WELL

Wallet for ELectronic heaLth Records

White Paper — Technical Overview & Research Contributions

FCT Grant 2024.07494.IACDC

WELL: A Decentralized Wallet for Electronic Health Records

Leveraging Blockchain, Cloud-of-Clouds, and Self-Sovereign Identity for Patient-Centric Healthcare

---

David R. Matos **António Rito Silva** **Beatriz Militão**
Diogo Melita **Daniel Nunes** **Daniela Camarinha**

INESC-ID, Instituto Superior Técnico, Universidade de Lisboa

{david.r.matos, antonio.silva, beatriz.militao, diogo.melita, daniel.m.nunes, daniela.camarinha}@tecnico.ulisboa.pt

Project: WELL — Wallet for ELectronic heaLth records
Grant: FCT 2024.07494.IACDC (IACDC Programme)
Principal contractos: INESC-ID, Instituto Superior Técnico, Universidade de Lisboa
Duration: March 2025 – January 2026 (11 months)
Total Budget: €42,679.74

Version 1.0 — January 2026

Abstract

Electronic Health Records (EHRs) are critical assets in modern healthcare, yet their management remains fragmented, insecure, and inaccessible across institutions. The WELL project proposes a decentralised patient-centric wallet for managing EHRs, combining a cloud-of-clouds storage backend with a blockchain-based access control layer and Self-Sovereign Identity (SSI). Through the development of the WELL Repository and WELL Wallet, the project delivers a system where patients own and control their clinical data, sharing it selectively with healthcare providers, insurers, and researchers. This white paper presents the motivation, architecture, implementation outcomes, and research contributions of WELL, including the Well Wallet mobile application, the Well Repository backend, and a consent management system for patient data. Experimental results demonstrate the feasibility of using Layer 2 blockchain networks for low-latency EHR access logging, and validate the scalability of the Well Repository backend for national-level healthcare deployments.

Contents

1 Introduction

Healthcare systems worldwide are undergoing digital transformation, with Electronic Health Records (EHRs) at the centre of this shift. EHRs consolidate a patient's clinical history — diagnoses, medications, lab results, imaging studies — into a digital format accessible across care settings. Yet, despite three decades of digitisation effort, the promise of seamless, patient-controlled health data remains largely unrealised.

In Portugal, the National Health Service (SNS) centralises public-sector EHRs through SPMS[1], while private institutions operate isolated silos with no shared interoperability protocol. This fragmentation creates tangible clinical risk: a patient receiving emergency care outside their usual network may arrive with an inaccessible history. Simultaneously, the GDPR [6] classifies EHRs as personal data and mandates that patients retain rights of access and erasure — rights that current centralised systems structurally undermine.

The WELL project (Wallet for ELectronic heaLth Records), funded by the Portuguese Foundation for Science and Technology (FCT) under grant 2024.07494.IACDC, proposes a different model: a patient-held cryptographic wallet that stores EHR credentials and mediates access to records distributed across a cloud-of-clouds infrastructure, with every access logged immutably on a blockchain. WELL draws on three pillars of recent computer science research:

- **Cloud-of-clouds storage** via RockFS [8], providing availability and confidentiality without single-provider dependency.
- **Blockchain for immutable storage** with test use cases with both a private blockchain (Hyperledger Fabric [1]) and a public blockchain (Ethereum [4]), enabling tamper-proof audit trails and smart-contract-enforced consent.
- **Self-Sovereign Identity** (SSI) [13], allowing patients to prove identity and disclose clinical attributes without exposing their full record.

This white paper surveys the WELL project's objectives, architecture, research contributions from the Well project team, evaluation results, and future directions.

2 Motivation and Problem Statement

2.1 EHR Fragmentation in Portugal

Figure 1 illustrates the current fragmentation of health data in Portugal. While the SNS maintains a centralised repository, private institutions neither contribute to nor draw from it. A pilot project by SPMS to allow some private institutions to read SNS records was announced in 2024 [14], but no reciprocal pathway exists.

2.2 Privacy and Regulatory Constraints

Under GDPR [6], EHRs constitute *special category personal data* subject to heightened protections. Two competing rights create tension: the *Right to Access* (patients must be able to retrieve their records) and the *Right to Erasure* (patients may demand deletion). Blockchain's immutability appears to conflict with erasure — a challenge WELL addresses by storing only encrypted metadata and cryptographic commitments on-chain, with actual data held off-chain.

