Trust Through Transparency: Blockchain for Consent and Accountability in Femtech Applications

Larissa Tomaz
David R. Matos
larissa.tomaz@tecnico.ulisboa.pt
david.r.matos@tecnico.ulisboa.pt
INESC-ID, Instituto Superior Técnico, Universidade de Lisboa
Lisbon, Portugal

Teresa Almeida
ITI/LARSyS, Instituto Superior Técnico, Universidade de Lisboa
Lisbon, Portugal
teresa.almeida@tecnico.ulisboa.pt

Abstract

In recent years, Femtech has emerged as a growing market category dedicated to women's health technologies. Despite its rapid expansion, this relatively new and largely unregulated sector has experienced several concerning security breaches that compromise user privacy and intimacy. To address this critical gap between innovation and protection, we propose a novel blockchain-based consent management framework specifically designed for Femtech applications. Our solution leverages distributed ledger technology and smart contracts to create a transparent, immutable system where users can granularly control access to their sensitive health data.

The proposed architecture implements a three-tier security model that ensures data are encrypted, fragmented, and accessible only to authenticated parties with explicit user authorization. Through extensive prototyping and security analysis, we demonstrate how our framework achieves GDPR compliance. The system provides comprehensive audit trails through tamper-proof access logs that enable both users and regulatory authorities to verify compliance with data legislation, creating accountability mechanisms previously unavailable in Femtech applications. This work contributes a practical implementation path for enhancing privacy in women's health technologies while establishing a foundation for responsible innovation in this sensitive domain.

CCS Concepts: • **Security and privacy** → **Information accountability and usage control**; • **Information systems** → *Data management systems*; Distributed storage; • **Human-centered computing** → *Human computer interaction (HCI)*.

Keywords: Blockchain, Smart Contracts, Consent Management, Intimate Data, Femtech

ACM Reference Format:
Larissa Tomaz, David R. Matos, and Teresa Almeida. 2018. Trust Through Transparency: Blockchain for Consent and Accountability in Femtech Applications. *ACM Trans. Graph.* 37, 4, Article 111 (August 2018), 9 pages. https://doi.org/XXXXXXX.XXXXXXX

1 Introduction

In today's data-driven society, a rising number of people are gaining interest in the quantified self movement [Lupton 2016], a movement focused on pursuing self-knowledge through numbers. Modern self-tracking devices and applications allow users to record, measure, and gain new information about their bodies. This technological advancement is especially empowering to historically marginalized groups in the health sector, such as women, since these tools can generate insights into their stigmatized and under-researched health issues [Kemble et al. 2022; Tuana 2006]. It serves as a means to validate and communicate health situations that have been traditionally invisible or challenging to convey to healthcare providers [Perez 2019]. This rise of interest in self-tracking coincides with an increasing focus on women's health, a field that has traditionally lacked investment and innovation. This intersection of health and technology has given rise to a new category of business dedicated to women, commonly referred to as Femtech [Tin 2016].

The rapidly expanding and relatively unregulated Femtech market, which reached a valuation of $40.2 billion in 2020 and is projected to exceed $75 billion by 2025 [& Intelligence 2021], has seen the emergence of numerous companies addressing the diverse health needs of women, with over 1300 Femtech companies classified across 10 subsectors, including

Authors' Contact Information: Larissa Tomaz, larissa.tomaz@tecnico.ulisboa.pt; David R. Matos, david.r.matos@tecnico.ulisboa.pt, INESC-ID, Instituto Superior Técnico, Universidade de Lisboa, Lisbon, Portugal; Teresa Almeida, ITI/LARSyS, Instituto Superior Técnico, Universidade de Lisboa, Lisbon, Portugal, teresa.almeida@tecnico.ulisboa.pt.

ACM 1557-7368/2018/8-ART111
https://doi.org/XXXXXXX.XXXXXXX

Menstrual Health, Reproductive Health, Mental Health, and Sexual Health [& Intelligence 2021]. This growth has been driven by a demand to address the historically underserved and underrepresented segments of the population, with a focus on breaking taboos surrounding sensitive topics. However, the industry faces significant challenges, particularly regarding data privacy and security. For instance, in 2020, the period and fertility tracking app Glow[1] was investigated by Consumer Reports[2], revealing several security vulnerabilities that exposed users to risks from stalkers, identity thieves, and online bullies [Beilinson 2020; Gilman 2021; Scatterday 2021]. The lack of specialized regulatory authorities and the sensitive nature of the information collected by Femtech companies further complicate efforts to address these privacy concerns, highlighting the need for more robust regulatory frameworks [Rosas 2019].

There are still issues to be discussed regarding the privacy and security practices of Femtech applications. Central to this discussion is the question of data ownership and user agency: to what extent are users able to control what is done to their intimate data, and how can their privacy be guaranteed and actively monitored by them? Additionally, is it possible to utilize women's health data to bridge the gender gap in healthcare while still safeguarding user privacy? Regarding regulation, how can the Femtech industry be regulated to safeguard user data, while also encouraging innovation and not hindering new Femtech companies' growth? Such questions must be carefully considered and new solutions must be studied in order to address these challenges.

This is where blockchain could emerge as a powerful tool to address some of these questions. Over recent years, various solutions leveraging blockchain technology have been proposed for consent management [Alhajri et al. 2022; Genestier et al. 2017; Mamo et al. 2020]. The transparency provided by blockchain solutions is one of the features that could be explored to enhance the trust of users in using Femtech applications.

