EBA) payment license, is the requirement to open the access to the financial (or banking) data, currently maintained by the banks, to third-party providers (TPPs). The rationale of this change is to enable banks and their customers to benefit from the usage of third-party APIs towards novel financial services that will foster the innovation in the banking sector. The opening of the payment services of the banks to other TPPs sets the basis for what is referenced in the banking sector as open banking. The initiative of open banking generally refers to the ability for banking customers to authorise third parties to access their bank account data either to collect account information or to initiate payments, as stated on a recent report by KPMG [3]. Through PSD2, the European Commission aims to boost the innovation, transparency and security in the single European payment market [4]. Moreover, PSD2 will support the collaboration between banks and fintech innovative institutions towards the realisation of disruptive business models and new financial services which their customers can leverage.

Open banking imposes that banks have to share personal, and in most cases even sensitive, data of their customers with TPPs. However, besides PSD2, the European Commission has enforced another important directive, the General Data Protection Regulation (GDPR) [5]. GDPR constitutes a European law related to data protection and data privacy imposed in EU and EEA. GDPR was put into effect on May 25, 2018, and imposes a set of strict privacy requirements for the collection, processing and retention of personal information. The primary aim of GDPR is to provide the person whose data is processed – which is referenced in the regulation as the data subject – the control over his/her personal data. It provides the right to data subjects to provide (or withdraw) to their consent for third parties to legitimately access and process their personal data, among others. Furthermore, GDPR imposes strict security and privacy-preserving requirements to the ones collecting and/or processing the data of the data subjects.

As both regulations, PSD2 and GDPR, come into force, it is imperative that the right balance between innovation and data protection is defined and assured by the banks. The reason for this is that, on the one hand, banks are obliged to share the personal and financial data of their customers to the TPPs, while at the same time, on the other hand, banks are responsible for the security of the personal data collected from their customers. To this end, while PSD2 is reshaping the banking sector and is supporting the open banking initiative towards the development and provision of novel financial services, the access to these services that involve personal data must be performed in a GDPR-compliant manner.

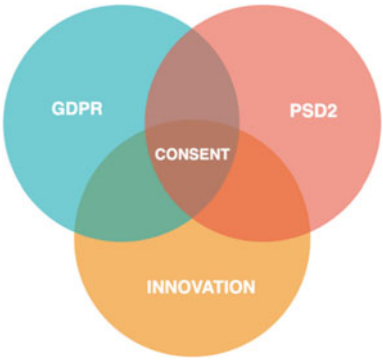

Fig. 8.1 Consent as the bridge between PSD2 and GDPR towards innovation

Hence, in order to properly harness the opportunities offered by PSD2, several aspects need to be taken into consideration. Nevertheless, as stated in a recent report from Ernst & Young, when properly implemented in harmony, PSD2 and GDPR enable banks to better protect and serve consumers, to move beyond compliance and to seize new opportunities for growth [6]. In addition to this, PSD2 constitutes a major opportunity for banks to further strengthen their business models, to introduce new capabilities to their customers and at the same time to become savvier about their customer's patterns of behaviour [3]. As reported by Deloitte, open banking will expand traditional banking data flows, placing the customer at its core and in control of their banking data, including their personal information [4].

Data sharing is the core aspect of open banking. Data sharing drives innovation and in most cases increases the effectiveness and efficiency of existing services, reduces costs and strengthens the relationships of businesses with their clients. However, in the case of open banking as it also involves sharing of personal data, strong requirements related to data protection exist, as explained above. While being two distinct regulations, the bridge between PSD2 and GDPR lays on the consent of the customer of the bank to share his/her data. According to GDPR [5], consent is one of the six legal grounds of lawful processing of personal data, and it needs to be given by a statement or by a clear affirmative action (Fig. 8.1).

Hence, the need for robust and efficient consent management becomes evident. Consent management is the act or process of managing consents from the data subject (or customers in the case of banks) for processing and/or sharing their personal data. And as the PSD2 is built around digital innovation and integration, digital consent management is considered the proper way to tackle the challenges faced for banks towards the compliance with PSD2 and GDPR. The Open Banking Working Group of Euro Banking Association (EBA) reports that digital consent management lies at the heart of any possible solution for the challenges ahead [7]. Digital consent is enabling the banks and/or third-party providers to leverage the opportunities offered by PSD2 in a GDPR-compliant manner. However, the consent management constitutes a process with multiple aspects which shall be taken into consideration during the design and implementation phase.

2 Consent Management for Financial Services

Consent is defined in Article 4 of GDPR as "any freely given, specific, informed and unambiguous indication of a data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her". Furthermore, GDPR requires the explicit consent of the customer in order to process and/or share his/her data. Additionally, the conditions of a consent are strictly defined under Article 7 of GDPR and include, among others, the exact definition of the context of the given consent, the explicit and distinguishable way of the consent gathering as well as the right of the customer to withdraw his/her consent at any time. PSD2 also clearly states that TPPs shall access, process and retain only the personal data that is necessary for the provision of their payment services and only with the "explicit consent" of the payment service user.

Hence, the main characteristics of consent can be grouped as follows [8]:

- The consent must be given as real choice and under the control of the customers. Any element that prevents the customers to exercise their free, such as inappropriate pressure or influence, invalidates the consent. Customer must be able to refuse their consent.
- Consent must be explicit, meaning that the customer must provide consent with affirmative action and the processing purpose must be thoroughly and granularly described to the customer and be distinguishable from other matters.
- The customer must be able to withdraw the consent at any point without negative consequences for him/her.
- In the case where multiple processing operations for more than one purpose, customers must be able freely to choose which purpose they accept rather than having to consent to a bundle of processing requests.
- Consent can be issued in a written and signed form, as well as in an electronic form using an electronic signature or a scanned document carrying the signature of the customer.

In addition to this, a consent must contain at least the following information [8] (Fig. 8.2):

- The data controller's identity
- The purpose of each of the processing operations for which consent is sought
- What (type of) data will be collected and used
- The existence of the right to withdraw consent
- Information about the use of the data for automated decision-making

Consent management constitutes the process of managing consents from the customers for processing their personal data. The effective consent management enables tracking, monitoring and management of the personal data lifecycle from the moment of opt-in to the data erase in GDPR-compliant manner. The core aim of this process is to facilitate and improve the customer's control over their personal

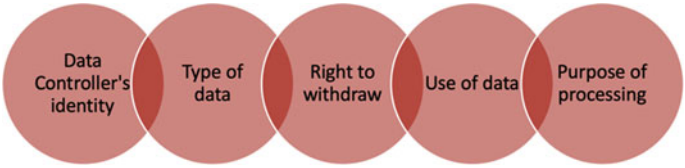

Fig. 8.2 Core content of a valid consent

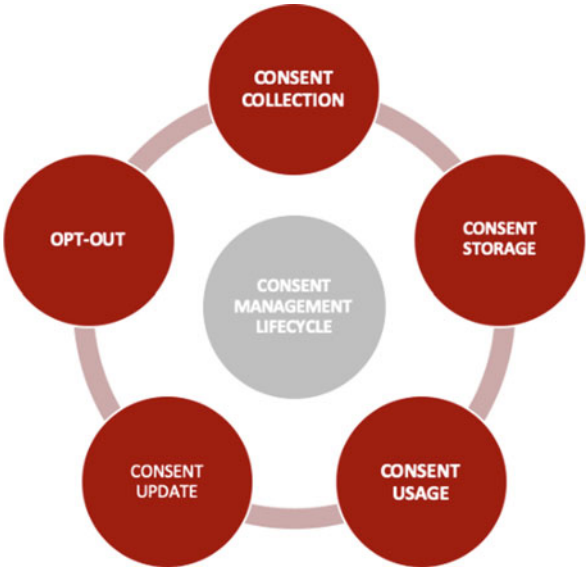

Fig. 8.3 Consent management lifecycle

data enabling their right to provide (or withdraw) consent which allows authorised parties to access their personal and business information and its immediate effect. As it enables granular permission consent, it constitutes a key enabler of trust which is vital to maximise data sharing and assure that customers are comfortable with sharing data.

Consent management is composed of the following distinct phases (Fig. 8.3):

- *Consent Collection*: During this first phase, the consent of the customer (data subject per the GDPR terminology) is formulated. The terms of the consent are strictly defined during this stage. The formulated consent includes at least the information described in the previous paragraph in a clear and unambiguous manner.
- *Consent Storage*: During this second phase, the formulated consent is stored and securely maintained into a single source of truth which is usually a secure data storage modality. To this end, it is imperative that all the necessary measures are undertaken to assure the preservation of the security, privacy and integrity of the stored information.