Additionally, Femtech applications — a growing class of health apps targeting women — have been shown to share intimate data with employers and third parties without adequate consent mechanisms [16, 9]. The WELL framework provides a generalisable consent substrate applicable beyond traditional EHR systems.

[1] Serviços Partilhados do Ministério da Saúde

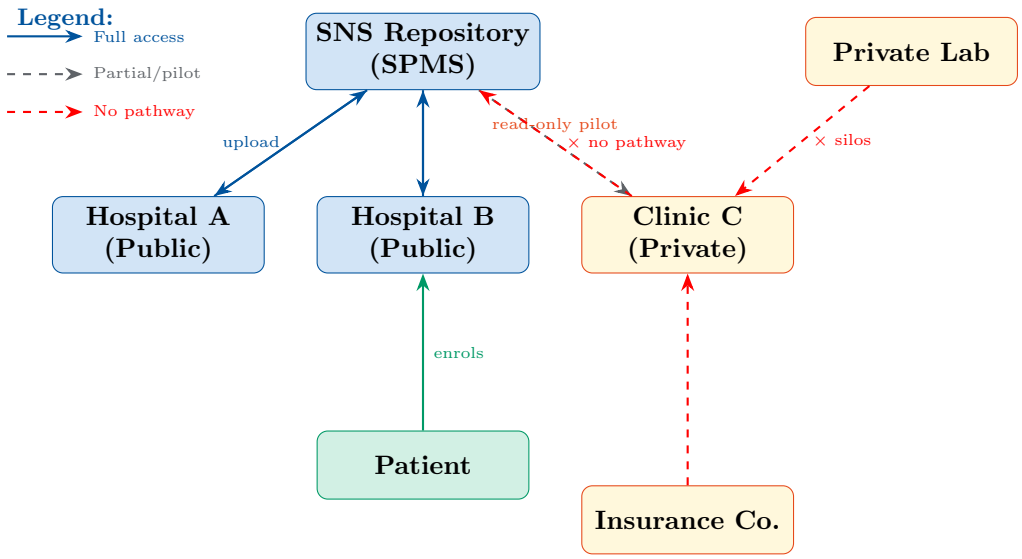

Figure 1: Current EHR fragmentation in Portugal: public institutions share records via SPMS, but private providers operate independently.

3 The WELL System

WELL decomposes into two primary components — the **WELL Repository** and the **WELL Wallet** — connected through a well-defined API contract.

3.1 The Well Trust Architecture

Figure 2 illustrates the three-layer trust architecture of WELL. The **Data Layer** stores EHR content across multiple cloud providers using RockFS, ensuring confidentiality through secret sharing and high availability. The **Ledger Layer** records every access event and all consent decisions in a Hyperledger Fabric blockchain, creating an append-only, tamper-resistant log. The **Identity Layer** relies on Self-Sovereign Identity (SSI) via Hyperledger Indy, so patients prove authorisation without exposing unnecessary personal data to third parties.

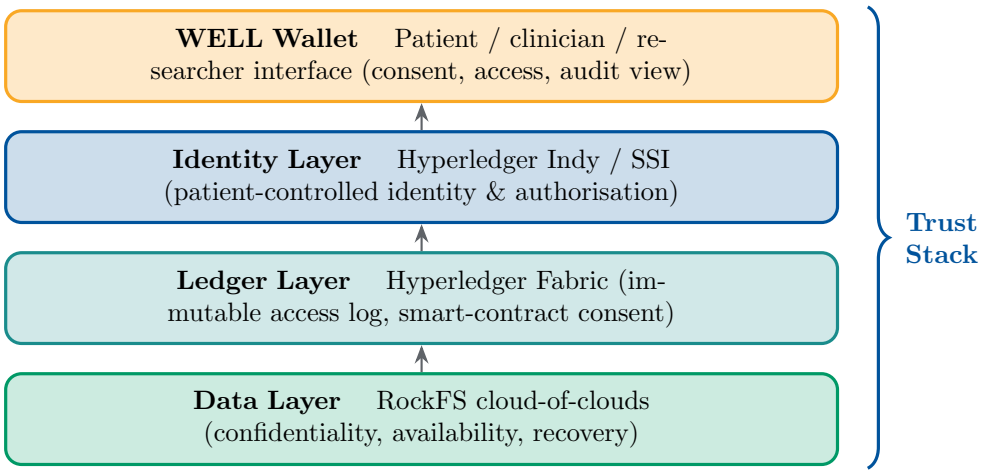

Figure 2: The WELL three-layer trust architecture. Each layer contributes a distinct security property; together they realise end-to-end transparency and accountability for EHR management.