Our research raised the following research questions:

RQ1 How can the implementation of blockchain and smart contracts in Femtech applications improve the autonomy and control of users over their intimate data?

RQ2 Is it feasible to develop a secure Femtech application with strong authenticity, integrity, and confidentiality features by leveraging blockchain and smart contracts?

RQ3 Can the adoption of blockchain and smart contracts in Femtech applications effectively address the privacy and security concerns associated with women's intimate data?

In light of these considerations, this paper presents PrivacHer, a Femtech system that incorporates blockchain and smart contracts[3] to provide a transparent and empowering tool for users to effectively monitor and control the use of their sensitive data. PrivacHerenables users to easily request data deletion, view the specific data stored about them, and update sharing and consent preferences in a user-friendly manner. The privacy aspect is carefully considered, and the design of the application ensures the implementation of robust confidentiality mechanisms. Additionally, auditability is achieved through an immutable log of data access that can be reviewed by regulatory authorities to ensure compliance and accountability.

To demonstrate the application of PrivacHer, we focus on the area of digital contraception and use the Natural Cycles app – a fertility tracking app that helps users monitor their menstrual cycles and predict ovulation using basal body temperature and cycle data – as a case study to guide the development of the proposed solution. By analyzing which data is collected from users and how they can interact with their data and privacy settings, the goal is to design a Femtech solution that enhances data control and privacy for users in a similar context. Additionally, we propose mechanisms for regulatory authorities to verify the service's compliance with data privacy regulations through transparent and auditable logs.

2 Background

2.1 Femtech and the Challenge of Intimate Data

Femtech, a term coined by Ida Tin in 2016, refers to technology-based products and services that address women's health needs, including menstruation, fertility, pregnancy, menopause, and sexual health. These applications often rely on sensitive personal data, sometimes categorized as intimate data, which includes physiological, behavioral, and biometric information. The mishandling or unauthorized sharing of such data poses significant privacy risks, ranging from identity theft to workplace discrimination.

2.2 Consent and Data Sovereignty

In digital health contexts, consent refers to a user's voluntary agreement to allow processing of their personal data. Effective consent must be informed, explicit, and revocable. Given that users often have limited visibility into how their data is used and shared, mechanisms that allow dynamic, fine-grained control over consent are essential for ensuring user autonomy and compliance with data protection regulations like the GDPR (General Data Protection Regulation) [European Parliament and Council of the European Union 2016a].

[1] https://glowing.com/

[2] https://www.consumerreports.org/

[3] self-executing programs that automatically enforce and execute agreements based on predefined rules

2.3 Blockchain: Definitions and Key Properties

Blockchain is a form of distributed ledger technology (DLT) that maintains a secure, decentralized, and immutable record of transactions. Unlike traditional databases controlled by a single authority, blockchain networks consist of multiple nodes that collectively validate and store data. The key properties of blockchain relevant to our work include:

- **Immutability**: Once data is written to a blockchain, it cannot be altered retroactively without consensus from the network. This is crucial for maintaining tamper-proof audit logs of consent and data access events.
- **Transparency**: Blockchain provides a publicly verifiable history of transactions, which can be selectively exposed to users or regulators to validate compliance.
- **Decentralization**: Control over data and transaction validation is distributed across the network, reducing dependency on a single trusted authority.
- **Auditability**: The permanent and traceable nature of blockchain records makes it ideal for verifying user consents and detecting unauthorized data accesses.
- **Smart Contract**s: Self-executing code stored on the blockchain that enforces rules and automates processes. In our case, smart contracts validate whether data access requests conform to stored user consents.

3 PrivacHer- A Consent-First Femtech Platform

PrivacHeris a consent-first femtech platform powered by smart sontracts. The proposed solution aims to address some of the problems that Femtech applications are currently facing. The system aims to give users control over their sensitive data, offering transparency in data transactions, and enabling regulatory authorities to audit third-party data accesses.

3.1 Requirements

The system requirements are divided into two categories:

- **Functional Requirements:** The system must support explicit consent management, provide users with the ability to update consent, maintain a permanent log of data access, and validate consent before processing any user data.
- **Security Requirements:** The system must ensure authentication, protect data integrity, maintain confidentiality, provide auditability, and secure communications. This ensures that only authorized parties can access user data and that all interactions with the system are secure and traceable.

3.2 Solution Overview

The diagram in figure 1 shows an overview of the proposed solution, which involves three primary interaction types: consent-related actions, data consultations, and data operations. The process is characterized by the following components:

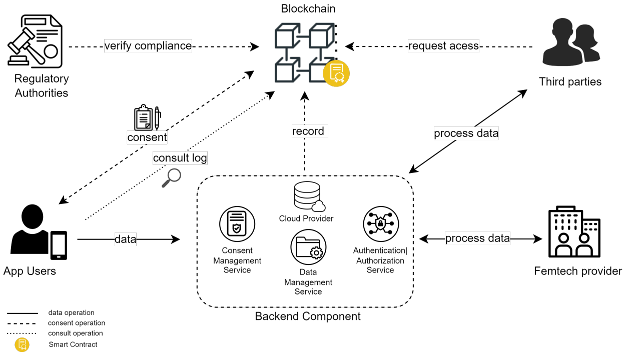


Figure 1. Solution Overview

- **Femtech data:** When the user uses the application, their intimate data is securely transmitted to the system and subsequently stored within a cloud service provider. This ensures that sensitive data is encrypted and protected during both transfer and storage.
- **Consent management:** All consents related to the user's data are immutably recorded on a blockchain ledger. This provides a secure and transparent mechanism for tracking user permissions and data usage agreements.
- **Data handling and audit trail:** Every process involving the user's data is logged on the blockchain. This creates an audit trail that can be reviewed by the user or regulatory bodies to verify who accessed the data, for what purpose, and when.
- **Compliance validation via Smart Contracts:** Smart contracts are responsible for verifying compliance with the consents on record. They check the validity of consents, such as their expiration time or any recent updates made by the user concerning their data.