- *Consent Usage*: During this third phase, the stored consents are effectively leveraged to formulate the decisions related to data access and processing. Hence, the stored consents are provided as input into the proper data access control mechanism in order to evaluate any request to access the personal data of the customer, thus regulating the access and preventing their unauthorised disclosure. The terms of the consent are the holding a critical role in this process. It is very important that they are solid and clear, as well as their integrity is assured.
- *Consent Update*: During this forth phase, it is safeguarded that the customer is able to update the terms of the consent and at the same time that the latest terms of the consent are maintained in a robust and transparent manner. This phase also introduces the requirement for storing the evolution of each consent during its existence.
- *Opt-Out*: During this last phase, the right of the customer to withdraw his/her consent, which constitutes a fundamental right of the data subject per GDPR, is ensured. Hence, at any point, the customer has the legitimate right to withdraw the consent he/she has provided to third parties to access and process their personal data.

A consent management system is the software that facilitates the execution of digital consent management by effectively handling all the operations performed during the complete consent management lifecycle. It acts as the mediator between the involved parties, enabling the formulation, as well as the update or a withdrawal, of a consent and finally its storage into a secure data storage modality.

3 Related Work

The importance of consent management is evident from the large research efforts and the broad number of diverse approaches and solutions that have been proposed in various domains. All the proposed approaches have the safeguarding of individual's privacy as their core requirement; however, the proposed solutions are handling the specific requirement in many different ways. It is also acknowledgeable that although some generic and cross-domain solutions exist, the majority of them are tailored to the needs of a specific domain. It is also evident from literature that IoT and health domains are the most widely explored research areas on this topic.

Taking into consideration the requirement for the existence of valid consent, a web standard protocol called User-Managed Access (UMA) is proposed [9] in an attempt to enable digital applications to offer the required consent management functionalities in a domain-agnostic manner. UMA enables the individuals to perform authorisation control over their personal data access and usage in a unified manner. Nevertheless, this generic solution is lacking in terms of data access auditing, access revocation and the right to be forgotten. Leveraging blockchain technology and smart contract is an additional proposed solution [10] for efficient and effective consent management. Another domain-agnostic approach is based on

blockchain technology and smart contracts [11]; however, it is more focused on data accountability and data provenance. The solution encapsulates the user's consent into a smart contract but is focused on the data subject and data controller aspects while lacking support of the data processor aspects in case where data controller and data processors are different entities.

When it comes to the health domain, multiple approaches and solutions have been proposed, as expected due to the nature of health data which are characterised as sensitive data per the GDPR. The generic consent management architecture (CMA) is proposed [12] as an extension of UMA in combination with the MyData [13] approach. It enables secure data transactions with a context-driven authorisation of multisourced data for secure access of health services maintaining personal data ownership and control. Nevertheless, the proposed architecture is still defined at a general level, and further work is still needed, while some of the utilised technologies require further development. Another approach for consent-based data sharing is also proposed via a web-based solution and video files [14]. In this approach for genomic data sharing, a single one page consent form is introduced on a web application, supplemented with online video that informs the user for the key risks and benefits of data sharing. Nevertheless, this approach does not effectively cover the complete consent management lifecycle. For mobile applications, another initiative is the participant-centred consent (PCC) toolkit [15] whose purpose is to facilitate the collection of informed consents from research participants via mobile. Researchers have also proposed several consent management solutions which are based on the blockchain technology and enable health data sharing. A domain-specific solution is proposed with a blockchain-based data sharing consent model that enables control of the individuals' health data [16]. The proposed solution offers – with the help of smart contracts – dynamic consent definition over health data with the Data Use Ontology (DUO), as well as their search and query via the Automatable Discovery and Access Matrix (ADA-M) ontology. An additional blockchain-based solution for consent management utilises smart contracts for interorganisational health data sharing [17]. It supports searching for patients in the framework that match certain criteria; however, it is based on open and public blockchain networks. Furthermore, several blockchain-based solutions have been proposed in literature [18–20] for the effective data sharing of EHRs and health data in a secured manner.

In addition to the health domain, for the IoT domain, a large number of solutions for consent management is also offered. ADVOCATE [21] platform is providing a user-centric solution that effectively implements the consent management lifecycle for secure access of personal data originating from IoT devices. The solution offers consent management and data disposal policy definition; however, it is domain-specific to the IoT ecosystem. Another solution offers the ability to set their privacy preferences of their IoT devices and safeguards that their data are only transmitted based on these preferences [22]. In this solution, blockchain is used to store and protect these preferences; however, this solution can be considered as a GDPR-compliant solution. A lightweight privacy-preserving solution for consent management is also proposed [23] with cryptographic consents being

issued by the individuals. The specific proposal supports multiple security features, such as untraceability and pseudonymity, exploiting the hierarchical identity-based signature (HIBS). Nevertheless, the proposed approach partially addresses the requirements of GDPR. Additionally, several solutions are proposed for specific IoT device-type only, such as Cooperative Intelligent Transport Systems [24], smart homes [25], medical devices [26, 27] and smart watches [28].

In the finance domain, despite the fact that the requirement for consent management is crucial for financial institutions, the list of available solutions is still limited. A solution built around the double-blind data sharing on blockchain has been proposed [29]. The specific solution is focused on establishing a Know Your Customer (KYC) application through which the consents are formulated supporting the dynamic definition of the consent terms with respect to the data usage. Nevertheless, the specific solution is not supporting the dynamic definition of the purpose of the data usage in the formulated consents. A new blockchain-based data privacy framework that is combined with the nudge theory is also proposed [30]. The specific solution offers a data privacy classification method according to the characteristics of financial data, as well as a new collaborative filtering-based model and a confirmation data disclosure scheme for customer strategies based on the nudge theory. However, the specific approach requires a layered architecture for the designed application that is based on hybrid blockchain, a combination of public and private blockchain which is not usually embraced by financial institutions that operate under strict regulations.

4 Methodology

Within the INFINITECH project, the consortium partners seek to exploit the open banking opportunity, aspiring to examine how open banking and internal banking data sources can be effectively combined in order to gain useful insights and extract knowledge on the customer's patterns of behaviour from a range of data analysis methods.

To this end, the consortium partners were engaged into a series of internal roundtable discussions and brainstorming sessions, bridging the expertise within the consortium in the banking sector services and the existing regulatory framework in the banking sector with the expertise in the design and delivery in technological solutions in order to formulate a novel solution.

The scope of these interactive sessions can be grouped into the following axes:

- To identify the needs of the banking sector with regard to the consent management which could act as the key ingredient of an ecosystem of innovative financial services
- To define the proper consent management process which will ensure the privacy preservation and trustworthiness for data sharing and analysis of financial information between banks, their customers and TPPs

- To define the proper framework which supports customer-centric data services that involve both data acquisition and collaborative data sharing where customers maintain complete control over the management, usage and sharing of their own banking data

As mentioned before, there is a clear need for a solution that bridges the gap between the two distinct regulations, namely, the PSD2 and GDPR regulations. The consent of the bank's customers to share their financial information is considered a hard requirement imposed by these regulations. Hence, it is imperative that banks seeking to leverage the opportunities of open banking design a data-sharing framework which is built around their customer's consent to provide access to their data to any interested party outside their organisation. Within this context, banks shall evaluate how these data are shared and how this proposition is aligned with the requirements and needs of the fintech ecosystem. The data-sharing framework shall take into consideration how these parameters are directly depicted into each consent agreement provided by their customers. As it is clearly stated in GDPR article 7 [5], the consent of the data subject (in this case, the customer of the bank) must contain, in clearly and in easily understandable terms, the information about what they are consenting and, above all, the use of data cannot go beyond what is specified in the consent agreement. Hence, the consent and its terms shall define not only which data can be shared but also when and under which conditions.

In addition to this, a crucial aspect in every data-sharing approach is the security measures that are employed in order to ensure the proper access control besides the security of data at rest. Security is the heart of any data-sharing framework. It constitutes one of the major concerns of any data provider and one of the core aspects that can lower the barriers of adoption of any data-sharing framework. In our case, the proper data access control should be based on the terms of the consent as provided by the customer of the bank. The terms of the consents should be translated into the proper data access policies which prevent unauthorised disclosure to personal data and clearly define what personal data can be accessed and by whom, as well as when and for how long can this personal data be accessed.