Here's a vertical layout — users on top, then wallet, API, repository, and infrastructure at the

bottom: latex

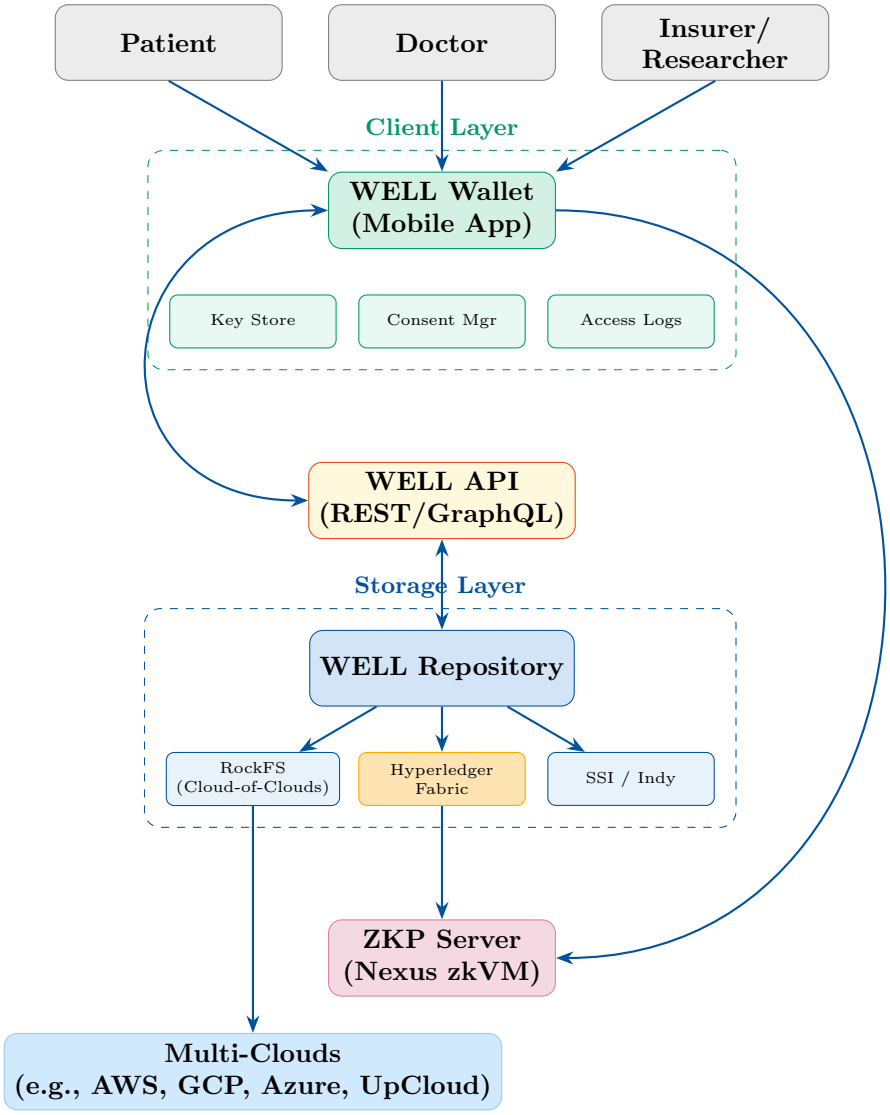

Figure 3: High-level architecture of the WELL system. The WELL Wallet acts as the patient-facing client; the WELL Repository provides hybrid cloud-blockchain storage.

3.2 WELL Repository

The repository is a hybrid system with two complementary components:

Cloud-of-Clouds (RockFS): RockFS [8] distributes EHR data across N cloud providers using a secret-sharing scheme based on erasure codes. To reconstruct a record, $k < N$ shares are required, ensuring that an attacker who compromises $f < k$ clouds gains nothing. RockFS also provides recovery from client-side attacks and unintended deletions. In the WELL context, this layer stores the encrypted EHR payload.