Authentication & Authorization Service: Authenticates the entity requesting access to the data and returns an access token if the entity has authorization to access the requested data.

- **Registration:** Registers a new user into the system, defining their role and the type of organization they belong to.
- **Authentication:** Authenticates users in the system by validating their credentials. Once validated, an access token is generated to be used by users in their subsequent requests to the system.
- **Authorization:** Verifies users' roles through the access token issued in the authentication phase. There will be five different roles in the system, each with different permissions regarding data access: Femtech Service Providers, Regulatory Authorities, Healthcare

Providers, Femtech Users, and Researchers.

Data Management Service: Stores and sends user data according to the permissions of the accessing party. Whenever an authorized entity makes a request to this service and the service returns the data, such access is recorded on the blockchain, along with the reason for the data usage by the requesting entity.

- **Set User Data:** Stores user data. The data are stored in a distributed storage solution hosted by a cloud provider. A pointer is created and stored on the blockchain ledger, referencing the data stored off-chain.
- **Fetch User Data:** Fetches user Femtech data that was stored previously. Every time data is accessed, the system registers the access in a blockchain ledger, thereby creating an access log.

Consent Management Service: Handles users' consent requests and responses. It is responsible for recording on the blockchain all information related to consent provided by users.

- **Set User Consent:** Stores user consent. The consent data are stored on the blockchain ledger.
- **Fetch User Consent:** Fetches user consent information that was stored previously.
- **Update User Consent:** Updates user consent information that was stored previously.
- **Fetch User Consent History:** Fetches a history of user consent versions.
- **Validate Data Processing:** Validates the entity's permission to access and perform the requested data processing. This validation is done by a smart contract that verifies permission through the stored consent information provided by the user.

The system architecture includes an API gateway that routes user requests to the appropriate microservice. A message broker (RabbitMQ) is used for inter-service communication, ensuring reliable message delivery even if a service is temporarily unavailable. The backend interacts with both off-chain and on-chain storage, with user data stored off-chain in an encrypted MongoDB database and only references recorded on the blockchain. Figure 3 shows the high-level architecture of the solution.

The frontend interface is designed to be user-friendly, incorporating visual privacy policies to simplify consent management. The design is demonstrated with a real-world application (Natural Cycles) to illustrate how the proposed model could be applied as presented in Figure 4.

The system uses a consortium blockchain network for controlled, secure access to sensitive Femtech data. Only authorized entities can access the data, reducing the risk of breaches. Key information recorded on the blockchain includes:

- Data access logs (specifying entity, date, and reasons for access)
- Consent records (defining the user consent settings)

The blockchain component is built on the Hyperledger Fabric framework, a permissioned ledger. The consortium consists of various organizations, including: the organization representing the consent management system, Femtech service providers, regulatory authorities (such as CNPD and Infarmed), research institutes and other third-party entities interested in the user data. The Hyperledger Service is implemented using the Hyperledger Fabric SDK, which provides the necessary tools to connect to the Fabric network, submit transactions, and query the ledger. It maintains a wallet to store user identities and uses the Fabric Gateway to establish a connection, retrieve contracts, and execute transactions.

The Hyperledger Service interacts with different channels and contracts based on the requirements of each microservice:

- **Registry Channel (registry contract):** Manages user registration and identity operations, such as creating, deleting, and querying user profiles.
- **Consent Channel (consent contract):** Handles consent management, including storing, updating, and retrieving user consent records.
- **Data Channel (data contract):** Manages user data operations, such as updating, retrieving, and deleting user information. Additionally, it records data access logs, capturing details about each access request, including the requesting entity and the purpose of access.

The sequence diagrams in Figures 2 and 5 illustrate the interaction flow between the system—ClientApp, API Gateway, Registry Service, Consent Manager, and Data Service—during user registration, consent submission, and data retrieval. The process begins when a user registers via the ClientApp, which sends a RegisterUser request through the API Gateway to the Registry Service. Upon successful user creation, the ClientApp sends a SetConsent request, which triggers the creation of a consent record via the Consent Manager, after authenticating the user. Once consent is recorded, the user can request their data using GetUserData. This request is validated by the Consent Manager, which first authenticates the user and verifies consent before fetching the data from the Data Service. Each interaction ensures proper authentication and consent validation, reflecting the system's emphasis on secure, consent-driven data access.

4 Evaluation

This section presents the evaluation of the developed proof-of-concept, focusing on functional and performance testing.