Finally, banks need a framework that is, on the one hand, capable of offering custodian services and, on the other hand, ensuring that customers maintain the control over the management, usage and sharing of their banking data. By placing the consent of a customer in the centre of the data-sharing framework, customers will remain in control of their data. This supports secure and controlled accessibility of the data, as the explicit consent of the customers will formulate the decision what data are accessed, who can access them and when this access is revoked. Through the use of consent, the data-sharing framework is enabling both data acquisition and collaborative data sharing to deliver added-value services, both being basic principles of PSD2, in a GDPR-compliant manner.

Towards the design of a novel consent management system that will empower the banks to leverage the PSD2 opportunities in a GDPR-compliant manner, the consortium analysed:

- The requirements elicited from the internal roundtable discussions and brainstorming sessions related to the PSD2 regulation and needs of the banking sector
- The requirements related to the legitimate formulation of a consent of a customer in accordance with the GDPR regulation
- The different phases and characteristics of each phase of the consent management lifecycle

From the analysis of these requirements and characteristics, it became clear that with regard to the consents and their validity period, two different approaches should be supported by the consent management system. The first approach supports the consents for which the validity period is a predefined period as set in the terms of the consent. This consent type is referred as "once off" consent. The expiration of the validity is translated as automatic revocation of the consent, and a new consent is required in order for the recipient to be able to access the customer's data. An example of the cases considered for this consent type is the customer's consent for sharing of KYC data between two financial institutions (banks) for the scenario of a loan origination/application or an account opening. The second approach supports the consents that have an infinite validity period, referred to as permanent (or "regular") consents. This consent type is only invalidated in the case where the consent is withdrawn. An example of the cases considered for this consent type is the peer-to-peer (including person-to-person, person-to-organisation, organisation-to-organisation cases) customer data-sharing consent in which a customer utilises an interface of a mobile application to select a set of its specific customer data (such as specific accounts, specific transactions or alerts) that they would like to share with an individual person or a group of persons.

In addition to the different consent types, the analysis of these requirements and characteristics has also driven the design of the corresponding use cases that should be implemented in order to ensure that all requirements are effectively addressed and that the designed consent management system will bring the added value to the banking sector's stakeholders. The defined use cases cover the complete lifecycle of consent management system, starting from the registration of the relevant users, the formulation of the consent and its storage to the retrieval of the stored consent in order to formulate the data access control decision.

The key stakeholders which are involved and are interacting with the proposed solution are:

- The internal financial institution (namely the bank) that collects and has access to its customer data
- The customer of internal financial institution (namely, customer of the bank) whose data are collected by the internal financial institution
- The external financial institution or peer (namely, third-party provider) that aspires to obtain the data of the customer of internal financial institution upon the formulation of a valid and legitimate consent that is formulated between the three parties

The consortium analysed also the latest state-of-the-art technologies which can be leveraged for the implementation of the aspired solution. The core aspect of any data-sharing framework is the employed security. However, traditional technologies have failed to become a key enabler of trust, due to multiple security/data tampering incidents as it is evidenced by the recent large-scale personal data breaches around the world [31]. Nevertheless, blockchain technology and its latest advancements appear as a compelling technology to overcome the underlying challenges around trusted data sharing by exploiting its attractive features such as immutability and decentralisation.

In the following paragraphs, the different use cases which are supported by the aspired solution are presented in detail.

4.1 User's Registration

The first step includes the registration of the different users in the consent management system. Different roles are assigned to the users based on the role in the consent formulation process. In order for a customer to be able to receive consent requests, it is mandatory that they are registered in the consent management system, creating their profile that will be used in order to receive consent requests. Their profile includes the minimum customer discovery and communication details required in order to receive a consent request, while it ensured that this information and any consequent private information are not disclosed to any interested party. In the same manner, the third-party provider registers in the consent management system in order to be able to initiate consent requests to a customer of the bank. The users of the bank, who are considered as the administrators of the consent management system, are already preregistered so as to facilitate the whole execution (Fig. 8.4).

4.2 Customer Receives a Request to Provide New Consent for Sharing His/Her Customer Data

The consent formulation is initiated from the third-party provider. In particular, the third-party provider issues a new consent request to the consent management system indicating the specific customer that accesses to his/her is requested along with the details of the requested customer data (i.e. specific data, period of usage). As a first step, the initial request is received and reviewed by the bank before it is pre-approved and received by the customer. Upon this approval, the customer receives a notification with all the required information for the consent request in a proper way that it allows them to review the request (Fig. 8.5).

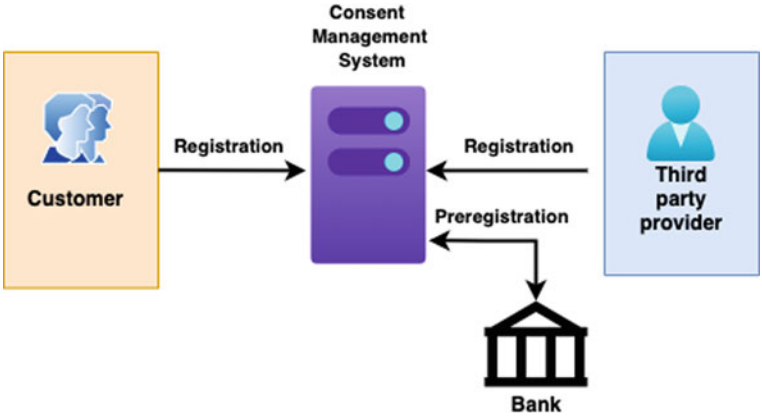

Fig. 8.4 User's registration

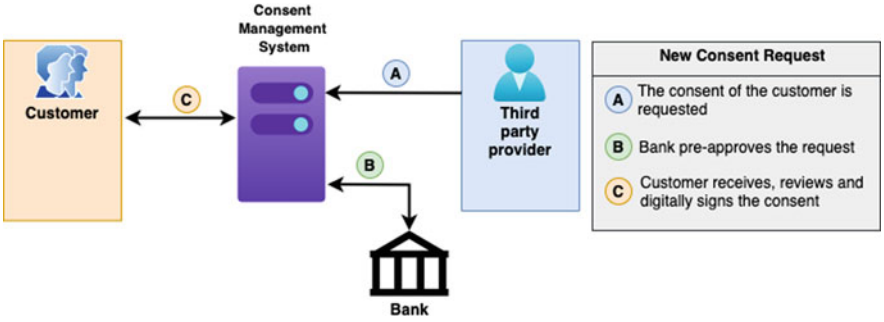

Fig. 8.5 New consent request

4.3 Definition of the Consent

In this step of the process, the customer is able to review, and possibly alter, the details and conditions of the consent request before he/she formulates his/her decision to provide the consent or deny the access to his/her personal data. In the case of approval, the final terms of the consent are defined by the customer, and it is submitted to the consent management system. The third-party provider is then informed and can approve the final terms of the consent, as set by the customer, or abandon the consent request. In the case of denial from the customer on the initial request, the request is blocked, and the third-party provider is informed for the completion of the process (Fig. 8.6).

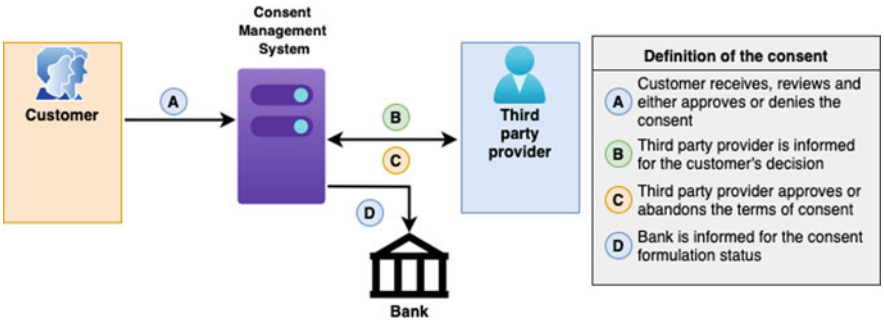

Fig. 8.6 Definition of the consent

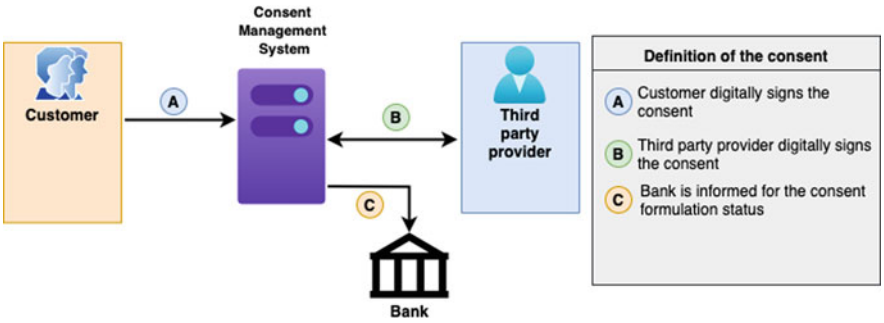

Fig. 8.7 Digital signing of the consent

4.4 Signing of the Consent by the Interested Parties

Once the terms of the consent have been formulated, the consent management system provides the formulated consent form to both parties (the customer and the third-party provider) in order to be digitally signed. The consent management system collects the digitally signed consent forms from both parties. At this point, the consent status is now set as "active" (Fig. 8.7).