Distributed Ledger (Hyperledger Fabric): The blockchain stores EHR metadata — record identifiers, cryptographic hashes, consent tokens, and access logs. Two smart contracts govern the system: `AccessLog` (recording all read/write events with timestamps and user identities) and `EHRManager` (managing record references and permission requests). The permissioned nature of Fabric aligns with GDPR requirements, allowing defined participants (hospitals, insurers, regulators) without public exposure.

latex

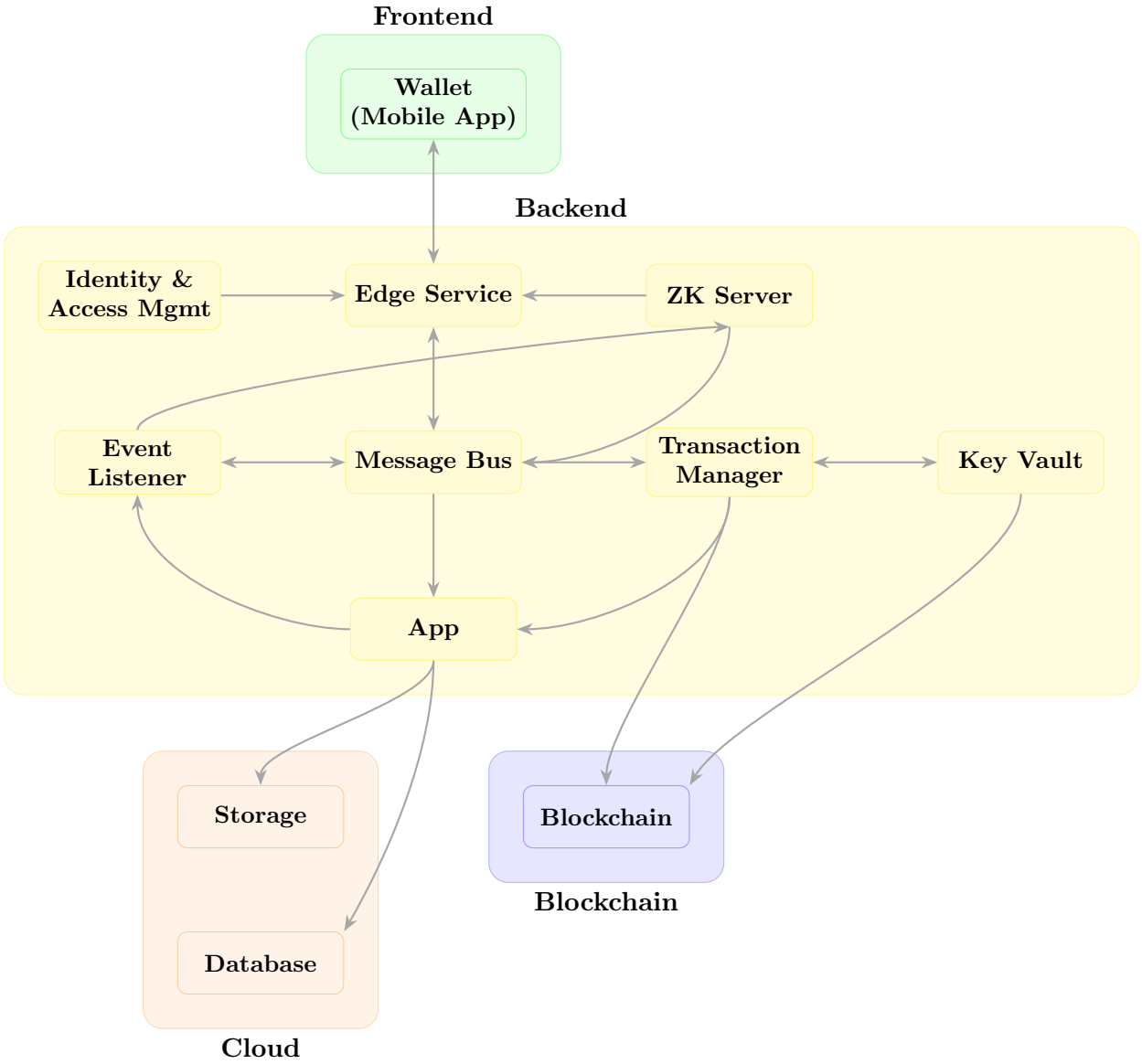

Figure 4: High-level architecture diagram showing Frontend, Backend, Blockchain, and Cloud layers.