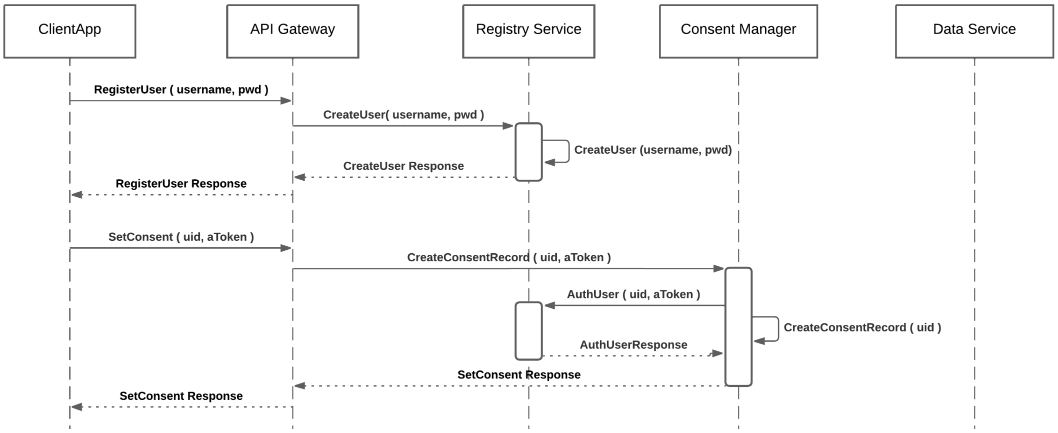


Figure 2. Sequence diagram with the Register and set consent operations of PrivacHer.

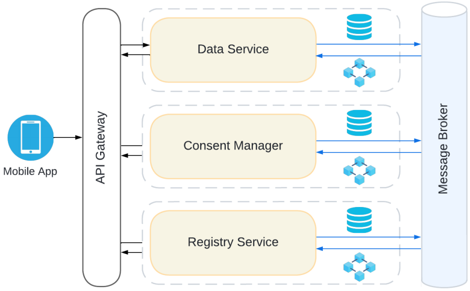
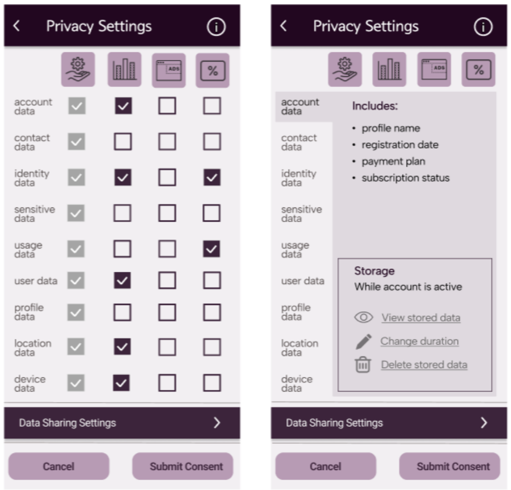


Figure 3. Architecture Overview


Privacy Settings

			ADS	%
account data	✓	☑	□	□
contact data	✓	□	□	□
identity data	✓	☑	□	☑
sensitive data	✓	□	□	□
usage data	✓	□	□	☑
user data	✓	☑	□	□
profile data	✓	□	□	□
location data	✓	☑	□	□
device data	✓	☑	□	□

Privacy Settings

account data
contact data
identity data
sensitive data
usage data
user data
profile data
location data
device data

Includes:

- profile name
- registration date
- payment plan
- subscription status

Storage
While account is active

Figure 4. Visual privacy example from the Natural Cycle app.

4.1 Functional Evaluation

Each system component was tested to ensure correct behavior both independently and in communication with other services. Functional tests covered user registration, consent management, data submission, and data retrieval, ensuring each operation performed as expected.

End-to-end workflow tests simulated real-world use cases, such as a user registering, submitting data, updating consent preferences, and retrieving access logs. These tests validated the system's behavior in handling typical interactions between users, service providers, and regulatory authorities.

4.2 Performance Evaluation

The system's performance was tested using Locust, a load testing tool, to simulate multiple users. The key performance metrics were latency and throughput, measuring how the system responds under increasing load. Figure 6 shows the performance charts of a test that simulates users interacting with the system while performing different operations.

The system handled the increasing load without failures but experienced rising response times as the number of users grew. Complex operations, such as data retrieval, exhibited the highest latency due to interactions between multiple microservices, the database, and the blockchain. The Get Data operation showed the highest latency, peaking at 13,000 ms, which highlights areas for optimization, particularly around blockchain and database performance.

5 Related Work

5.1 Privacy and Security in the Femtech field

Privacy in Femtech services has been discussed in the literature [Alfawzan et al. 2022; Erickson et al. 2022; Felizi and Varon 2017; Mehrnezhad and Almeida 2021; Mehrnezhad et al. 2022; Shipp and Blasco 2020]. Regarding to privacy policies, both [Alfawzan et al. 2022] and [Shipp and Blasco 2020] state that although all the reviewed apps collect personal and intimate data, the privacy policy was not always available to the users. Another concern is related to the complexity of the language used. Shipp et al. [Shipp and Blasco 2020] analyzed the language accessibility in the privacy policies

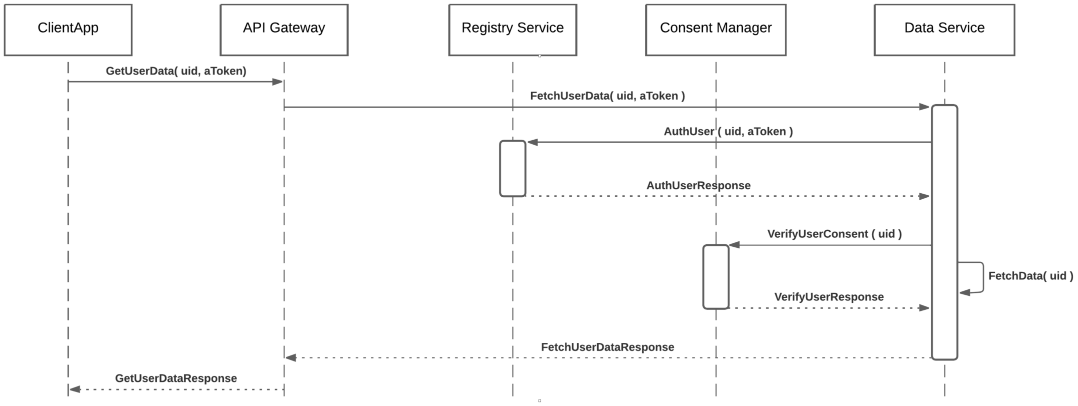


Figure 5. Sequence diagram of the `get data` operation in PrivacHer.