4.5 Consent Form Is Stored in the Consent Management System

Once the digitally signed consent form is available, the consent management system is able to store this information in order to be used in the access control formulation process. In the case of the "once off" consent, where a specific validity period is defined, the consent management system is internally handling the validation of

consent time period by creating and monitoring the specific timer in order to perform the validation of consent time period.

4.6 Consent Update or Withdrawal

In accordance with the GDPR regulation, the formulated consent form can be updated or withdrawn at any time by the customer side. On the one hand, the terms of the consent can be updated following the previously described steps (from the definition of the consent till the consent storage) in order to formulate the updated consent and maintain the consent status "active". In the case of the "once off" consent, the associated timer is restarted when the consent is updated. On the other hand, the consent can be withdrawn, which is internally translated into the update of the consent status to "withdrawn". In this case, if the withdrawn consent is a "once off" consent, the associated timer is stopped. For both cases, the consent management system ensures that the complete history of each consent is maintained for later usage (Figs. 8.8 and 8.9).

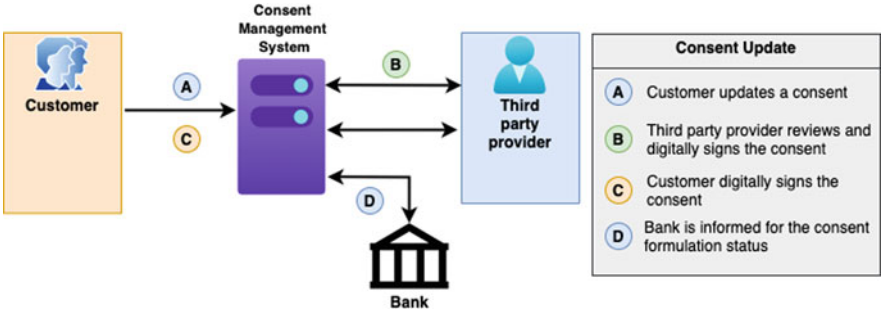

Fig. 8.8 Consent update

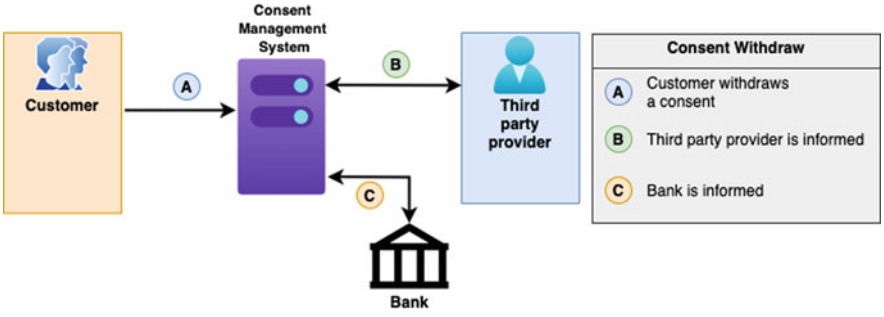

Fig. 8.9 Consent withdrawal

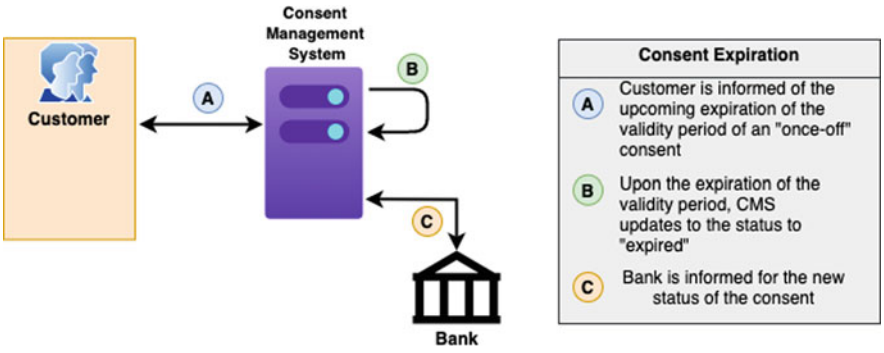

Fig. 8.10 Consent expiration

4.7 Expiration of the Validity Period

In the case of the "once off" consent, the validity period is set to a predefined time period. When consent is formulated, the consent management system creates and monitors the specific timer in order to perform the validation of consent time period. The consent management system informs the customer before the validity period of a "once off" consent expires in case he/she would like to initiate an update before the validity period expires. Once this timer is expired, the consent management system sets the status of the specific consent to "expired" (Fig. 8.10).

4.8 Access Control Based on the Consent Forms

The key aspect of the aspired data-sharing framework is the efficient and robust access control mechanism with the consent management system at its core. During each data access request to underlying data management system, the consent management system is consulted in order to validate the consent status between the requesting party and the customer whose data are requested. The data access control decision is formulated by the existing consents and their status, as well as the underlying terms of each consent (Fig. 8.11).

4.9 Retrieve Complete History of Consents

Another key aspect of the proposed solution is that the customer is able to be constantly informed of all the consents that are given to each specific recipient, as well as of the complete history of these consents. Furthermore, for each consent, all the different versions of the provided consent can be retrieved besides the latest

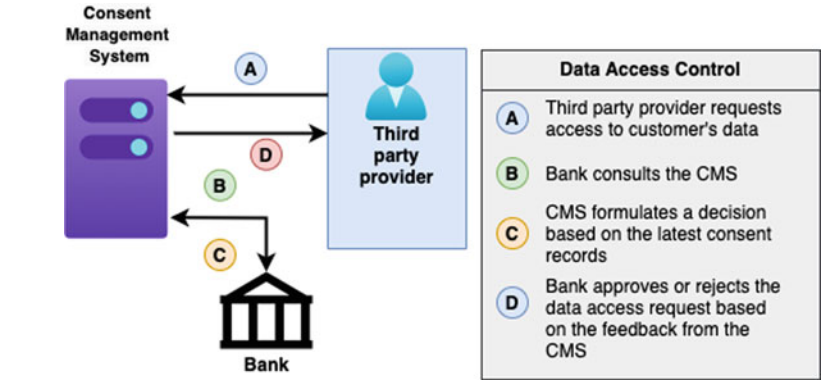

Fig. 8.11 Access control based on consents

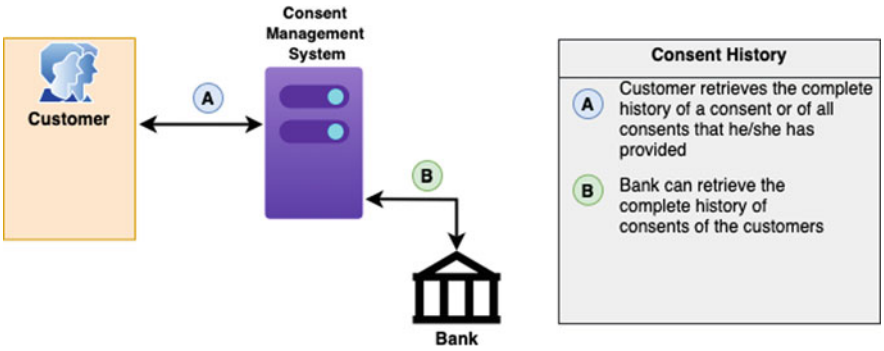

Fig. 8.12 Complete history of consents retrieval

one. In this sense, the customer shall be able to retrieve at any time their consent history per specific stakeholder or for all stakeholders, while the bank shall be to retrieve all the consents given by the customers for a stakeholder (Fig. 8.12).

5 The INFINITECH Consent Management System

The designed solution aims to enable the collaborative data sharing between customers, banks and other organisations, in order to facilitate the application of advanced analytics over particular datasets and intelligent support tools for better understanding of customers and their financial relationships among others, which is considered critically important in today's financial markets.

As explained, the development of such intelligence support tools is highly dependent on the customer's permission to share data. Hence, the requirement for a trusted and secure sharing mechanism of customer consent arises in order

enable the development of new customer services that solve business problems, such as improved KYC processes and consequently AML, credit scoring and fraud detection services. A robust and solid consent management system that will support the granular permission consent is considered as a key enabler of trust which is vital to maximise data sharing and ensure customers are comfortable with sharing data.