3.3 WELL Wallet

The WELL Wallet is a mobile application that:

- Stores asymmetric key pairs in an encrypted local database.
- Submits blockchain transactions to log EHR accesses.
- Manages consent tokens granting or revoking third-party access.
- Displays a complete, tamper-evident access history.
- Generates Zero-Knowledge Proofs (ZKPs) to selectively disclose health attributes.

4 Research Contributions

The WELL project has generated three research contributions from its team:

4.1 Well Wallet: A Blockchain Wallet for EHRs

Further reading: A prototype of the WELL Wallet can be found at https://github.com/INESC-ID-Project-WELL/Well-Wallet and https://github.com/INESC-ID-Project-WELL/Well-Wallet-ChainCode

Well Wallet is the patient-facing mobile application produced within the WELL project. It realises the WELL vision—giving patients full ownership of their Electronic Health Records (EHRs)—by combining a blockchain-based access control layer with a cloud-of-clouds storage backend, and extending it with Zero-Knowledge Proof (ZKP) capabilities that allow selective, privacy-preserving disclosure of clinical data. Where the WELL Repository focuses on the server-side infrastructure (RockFS, Hyperledger Fabric, and Self-Sovereign Identity), Well Wallet is the endpoint through which patients, clinicians, and stakeholders interact with that infrastructure. Together, they form a complete, end-to-end platform for secure EHR management.

System Architecture

Figure 5 shows the three-component architecture of Well Wallet. The Wallet (Mobile application) is the user-facing interface. It communicates with Well Repository, a backend system comprising a MedPlum FHIR server, an Ethereum smart-contract layer, and RockFS multi-cloud storage. A dedicated ZKP Server offloads computationally expensive proof generation from the mobile device, returning verifiable cryptographic proofs that the wallet renders as scannable QR codes.

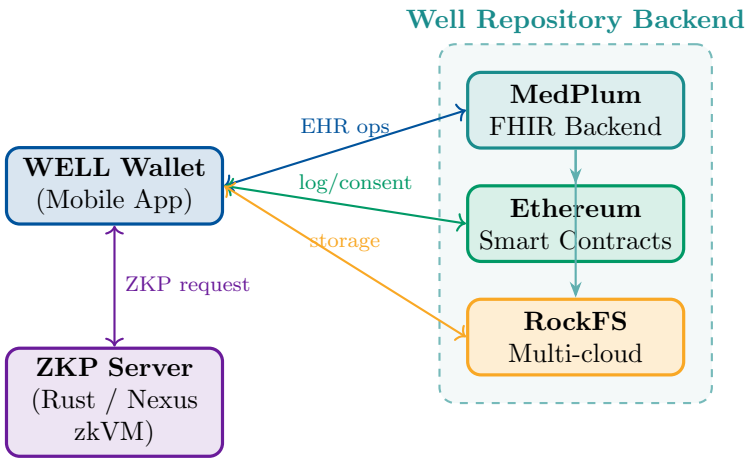

Figure 5: Well Wallet system architecture. The Mobile wallet interfaces with Well Repository (FHIR backend, Ethereum smart contracts, and RockFS cloud-of-clouds storage) and an off-device ZKP Server for privacy-preserving proof generation.

User Roles and Operations

Well Wallet defines four distinct user roles — *Patients*, *Medical Staff*, *Stakeholders*, and *System Administrators* — each with a tailored permission set. Figure 6 summarises the operations available to each role and the blockchain events they trigger.