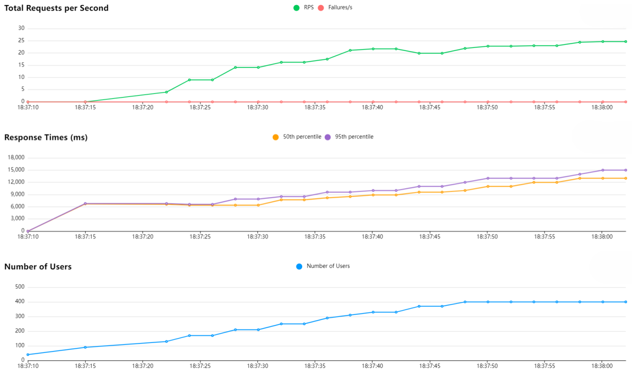


Figure 6. Performance test with different operations

of 30 menstruapps [4]. The researchers point out that many of these policies adopted language that was misleading in some way, while others were excessively lengthy, resulting in users remaining uninformed.

In [Mehrnezhad and Almeida 2021] the authors evaluated the privacy notices of 30 fertility apps. Among the applications analyzed, over half adopted a "take it or leave it" stance, an approach the authors consider inappropriate as it does not provide users with a genuine choice. The authors also highlight practices inconsistent with the General Data Protection Regulation (GDPR), such as failing to present a clear option for rejection or highlighting the accept option over the reject alternative and other options.

Turning to data-sharing practices, Alfawzan et al. [Alfawzan et al. 2022] report that 87% of the apps reviewed in their research shared user data with third parties, while in a distinct analysis [Shipp and Blasco 2020], Ship et al. mention that all analyzed apps in their study transmitted device data to Facebook servers. Some apps even neglected to require explicit consent before sharing user data or failed to provide any information about it in their privacy policies.

In [Mehrnezhad et al. 2022], the authors highlight real-world threats of data misuse, including workplace monitoring. For example, the Ovia app, promoted by employers for health tracking, shares intimate user data with companies, potentially enabling discrimination and harassment [Brown 2021; Gilman 2021].

The threats arising from the misuse and abuse of Femtech data are amplified by the failure to recognize the sensitivity of such information. Many app developers do not recognize intimate data as especially sensitive, only mentioning standard PII in their privacy policies [Shipp and Blasco 2020]. This oversight is also reflected in the law, as most Femtech companies fail to be classified as HIPAA Covered Entities [Rosas 2019], and fertility-related data is not explicitly mentioned in the ICO guidelines or in the GDPR [McMillan 2022]. Such facts create a gray area, making it easier for Femtech companies to adopt less rigid attitudes regarding the security and privacy of their users' data [Rosas 2019].

Rosas [Rosas 2019] highlights how weak regulations allow companies to neglect basic security measures like encryption. Supporting this, Alfawzan et al. [Alfawzan et al. 2022] found that over half of 23 analyzed apps failed to explain data security practices, and all enabled behavioral tracking. Notably, Flo once stated it could not "guarantee the security of the application." These cases underscore the urgent need for Femtech to prioritize transparency and user data protection.

5.2 Consent Receipts

Data protection laws, such as the GDPR [European Parliament and Council of the European Union 2016a], emphasize not only the importance of obtaining consent but also the necessity of being able to prove it. According to Article 7, service providers must be able to demonstrate that consent was obtained lawfully, freely, and transparently [European Parliament and Council of the European Union 2016b]. Other

[4] Menstruapps are mobile applications designed to help users monitor menstrual cycles, track symptoms, and predict fertility windows.

regulatory authorities, such as the UK's ICO, advise controllers to record consent, "you must have an effective audit trail of how and when consent was given, so you can provide evidence if challenged", and also to "keep a master copy of the document or data capture form containing the consent statement in use at that time" [Information Commissioner's Office 2023].

Some studies [Jesus 2020; Jesus and Pandit 2022; Nati 2018; Pandit et al. 2024; Styliari and Nati 2016] propose the use of consent receipts—artifacts that record data transactions similarly to conventional shopping receipts. These artifacts encourage accountability and transparency in consent management, benefiting both organizations and users.

Jesus et al. [Jesus and Pandit 2022] analyze the feasibility of consent receipts, outlining their requirements, benefits, and real-world applications in web interactions like cookie banners. They also address challenges in IoT contexts lacking interfaces, using Alexa as an example of consent via audio.

A major challenge in adopting consent receipts is the absence of a standard. The Kantara Consent Receipt Specification [Initiative 2018] addresses this by proposing an interoperable, human-readable, JSON-based model. It includes links to privacy policies, details on data collection and use, and a unique ID to serve as a shared reference for Controllers and Data Subjects.