Blockchain is a continuously growing, distributed, shared ledger of uniquely identified, linked transaction records organised in blocks that are sealed cryptographically with a digital fingerprint generated by a hashing function and are sequentially chained through a reference to their hash value [32]. In general, the blockchain technology is composed of multiple technologies related to cryptography, peer-to-peer networks, identity management, network security, transaction processing, (distributed) algorithms and more, which are all leveraged in order to formulate an immutable transaction ledger which is maintained by a distributed network of peer nodes formulating the blockchain network. The key characteristics of the blockchain technology are that it is decentralised, immutable, transparent, autonomous and open-sourced [33].

The blockchain technology has a set of key concepts that includes (a) the distributed ledger that is composed by blocks containing the transaction records, (b) the consensus model that is utilised in order to validate a transaction and to keep the ledger transactions synchronised across the blockchain network and (c) the smart contracts or chaincodes which are the trusted distributed applications that are deployed within the nodes of the blockchain network and encapsulate the business logic of the blockchain applications. The blockchain implementations can be characterised and grouped into two major high-level categories based on the permission model applied on the blockchain network, the *permissionless blockchain networks* which are open and publicly and anonymously accessible blockchain networks and the *permissioned blockchain networks* where only authorised users are able to maintain, read and access the underlying blockchain.

Our solution exploits the benefits of blockchain technology and specifically the permissioned blockchain that is considered as the appropriate candidate solution due to its security and trust characteristics. It is built around a blockchain application that implements a decentralised and robust consent management mechanism which facilitates the sharing of the customers' consent to exchange and utilise their customer data across different banking institutions. Built on top of the core offerings of the blockchain technology, namely, its decentralised nature and immutability, as well as the impossibility of ledger falsification, our approach ensures the integrity of customer data processing consents and their immutable versioning control through the use of the appropriate blockchain infrastructure. Hence, the blockchain-enabled consent management mechanism enables the financial institutions to effectively manage and share their customers' consents in a transparent and unambiguous manner.

Its key differentiating points, from the financial institutions' perspective, is the ability to inform the customer at any time:

- For any customer data that it managed upon their consent
- The latest status of their consent (active or revoked/withdrawn)
- The recipients (financial institutions or peers) of their customer data upon their consent
- The purpose (or even legal basis) and time period of their customer data sharing to the recipient (financial institutions or peers)

On the other hand, its key differentiating points, from the customer's perspective, are enables them to:

- Be constantly informed for all the requests for sharing their customer data
- Be able to activate or revoke their consents
- Be constantly aware of the active consents they have given to each specific recipient

Our solution exploits the benefits of the blockchain technology in order to assure the integrity of the formulated consents with the utilisation of its cryptographic techniques in combination with the usage of digital signatures. In addition to this, the formulated consent and their complete update history are stored in a secure and trusted manner within the blockchain infrastructure. Hence, the blockchain technology is leveraged to store this sensitive information, to apply immutable versioning control and to enable the retrieval of this information in an indisputable manner. With the use of blockchain technology, both the financial institutions and their customers are able to retrieve the latest untampered consent information, as well as any previous versions of the consent.

The solution is designed to hold the role of the middleware application between the data management applications of the financial institution, in which the secured APIs are available, and the third-party providers. Hence, the designed consent management system does not save or distribute any customer data. Being a middleware application, it provides the means to formulate a consent agreement and utilise the existing consent agreements to formulate an access control decision that should be propagated to the underlying data management applications through which the customer data are actually shared to the third-party provider.

The high-level architecture of our solution is depicted in Fig. 8.13. Our solution is composed by a set of core components, namely, the *consent management system*, the *file storage* and the *blockchain infrastructure*, which are effectively interacting via well-defined RESTful APIs. Following the analysis performed in the previous section, the main stakeholders that are involved are the internal financial institution (namely, the bank), the customer of internal financial institution (namely, customer of the bank) and the external financial institution or peer (namely, third-party provider).

The consent management system constitutes the mediator between the stakeholders and the underlying blockchain infrastructure. It receives and effectively handles the requests for the consent formulation from the external financial institution or peer to the internal financial institution and consequently the customer of the internal institution. The consent management system implements the complete consent

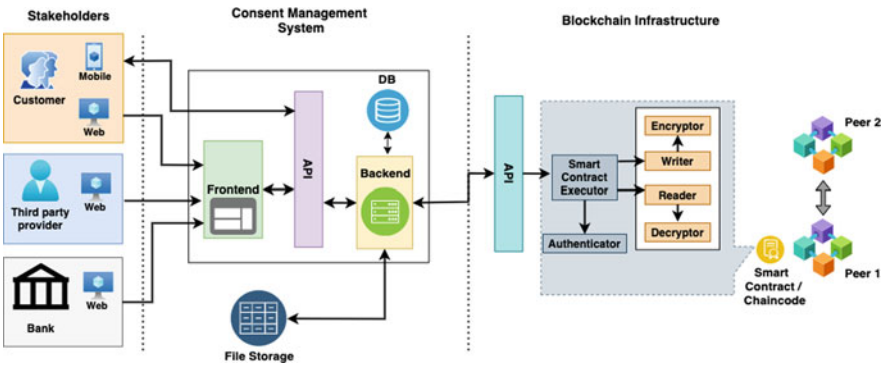

Fig. 8.13 High-level architecture of the blockchain-enabled consent management system

management lifecycle by leveraging the functionalities offered by the underlying blockchain infrastructure. To facilitate the interactions of the stakeholders with the consent management system, it offers both a Web application and a mobile application. The Web application is offered to all the involved stakeholders, in order to interact with the system on each step of the process. The Web application is composed of the core backend component that provides all the backend operations of the system, such as the processing of the input data, the retrieval of the requested information and all the interactions with the underlying blockchain infrastructure. The core backend component is supported by a local database instance in which only the operational data is maintained, such as the user management data or the data of a consent that is still under formulation. The graphical interface of the consent management system which provides all the functionalities of the Web application to the stakeholders is offered by the frontend component. The frontend component interacts with the backend via a set of APIs provided by the backend in order to perform all the requested activities by the stakeholders. In addition to the Web application, the customers of the bank are offered with the mobile application through which they are able to perform all the required operations in the same manner as they are offered by the web application.

The file storage component is providing the file repository that stores the finalised consent forms in digital format once all the steps of the process have been completed upon the acceptance of the details and terms of the consent by all the involved parties. It provides the required interface to the consent management system in order to store or retrieve the formulated consent forms upon need.

The blockchain infrastructure is providing the permissioned blockchain network of the solution. The designed blockchain network constitutes the cornerstone of the proposed solution and is based on Hyperledger Fabric[1]. In detail, the designed blockchain network is formulated by two peers (P1 and P2), which are owned by

[1] Hyperledger Fabric, https://www.hyperledger.org/use/fabric

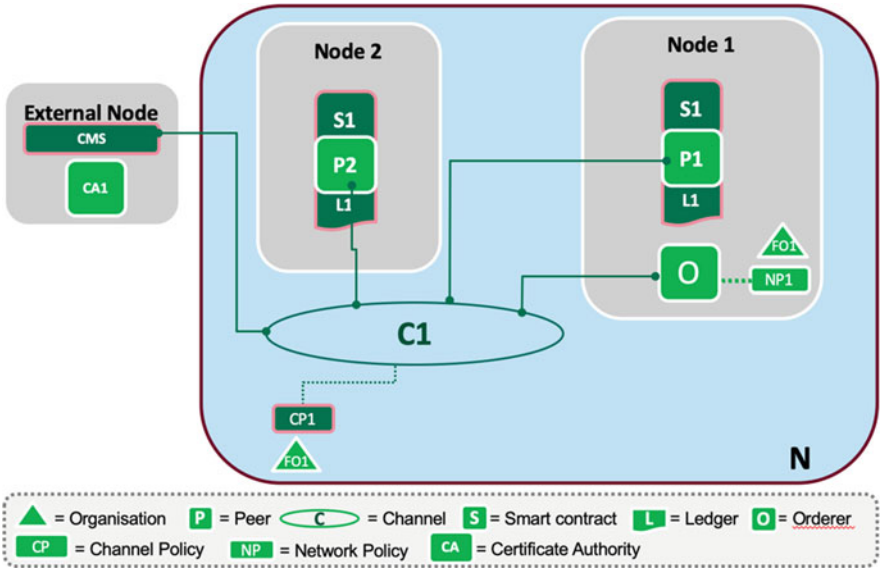

Fig. 8.14 Blockchain network of the solution

one single organisation (FO1) and are hosting their own copy of the distributed ledger (L1). Both peers are operating in one channel (C1) in which the smart contract/chaincode (S1) is deployed. In the designed blockchain network, a single order (O), which formulates the transactions into blocks and ensures the delivery of the blocks to the peers of the channel, is deployed. In this blockchain network, the consent management system is deployed on an external node which also holds the single certificate authority (CA1) that is utilised for the secure interaction with channel C1. Channel C1 is regulated by the underlying channel policy CP1 that ensures the isolation of the channel from external peers and other channels. Finally, the complete blockchain network is regulated by the network policy NP1 that is applied across the whole network with permissions that are determined prior to the network creation by organisation FO1. The interaction between the blockchain infrastructure and the backend of the consent management system is realised through the well-defined APIs provided by the smart contract/chaincode S1 (Fig. 8.14).