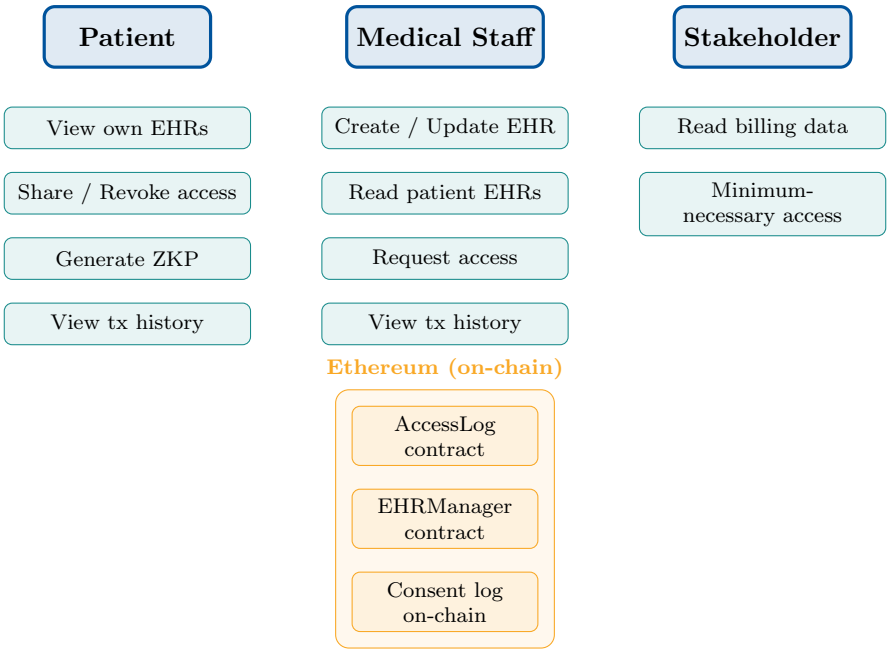

Figure 6: User roles in Well Wallet and their relationship to on-chain events. Every access, consent change, and EHR creation triggers a blockchain transaction, ensuring a complete and tamper-proof audit trail.

Performance Evaluation

The Well Wallet prototype was evaluated across three dimensions: blockchain latency, backend throughput, and mobile resource usage.

Blockchain latency. Operations were tested against MedPlum alone (without blockchain), Ethereum Sepolia (Layer 1), and Arbitrum Sepolia (Layer 2). Figure 7 shows that Layer 2 reduces average read latency by approximately 79% compared to Layer 1 (from 10 744 ms to 2 309 ms), while still providing the immutability and auditability guarantees required by WELL. The overhead relative to the no-blockchain baseline remains below 250%, an acceptable trade-off given the added transparency.

Backend throughput. A stress test of the MedPlum backend showed logarithmic latency growth up to approximately 25 600 concurrent requests, beyond which saturation effects appear. Peak throughput stabilises near 1 380 requests per second, well within the expected load of a national-scale EHR deployment.

Mobile resource footprint. Profiling on a standard Mobile device confirmed that Well Wallet is lightweight: CPU usage remained below 10% throughout typical sessions, and resident memory stabilised at approximately 121 MB. Local storage for the encrypted database totals only ˜1.4 MB, and the installed application occupies 90 MB. These figures are compatible with devices carrying as little as 2 GB of RAM— covering over 96% of active Mobile handsets worldwide, confirming suitability for population-wide deployment.

Zero-Knowledge Proofs: Extending WELL's Privacy Model

A distinguishing feature of Well Wallet is its use of ZKPs not merely for identity verification but for *clinical data itself*. Using the Nexus zkVM, the ZKP Server generates Rust-based proofs that a private measurement (e.g., a haemoglobin level) falls within a clinically acceptable range,

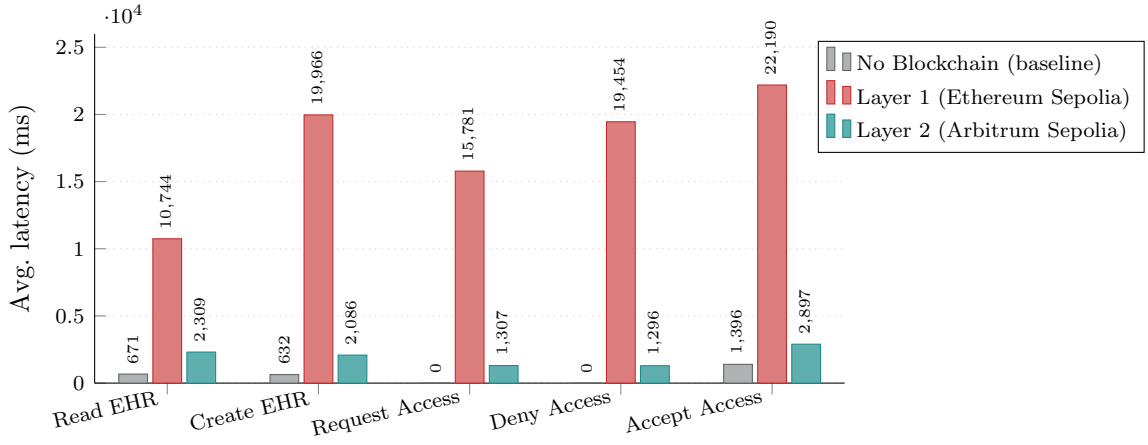

Figure 7: Average latency for EHR operations across three blockchain configurations (30 trials each). Layer 2 consistently outperforms Layer 1 while preserving full auditability, making it the recommended configuration for WELL deployments. Bars for *Request Access* and *Deny Access* have no baseline because these operations require blockchain interaction by design.