Alongside the Kantara Initiative, ISO/IEC TS 27560:2023 [International Organization for Standardization (ISO) 2023] provides guidance on consent records, including lifecycle management and minimal metadata requirements. As consent receipts lack strict legal definitions, the standard allows implementation flexibility. Pandit et al. [Pandit et al. 2024] explore how ISO 27560 can support GDPR compliance through machine-readable consent records, promoting adoption among stakeholders.

Styliari et al. [Styliari and Nati 2016] used an HCI approach to design a consent receipt prototype through interviews and a participatory design workshop. Their study highlights users' desire for clearer data practices and suggests that consent receipts can enhance user trust and support GDPR compliance.

5.3 Personal Health Records

A Personal Health Record (PHR) is an electronic application that allows individuals to manage and access their own personal health data [Tang et al. 2006]. Unlike EHR, which are controlled and maintained by institutions such as hospitals or clinics [Wang et al. 2003], PHR give individuals more control over their own health data, placing the responsibility for data management in the hands of users [Tang et al. 2006]. Recent works have explored blockchain-based solutions for developing PHR [Cernian et al. 2020; Leeming et al. 2019; Pawar et al. 2022; Thwin and Vasupongayya 2019].

Leeming et al. [Leeming et al. 2019] analyzed blockchain-based healthcare solutions and identified key features that also inform our approach. Health data is stored off-chain, with only metadata (e.g., ownership, access) on-chain to reduce costs and support GDPR compliance. Blockchain enables immutable audit trails, enhancing transparency and accountability. Consent mechanisms are central, giving users control over data access through smart contracts and identity management. For secondary uses—like research or marketing—consent remains critical, with some systems exploring data monetization. Blockchain also supports secure, interoperable telehealth solutions beyond traditional EHRs.

Additionally to the aforementioned analysis, Leeming et al. [Leeming et al. 2019] also proposed a reference architecture for a blockchain-based PHR solution, named Ledger of Me. This solution focuses on recording blockchain meta-information about entities and their interactions. Although the main goal of the system goes beyond consent and data sharing, it also serves as a support platform for the users within the healthcare system. Some of its features include triggering medication reminders and registering medical prescriptions.

In a similar way, Thwin et al. [Thwin and Vasupongayya 2019] also propose a blockchain-based system for PHR, that emphasizes privacy and tamper resistance. The proposed model aims to ensure data integrity and privacy, employing cryptographic techniques and proxy re-encryption for secure data sharing and consent management. The system includes a gateway server that maintains an access log, serving as an audit mechanism.

With a different focus, Cernian et al. [Cernian et al. 2020] developed PatientDataChain, a patient-centered model focusing on integrating heterogeneous data sources. The system is built over ModexBCDB, a technology that adds a blockchain layer to an existing database. With this solution, it becomes easy to integrate PatientDataChain with different medical databases and EHR.

5.4 Consent Management

Consent is an essential instrument for individuals to exercise their right to autonomy and control over their personal data. According to the GDPR [Voigt and Von dem Bussche 2017], the prevailing data protection legislation in Europe, companies are required to obtain consent for the use and processing of data in an explicit and unambiguous way. Over recent years, various solutions leveraging blockchain technology have been proposed for consent management [Genestier et al. 2017; Mamo et al. 2020]. Numerous studies have emphasized the significance of transforming consent from a one-time agreement into a dynamic process, enabling individuals to adjust their preferences over time [Goncharov et al. 2022; Kaye et al. 2015; Mamo et al. 2020; Steinsbekk et al. 2013].

Genestier et al. [Genestier et al. 2017] propose a blockchain-based consent management system for eHealth, where patients control access to their data via smart contracts. Consent is stored in a consortium blockchain and verified by a dedicated server before data access. While offering auditability, the approach lacks details on data protection and access control.

In contrast, the Dwarna project [Mamo et al. 2020], tailored for the biobanking sector in Malta, focuses on managing consent from research participants for their biospecimen data in research contexts. All stakeholders interact through a web portal supported by a Hyperledger Composer blockchain framework. The authors reinforce the importance of trust when dealing with sensitive information, such as genomic data, highlighting fundamental properties like accountability and transparency.

[Ameyed et al. 2021] presents a multi-blockchain-based model that emphasizes user trust by enhancing transparency. The system relies on a permissioned blockchain, enabling data controllers to request access to stored data. The data subjects, who own the data, retain the authority to grant or deny access to their personal data. Unauthorized attempts by third parties to access data without consent contribute to a non-repudiation system.

Consentio [Agarwal et al. 2020] is a consent management system based on Hyperledger Fabric. Data is stored off-chain, while the respective consent to access it is persisted on-chain. Data management is handled by third-party data stores, assumed to be trusted, while consent management is dealt with by the proposed system. Data access is recorded on the ledger, serving as an auditable trail.

ADvoCATE [Rantos et al. 2019] is a cloud service platform that consists of three main components: a consent management component, a consent notary component, and an intelligence component. The consent management component manages users' consent regarding their personal data, utilizing the privacy ontology proposed by to ensure GDPR compliance.

6 Conclusion

This paper presented a Femtech consent management system leveraging blockchain and smart contracts to enhance user control, transparency, and security in managing intimate data.

We revisit the research questions that guided our research:

RQ1 How can blockchain and smart contracts improve user control over intimate data?
Our solution ensures decentralization, preventing single-entity control which empowers users to manage their data compared to existing Femtech systems.