As explained before, the smart contract/chaincode is the trusted distributed application that encapsulates the business logic of solution. It contains the definition of the business objects for which the current and historical state will be maintained and updated through a set of functions which are also included in the chaincode. To facilitate the desired operations, the data schema that defines the core business objects has been defined, and it is depicted in Fig. 8.15. The definition was based on the consent receipt specification that is proposed by the Kantara Initiative [34] which has been adapted in terms of terminology in order to be aligned with the EU GDPR

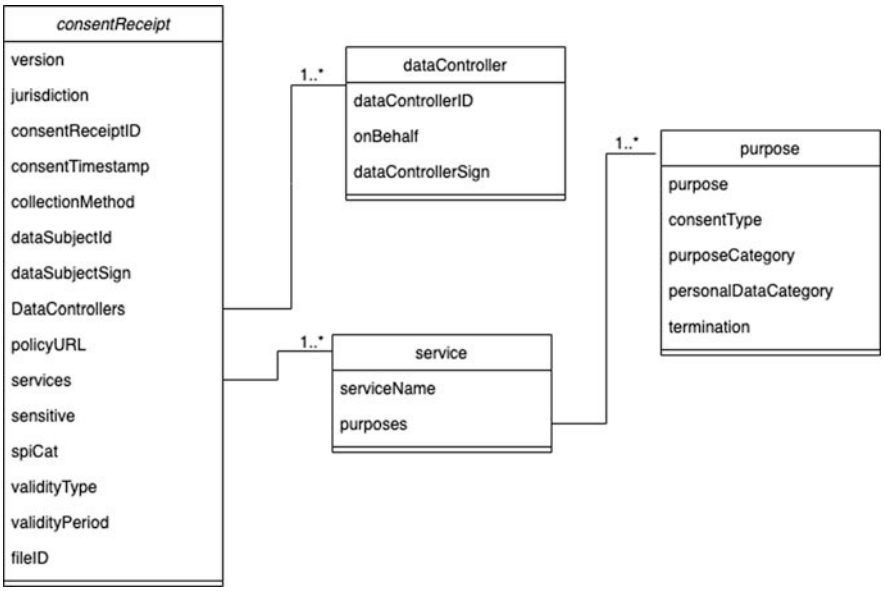

Fig. 8.15 Data schema

legislation. The designed data schema covers all the aspects of a consent, spanning from the generic information, such as the version number, the unique identifier and the timestamp of creation or modification, to more specific information such as the data subject information, the data controllers' information, the applied privacy policy, the service or group of services for which personal data are collected and the relevant purposes and of course the exact personal and/or sensitive data that are collected. Additionally, key information for the consent management lifecycle execution is included, such as the latest status of the consent, the validity type (permanent or once off) and the validity period in the case of once off consent**.**

The chaincode is directly built on top of the presented data schema with a set of functions which are conceptually organised into the following groups of functions:

- *Blockchain Reader*: The main purpose of this group is to enable the fetching of the requested data from the blockchain ledger. It provides the necessary functions to read the ledger state, fetch a particular consent by id, query the ledger state given different parameters to fetch a set of consents matching those parameters and get the consent history (history of all updates for particular consent data entity or data entities).
- *Blockchain Writer*: The main purpose of this group is to facilitate the submission of new transactions to the blockchain ledger. In particular, this group submits new transactions for a new consent, an updated consent or a withdrawn consent.

- *Smart Contract Executor*: The main purpose of this group is to encapsulate the business logic of the designed solution and execute the smart contracts on the blockchain ledger. In particular, this group invokes all the operations related to the read and write operations, leveraging the respective functions of the blockchain writer and blockchain reader.
- *Blockchain Authenticator*: The main purpose of this group is to perform the authentication of the blockchain network user in order to grant access to a specific channel of the blockchain network.
- *Blockchain Encryptor*: The main purpose of this group is to execute the encryption operations which are performed on the consent data prior to being inserted as new transactions to the blockchain ledger.
- *Blockchain Decryptor*: The main purpose of this group is to perform the decryption of the consent data which were encrypted by the *blockchain encryptor*.

5.1 Implemented Methods

In the following paragraphs, the implemented methods of the designed solution are presented. The basis of the implementation was the initial use cases, as well as the collected requirements, which were described in the methodology section. The implemented methods effectively cover all the aspects of the consent management lifecycle. On each method, the different interactions of the various components of the solution, as well as the interactions of the stakeholders with these components, are highlighted.

5.1.1 Definition of Consent

The formulation of the consent involves several steps from the initial consent request, as initiated by the third-party provider to the consent management system, to the actual consent formulation with the exact terms and validity period and its storage within the blockchain infrastructure. At first, the received consent request is pre-approved by the bank through the consent management system via the Web application. Once it is pre-approved by the bank again via the Web application, the request is received by the customer through the consent management system either via the Web application or via the mobile application. The customer reviews and defines the final terms of the consent and submits the digitally signed consent in the consent management system. The formulated consent is received by the third-party provider and is also digitally signed. Once the consent is digitally signed by both parties, the consent management system interacts with the blockchain infrastructure via the provided API, and a new transaction is created and inserted into the blockchain via the deployed chaincode with status “active”. In the case of the “once off” consent, where a specific validity period is defined, the consent management system is internally handling the validation of consent time period

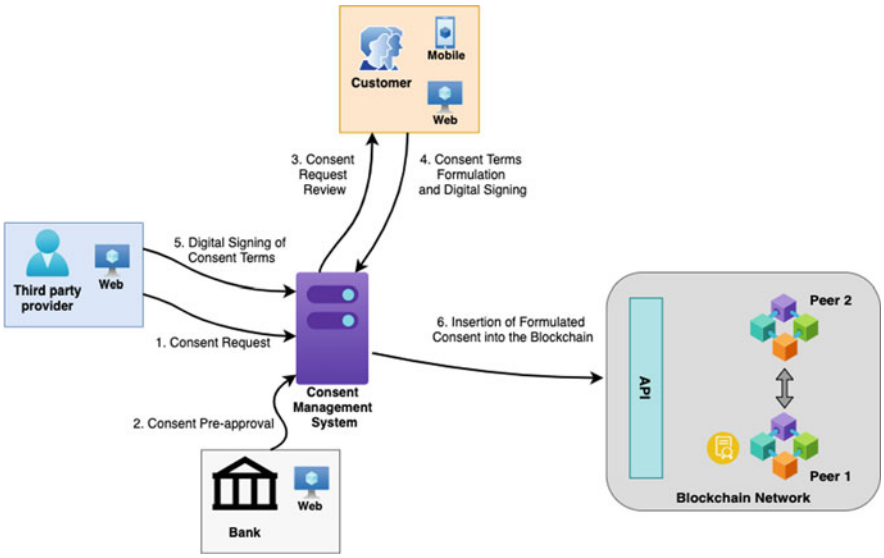

Fig. 8.16 The definition of consent method

by creating and monitoring the specific timer in order to perform the validation of consent time period (Fig. 8.16).

5.1.2 Consent Update or Withdrawal

The customer is able to retrieve and update or withdraw a consent at any time. At first, the selected consent is retrieved from the consent management system by interacting with the API of the blockchain infrastructure. At this point, the customer is presented with the existing terms of the consent and can modify its terms or withdraw it. In the consent update case, the updated terms are digitally signed by the customer and received by the consent management system. The involved third-party provider is notified and digitally signs the updated consent. Once the updated consent is digitally signed by both parties, the consent management system interacts again with the blockchain infrastructure via the provided API in order to initiate a new transaction and insert it into the blockchain via the deployed chaincode while the status remains "active". In the case of the "once off" consent, the associated timer is restarted when the consent is updated.