returning only a binary result and a timestamp — no raw data is disclosed. This capability directly supports WELL's broader objective of enabling privacy-preserving health analytics, opening the door to population-level statistical verification without exposing individual records. Discussions with SPMS, the organisation responsible for Portugal's national eHealth infrastructure, confirmed that this ZKP layer could be integrated atop the existing national message bus architecture, marking a novel contribution to privacy-preserving healthcare systems.

4.2 Well Repository: Multi-Cloud Blockchain EHR Backend

A prototype of the WELL Wallet can be found at https://github.com/INESC-ID-Project-WELL/Well-Repository and https://github.com/INESC-ID-Project-WELL/Well-Contracts

The Well Repository system represents one of the primary technical outputs of the WELL project, functioning as the high-availability repository for the WELL - Wallet for Electronic health records. Developed to overcome the limitations of centralized and single-cloud EHR storage, Well Repository integrates Hyperledger Fabric blockchain technology with a multi-cloud storage strategy powered by RockFS.

Role within the WELL Ecosystem

In the context of the WELL project, Well Repository provides the underlying storage infrastructure that ensures the confidentiality, integrity, and availability of clinical data. While the WELL Wallet serves as the client-side application for patients and medical professionals to manage their data, Well Repository handles the complex off-chain storage and on-chain access logging.

By shifting to a patient-centric model, Well Repository allows patients to maintain control over their medical history while ensuring that healthcare institutions can access accurate information when authorized. This integration is facilitated through the Medplum framework, marking a novel implementation that combines FHIR-standardized applications with blockchain and multi-cloud backends.

System Architecture

The Well Repository architecture (illustrated in Figure 8) follows a hybrid model. Sensitive EHR files, such as imaging (X-rays, MRIs), are stored across multiple cloud providers to ensure high availability and prevent vendor lock-in. Concurrently, the Hyperledger Fabric blockchain stores an immutable record of every data access, providing a transparent audit trail for the patient.

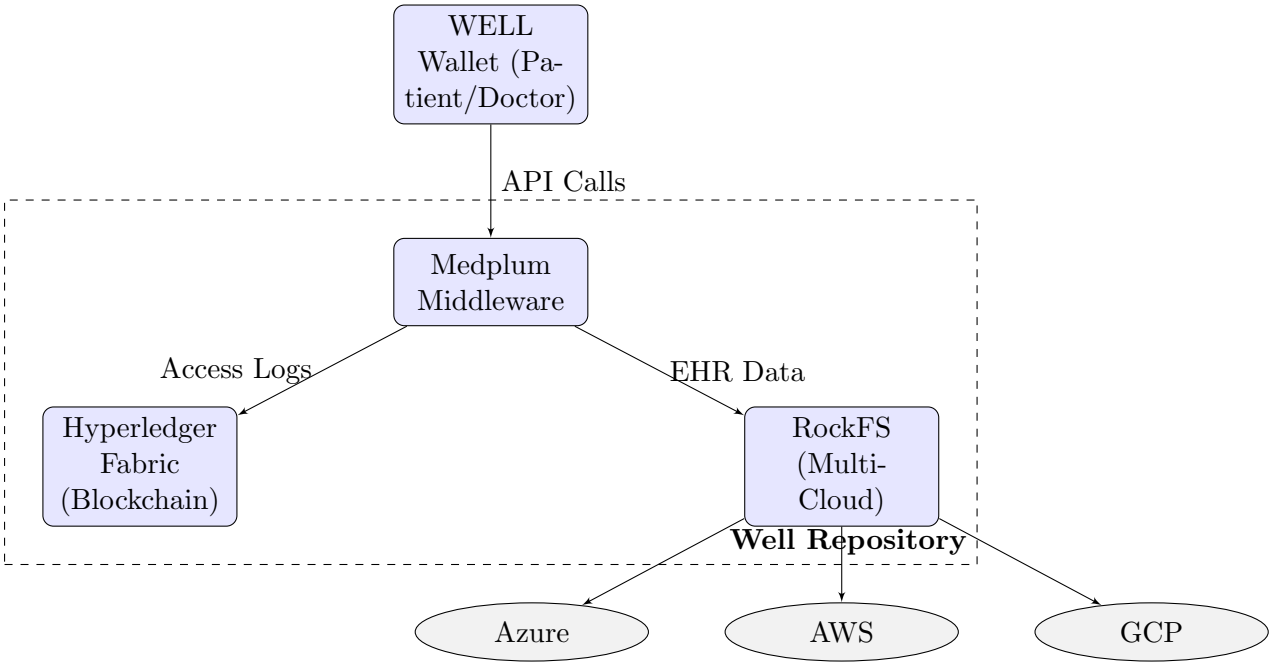

Figure 8: Well Repository Hybrid Architecture for the WELL Project.