RQ2 Is it feasible to develop a secure Femtech app with blockchain and smart contracts?
A proof-of-concept demonstrated feasibility, with simple authentication and blockchain ensuring data integrity and confidentiality. Though sensitive data is stored off-chain, the system needs optimization for scalability due to high latency under heavy load.

RQ3 Can blockchain and smart contracts address privacy concerns in Femtech?
Blockchain offers an immutable record of data interactions, while smart contracts enforce user consent. These technologies address privacy and security concerns but require further user testing to fully validate their effectiveness.

In conclusion, this work introduces a novel approach to securing sensitive data in Femtech, using blockchain and smart contracts to empower users and enhance privacy, security, and transparency in digital health applications. Future improvements will focus on performance and scalability.

Acknowledgments

This work was financially supported by Project Blockchain.PT – Decentralize Portugal with Blockchain Agenda, (Project no 51), WP1: Agriculture and Agri-food, Call no 02/C05-i01.01/2022, funded by the Portuguese Recovery and Resilience Program (PPR), The Portuguese Republic and The European Union (EU) under the framework of Next Generation EU Program; by the European Union's Horizon 2020 research and innovation program under grant agreement No 952226, project BIG (Enhancing the research and innovation potential of Técnico through Blockchain technologies and design Innovation for social Good); and by the Fundação para a Ciência e Tecnologia (FCT), Portugal through projects UIDB/50021/2020 (INESC-ID) and 2024.07494.IACDC (WELL).

References

Arizton Advisory & Intelligence. 2021. Femtech market size to reach revenues of around USD 75.74 billion by 2026 - Arizton. https://www.prnewswire.com/news-releases/femtech-market-size-to-reach-revenues-of-around-usd-75-74-billion-by-2026--arizton-301303872.html

Rishav Raj Agarwal, Dhruv Kumar, Lukasz Golab, and Srinivasan Keshav. 2020. Consentio: Managing consent to data access using permissioned blockchains. In *2020 ieee international conference on blockchain and cryptocurrency (icbc)*. IEEE, 1–9.

Najd Alfawzan, Markus Christen, Giovanni Spitale, Nikola Biller-Andorno, et al. 2022. Privacy, data sharing, and data security policies of women's mhealth apps: scoping review and content analysis. *JMIR mHealth and uHealth* 10, 5 (2022), e33735.

May Alhajri, Carsten Rudolph, and Ahmad Salehi Shahraki. 2022. A blockchain-based consent mechanism for access to fitness data in the healthcare context. *IEEE Access* 10 (2022), 22960–22979.

Darine Ameyed, Fehmi Jaafar, Francis Charette-Migneault, and Mohamed Cheriet. 2021. Blockchain based model for consent management and data transparency assurance. In *2021 IEEE 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C)*. IEEE, 1050–1059.

Jerry Beilinson. 2020. Glow pregnancy app exposed women to privacy threats, Consumer Reports finds. https://www.consumerreports.org/electronics-computers/mobile-security-software/glow-pregnancy-app-exposed-women-to-privacy-threats-a1100919965/

Elizabeth A Brown. 2021. The femtech paradox: How workplace monitoring threatens women's equity. *Jurimetrics* 61, 3 (2021), 289–329.

Alexandra Cernian, Bogdan Tiganoaia, Ioan Sacala, Adrian Pavel, and Alin Iftemi. 2020. Patientdatachain: A blockchain-based approach to integrate personal health records. *Sensors* 20, 22 (2020), 6538.

Jacob Erickson, Jewel Y Yuzon, and Tamara Bonaci. 2022. What You Do Not Expect When You Are Expecting: Privacy Analysis of Femtech. *IEEE Transactions on Technology and Society* 3, 2 (2022), 121–131.

European Parliament and Council of the European Union. 2016a. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj. Accessed: date-of-access.

European Parliament and Council of the European Union. 2016b. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj. Article 7, Conditions for consent.

N Felizi and J Varon. 2017. MENSTRUAPPS – how to turn your period into money (for others). https://chupadados.codingrights.org/en/menstruapps-como-transformar-sua-menstruacao-em-dinheiro-para-os-outros-2/

Philippe Genestier, Sajida Zouarhi, Pascal Limeux, David Excoffier, Alain Prola, Stephane Sandon, and Jean-Marc Temerson. 2017. Blockchain for consent management in the ehealth environment: A nugget for privacy and security challenges. *Journal of the International Society for Telemedicine and eHealth* 5 (2017), GKR–e24.

Michele Estrin Gilman. 2021. Periods for profit and the rise of menstrual surveillance. *Colum. J. Gender & L.* 41 (2021), 100.

Liza Goncharov, Hanna Suominen, and Matthew Cook. 2022. Dynamic consent and personalised medicine. *The Medical Journal of Australia* 216, 11 (2022), 547.

Information Commissioner's Office. 2023. How Should We Obtain, Record and Manage Consent. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/how-should-we-obtain-record-and-manage-consent/how4. Accessed on: 2024-07-12.

Kantara Initiative. 2018. Consent Receipt Specification. https://kantara.atlassian.net/wiki/spaces/archive/pages/3508790/Consent+Receipt+Specification. Accessed on: 2024-06-12.

International Organization for Standardization (ISO). 2023. ISO/IEC TS 27560:2023 - Privacy and data protection – Framework for managing and communicating privacy consent. https://www.iso.org/obp/ui/en/iso:std:iso-iec:ts:27560:ed-1:v1:en. Accessed on: 2024-07-12.