In the case of withdrawal, the consent management system interacts with the blockchain infrastructure via the provided API in order to "invalidate" the existing consent with the new transaction which sets the new status to "withdrawn". In the case of the "once off" consent, the consent management system also stops the respective timer. Every update or withdrawal of an existing consent introduces in

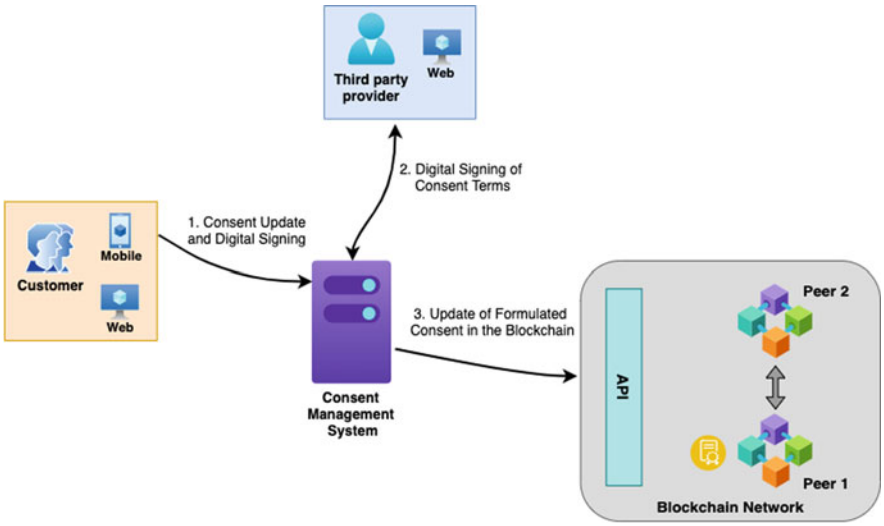

Fig. 8.17 The consent update method

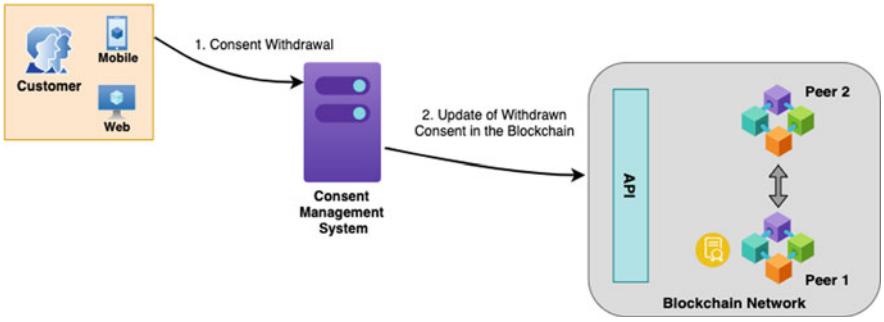

Fig. 8.18 The consent withdrawal method

a new version of the specific consent is appended into the complete history that is maintained within the blockchain infrastructure (Figs. 8.17 and 8.18).

5.1.3 Consent Expiration

The "once off" consent has a validity period as defined in the terms of the consent. Once a "once off" consent has been formulated, the consent management system creates and monitors the specific timer. At the point where the timer is about to expire, the consent management system informs the respective customer to initiate an update of the consent that will result in the timer renewal based on the terms of the updated consent. In the case where the timer expires, the consent management

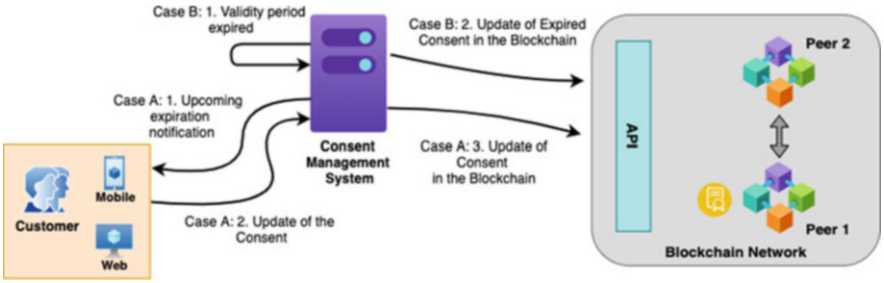

Fig. 8.19 The consent expiration method

system interacts with the blockchain infrastructure via the provided API in order to "invalidate" the existing consent with the new transaction which sets the new status to "expired" (Fig. 8.19).

5.1.4 Access Control

Once a data access request is received by the bank on their data management system from a third-party provider, the bank consults the consent management system via the Web application in order to verify and approve the specific data access request based on the terms and current status of the consent between the third party and the customer whose data are requested. To this end, the consent management system receives the information of the involved parties from the bank and initiates a query into the blockchain infrastructure via the provided API in order to retrieve the latest consent between them.

In the case where the consent status is "active" and the terms are met, the data access request can be approved, while in the case where the status is set to "withdrawn" and "expired" or a consent between the involved parties does not exist, the data access request should be denied (Fig. 8.20).

5.1.5 Complete History of Consents

The consent management system offers the retrieval and display of the latest consent information, as well as the complete history of the existing consents, at any point. The customer can retrieve the list of consents in a user-friendly way via the Web application or the mobile application. Depending on his/her selection, the customer can select and view a specific consent that has been provided to a third-party provider, as well as the complete of consents that he/she has provided to any third party provider. On the other hand, the bank is also able to retrieve a specific consent between a specific customer and a third-party provider, all the consents that a third

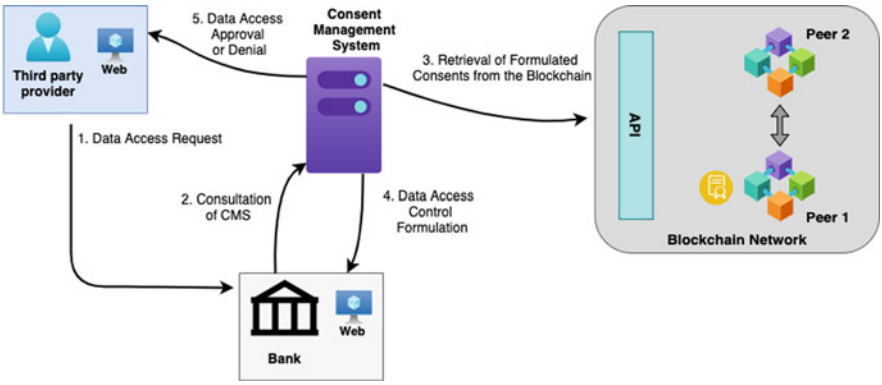

Fig. 8.20 The access control based on consent method

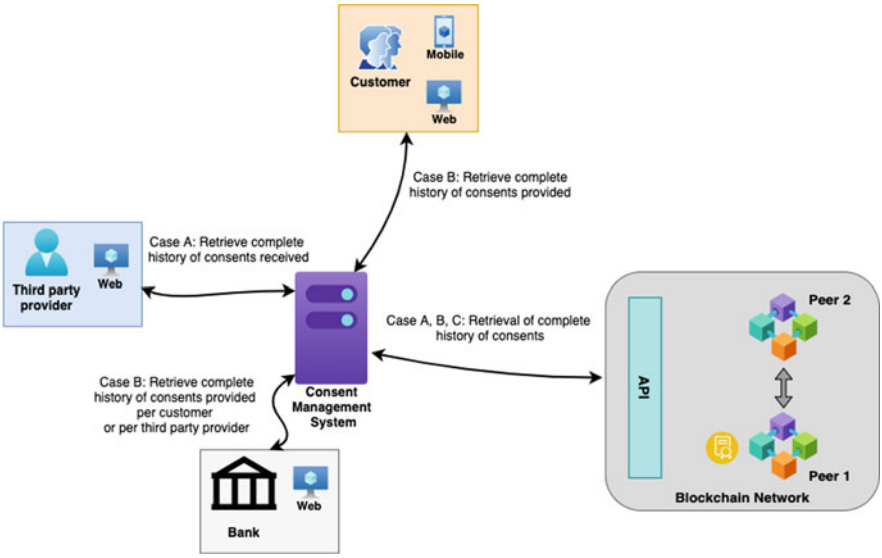

Fig. 8.21 The retrieval of the complete history of consent method

party has received by any of its customers and finally the complete list of consents provided by all his/her customer to any third-party provider.

To achieve this, the consent management system translates the request initiated by either the customer or the bank into a query with specific parameters which is executed into the blockchain infrastructure via the provided API in order to retrieve the requested information and display it to the requestor (Fig. 8.21).

6 Conclusions

The designed and implemented solution of the blockchain-empowered consent management system enables the sharing of customers' consent, thus facilitating the exchange and the utilisation of customer data, across different banking institutions. It enables the exploitation of the open banking opportunities towards the realisation of novel financial services through the collaborative data sharing in a PSD2- and GDPR-compliant manner.

Building directly on top of the key offering of the blockchain technologies that address the underlying challenges around trusted data sharing, the proposed consent management system effectively supports the employment of a trusted and secure sharing mechanism that is based on the customer consent to share his/her data. The provided solution constitutes a robust and solid consent management system that can act as a key enabler of trust of an ecosystem of innovative financial services in which customers are comfortable with sharing data since they are maintaining complete control over the management, usage and sharing of their own banking data.

Acknowledgments The research leading to the results presented in this chapter has received funding from the European Union's funded Project INFINITECH under Grant Agreement No. 856632.

References

1. European Commission – European Commission. (2021). *Payment services (PSD 2) – Directive (EU) 2015/2366* [online]. Available at: https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en. Accessed 10 June 2021.
2. Tuononen, K. (2019). *The impact of PSD2 directive on the financial services industry*.
3. KPMG. (2021). *Open banking opens opportunities for greater customer* [online]. Available at: https://home.kpmg/ph/en/home/insights/2019/07/open-banking-opens-opportunities-for-greater-value.html. Accessed 8 June 2021.
4. Deloitte. (2018). *Open banking – Privacy at the epicentre* [online]. Deloitte. Available at: https://www2.deloitte.com/content/dam/Deloitte/au/Documents/financial-services/deloitte-au-fs-open-banking-privacy-epicentre-170718.pdf. Accessed 9 June 2021.
5. Official Journal of the European Union. (2016). *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL* [online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN. Accessed 6 June 2021.
6. Ernst & Young Global Limited. (2019). *How banks can balance GDPR and PSD2* [online]. Available at: https://www.ey.com/en_lu/banking-capital-markets/how-banks-can-balance-gdpr-and-psd2. Accessed 18 June 2021.
7. Euro Banking Association, B2B Data Sharing: Digital Consent Management as a Driver for Data Opportunities. 2018.
8. European Data Protection Board. (2020). *Guidelines 05/2020 on consent under Regulation 2016/679* [online]. Available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en. Accessed 5 June 2021.

9. Maler, E. (2015, May). Extending the power of consent with user-managed access: A standard architecture for asynchronous, centralizable, internet-scalable consent. In 2015 *IEEE security and privacy workshops* (pp. 175–179). IEEE.
10. Sağlam, R. B., Aslan, Ç.B., Li, S., Dickson, L., & Pogrebna, G. (2020, August). A data-driven analysis of blockchain systems' public online communications on GDPR. In 2020 *IEEE international conference on decentralized applications and infrastructures* (DAPPS) (pp. 22–31). IEEE.
11. Neisse, R., Steri, G., & Nai-Fovino, I. (2017, August). A blockchain-based approach for data accountability and provenance tracking. In *Proceedings of the 12th international conference on availability, reliability and security* (pp. 1–10).
12. Hyysalo, J., Hirvonsalo, H., Sauvola, J., & Tuoriniemi, S. (2016, July). Consent management architecture for secure data transactions. In *International conference on software engineering and applications* (Vol. 2, pp. 125–132). SCITEPRESS.
13. Alén-Savikko, A., Byström, N., Hirvonsalo, H., Honko, H., Kallonen, A., Kortesniemi, Y., Kuikkaniemi, K., Paaso, T., Pitkänen, O. P., Poikola, A., & Tuoriniemi, S. (2016). *MyData architecture: consent based approach for personal data management*.
14. Riggs, E. R., Azzariti, D. R., Niehaus, A., Goehringer, S. R., Ramos, E. M., Rodriguez, L. L., Knoppers, B., Rehm, H. L., & Martin, C. L. (2019). Development of a consent resource for genomic data sharing in the clinical setting. *Genetics in Medicine, 21*(1), 81–88.
15. Wilbanks, J. (2018). Design issues in e-consent. *The Journal of Law, Medicine & Ethics, 46*(1), 110–118.
16. Jaiman, V., & Urovi, V. (2020). A consent model for blockchain-based distributed data sharing platforms. *arXiv preprint arXiv*:2007.04847.
17. Shah, M., Li, C., Sheng, M., Zhang, Y., & Xing, C. (2020, August). Smarter smart contracts: Efficient consent management in health data sharing. In *Asia-Pacific Web (APWeb) and Web-Age Information Management (WAIM) joint international conference on web and big data* (pp. 141–155). Springer.
18. Thwin, T. T., & Vasupongayya, S. (2018, August). Blockchain based secret-data sharing model for personal health record system. In *2018 5th international conference on advanced informatics: Concept theory and applications* (ICAICTA) (pp. 196–201). IEEE.
19. Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F., 2017. Secure and trustable electronic medical records sharing using blockchain. In *AMIA annual symposium proceedings* (Vol. 2017, p. 650). American Medical Informatics Association.
20. Zheng, X., Mukkamala, R.R., Vatrapu, R., & Ordieres-Mere, J. (2018, September). Blockchain-based personal health data sharing system using cloud storage. In *2018 IEEE 20th international conference on e-health networking, applications and services* (Healthcom) (pp. 1–6). IEEE.
21. Rantos, K., Drosatos, G., Kritsas, A., Ilioudis, C., Papanikolaou, A., & Filippidis, A. P. (2019). A blockchain-based platform for consent management of personal data processing in the IoT ecosystem. *Security and Communication Networks*, 2019.
22. Cha, S. C., Chen, J. F., Su, C., & Yeh, K. H. (2018). A blockchain connected gateway for BLE-based devices in the internet of things. *IEEE Access, 6*, 24639–24649.
23. Laurent, M., Leneutre, J., Chabridon, S., & Laaouane, I. (2019). Authenticated and privacy-preserving consent management in the internet of things. *Procedia Computer Science, 151*, 256–263.
24. Neisse, R., Baldini, G., Steri, G., & Mahieu, V. (2016, May). Informed consent in Internet of Things: The case study of cooperative intelligent transport systems. In *2016 23rd international conference on telecommunications (ICT)* (pp. 1–5). IEEE.
25. Song, T., Li, R., Mei, B., Yu, J., Xing, X., & Cheng, X. (2017). A privacy preserving communication protocol for IoT applications in smart homes. *IEEE Internet of Things Journal, 4*(6), 1844–1852.
26. Fan, K., Jiang, W., Li, H., & Yang, Y. (2018). Lightweight RFID protocol for medical privacy protection in IoT. *IEEE Transactions on Industrial Informatics, 14*(4), 1656–1665.

27. O'Connor, Y., Rowan, W., Lynch, L., & Heavin, C. (2017). Privacy by design: Informed consent and internet of things for smart health. *Procedia computer science, 113*, 653–658.
28. Jahan, M., Seneviratne, S., Chu, B., Seneviratne, A., & Jha, S. (2017, October). Privacy preserving data access scheme for IoT devices. In 2017 *IEEE 16th international symposium on network computing and applications* (NCA) (pp. 1–10). IEEE.
29. Bhaskaran, K., Ilfrich, P., Liffman, D., Vecchiola, C., Jayachandran, P., Kumar, A., Lim, F., Nandakumar, K., Qin, Z., Ramakrishna, V., & Teo, E. G. (2018, April). Double-blind consent-driven data sharing on blockchain. In *2018 IEEE international conference on cloud engineering (IC2E)* (pp. 385–391). IEEE.
30. Ma, S., Guo, C., Wang, H., Xiao, H., Xu, B., Dai, H. N., Cheng, S., Yi, R., & Wang, T. (2018, October). Nudging data privacy management of open banking based on blockchain. In *2018 15th international symposium on pervasive systems, algorithms and networks* (I-SPAN) (pp. 72–79). IEEE.
31. Lim, S. Y., Fotsing, P. T., Almasri, A., Musa, O., Kiah, M. L. M., Ang, T. F., & Ismail, R. (2018). Blockchain technology the identity management and authentication service disruptor: A survey. *International Journal on Advanced Science, Engineering and Information Technology, 8*(4-2), 1735–1745.
32. Treleaven, P., Brown, R. G., & Yang, D. (2017). Blockchain technology in finance. *Computer, 50*(9), 14–17.
33. Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. (2019). Analysis of Blockchain technology: Pros, cons and SWOT. *Cluster Computing, 22*(6), 14743–14757.
34. Kathrein, A. (2019). Consent receipt specification – Kantara initiative [online]. Kantara Initiative. Available at: https://kantarainitiative.org/download/7902/. Accessed 1 June 2021.