Vitor Jesus. 2020. Towards an accountable web of personal information: The web-of-receipts. *IEEE Access* 8 (2020), 25383–25394.

Vitor Jesus and Harshvardhan J Pandit. 2022. Consent receipts for a usable and auditable web of personal data. *IEEE Access* 10 (2022), 28545–28563.

Jane Kaye, Edgar A Whitley, David Lund, Michael Morrison, Harriet Teare, and Karen Melham. 2015. Dynamic consent: a patient interface for twenty-first century research networks. *European journal of human genetics* 23, 2 (2015), 141–146.

Emma Kemble, Lucy Pérez, Valentina Sartori, Gila Tolub, and Alice Zheng. 2022. Unlocking opportunities in women's healthcare. *McKinsey & Company* (Feb 2022). https://www.mckinsey.com/industries/healthcare/our-insights/unlocking-opportunities-in-womens-healthcare

Gary Leeming, James Cunningham, and John Ainsworth. 2019. A ledger of me: personalizing healthcare using blockchain technology. *Frontiers in medicine* 6 (2019), 171.

Deborah Lupton. 2016. *The quantified self.* John Wiley & Sons.

Nicholas Mamo, Gillian M Martin, Maria Desira, Bridget Ellul, and Jean-Paul Ebejer. 2020. Dwarna: a blockchain solution for dynamic consent in biobanking. *European Journal of Human Genetics* 28, 5 (2020), 609–626.

Catriona McMillan. 2022. Monitoring Female Fertility Through 'Femtech': The Need for a Whole-System Approach to Regulation. *Medical Law Review* 30, 3 (2022), 410–433.

Maryam Mehrnezhad and Teresa Almeida. 2021. Caring for intimate data in fertility technologies. In *Proceedings of the 2021 CHI conference on human factors in computing systems.* 1–11.

Maryam Mehrnezhad, Laura Shipp, Teresa Almeida, and Ehsan Toreini. 2022. Vision: Too Little too Late? Do the Risks of FemTech already Outweigh the Benefits?. In *Proceedings of the 2022 European Symposium on Usable Security.* 145–150.

Michele Nati. 2018. Personal Data Receipts: How transparency increases consumer trust. *Catapult Digital, London, UK, Tech. Rep* (2018).

Harshvardhan J Pandit, Jan Lindquist, and Georg P Krog. 2024. Implementing ISO/IEC TS 27560: 2023 Consent Records and Receipts for GDPR and DGA. *arXiv preprint arXiv:2405.04528* (2024).

Pravin Pawar, Neeraj Parolia, Sameer Shinde, Thierry Oscar Edoh, and Madhusudan Singh. 2022. eHealthChain—a blockchain-based personal health information management system. *Annals of Telecommunications* (2022), 1–13.

Caroline Criado Perez. 2019. *INVISIBLE WOMEN: Data bias in a world designed for men.* Abrams Press.

Konstantinos Rantos, George Drosatos, Konstantinos Demertzis, Christos Ilioudis, Alexandros Papanikolaou, and Antonios Kritsas. 2019. ADvoCATE: a consent management platform for personal data processing in the IoT using blockchain technology. In *Innovative Security Solutions for Information Technology and Communications: 11th International Conference, SecITC 2018, Bucharest, Romania, November 8–9, 2018, Revised Selected Papers 11.* Springer, 300–313.

Celia Rosas. 2019. The future is femtech: Privacy and data security issues surrounding femtech applications. *Hastings Bus. LJ* 15 (2019), 319.

Allysan Scatterday. 2021. This is no ovary-action: Femtech apps need stronger regulations to protect data and advance public health goals. *NCJL & Tech.* 23 (2021), 636.

Laura Shipp and Jorge Blasco. 2020. How private is your period?: A systematic analysis of menstrual app privacy policies. *Proc. Priv. Enhancing Technol.* 2020, 4 (2020), 491–510.

Kristin Solum Steinsbekk, Bjørn Kåre Myskja, and Berge Solberg. 2013. Broad consent versus dynamic consent in biobank research: is passive participation an ethical problem? *European Journal of Human Genetics* 21, 9 (2013), 897–902.

Tatiana C Styliari and Michele Nati. 2016. Researching the Transparency of Personal Data Sharing: Designing a Consent Receipt. *Digital Catapult* (2016).

Paul C Tang, Joan S Ash, David W Bates, J Marc Overhage, and Daniel Z Sands. 2006. Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption. *Journal of the American Medical Informatics Association* 13, 2 (2006), 121–126.

Thein Than Thwin and Sangsuree Vasupongayya. 2019. Blockchain-based access control model to preserve privacy for personal health record systems. *Security and Communication Networks* 2019 (2019).

Ida Tin. 2016. The rise of a new category: Femtech. https://helloclue.com/articles/culture/rise-new-category-femtech

Nancy Tuana. 2006. The speculum of ignorance: The women's health movement and epistemologies of ignorance. *Hypatia* 21, 3 (2006), 1–19.

Paul Voigt and Axel Von dem Bussche. 2017. The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing* 10, 3152676 (2017), 10–5555.

Samuel J Wang, Blackford Middleton, Lisa A Prosser, Christiana G Bardon, Cynthia D Spurr, Patricia J Carchidi, Anne F Kittler, Robert C Goldszer, David G Fairchild, Andrew J Sussman, et al. 2003. A cost-benefit analysis of electronic medical records in primary care. *The American journal of medicine* 114, 5 (2003), 397–403.