Multi-Cloud Strategy via RockFS

Well Repository leverages the **RockFS** framework to distribute data shares across multiple cloud providers. This approach uses a secret-sharing scheme based on erasure codes, ensuring that if a single cloud provider is compromised or experiences an outage, the patient's data remains secure and available. As a cloud-of-clouds file system, RockFS eliminates the risk of a single point of failure and provides a recovery mechanism to undo unintended operations.

Blockchain-Based Access Control

Hyperledger Fabric acts as the permissioned blockchain backbone. It manages the "world state" of EHR metadata and permissions, ensuring that only authorized parties with patient consent can retrieve data. Every interaction is recorded as a transaction, addressing the critical requirement of providing patients with a means to consult who has accessed their data.

Performance Evaluation

Evaluations of Well Repository demonstrate that while the integration of blockchain and multi-cloud storage introduces a performance overhead compared to centralized systems, the results remain within acceptable levels for real-world healthcare environments. The trade-off between increased security (confidentiality and integrity) and slightly higher latency is justified by the enhanced trust and patient-sovereignty the system provides.

The Well Reporitory fulfills the WELL project's objective of creating a tamper-resistant, high-availability storage solution for EHRs. By combining the transparency of blockchain with the

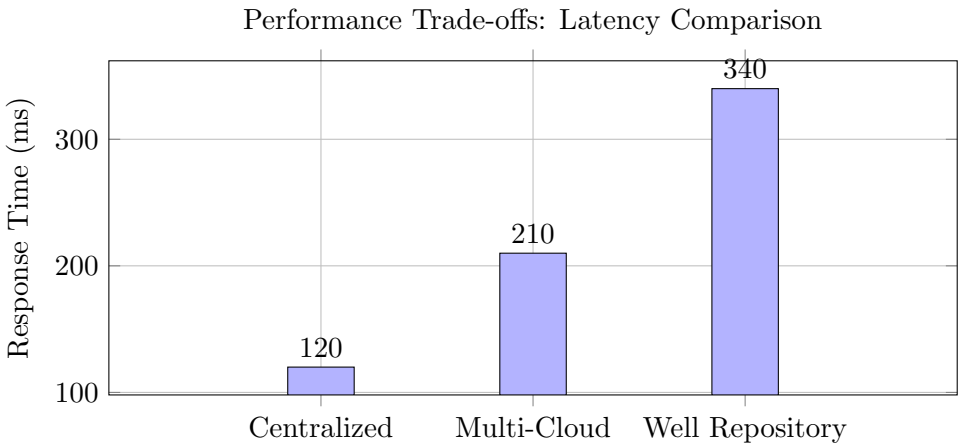

Figure 9: Representative comparison of latency across different storage models within the WELL project contexts.

resilience of multi-cloud storage, it offers a scalable reference architecture for future e-health systems seeking to empower patients while maintaining rigorous security standards.

4.3 Trust Through Transparency: Connecting PrivacHer Insights to WELL

Full description of this work can be found in: Larissa Tomaz, David R. Matos, and Teresa Almeida, *"Trust Through Transparency: Blockchain for Consent and Accountability in Femtech Applications,"* GoodIT '25, Antwerp, Belgium, September 2025.
https://doi.org/10.1145/3748699.3749771

A core challenge in electronic health record (EHR) systems is the tension between *data accessibility* and *user trust*. Patients readily surrender control of sensitive clinical information to healthcare institutions, yet they have historically lacked any means to verify who accessed their records, under what authority, or for what purpose. The WELL project directly addresses this gap by embedding transparency and accountability as first-class design principles, building on the theoretical and practical groundwork laid by the *PrivacHer* system [**?**].

PrivacHer demonstrated, in the Femtech domain, that a blockchain-based consent management framework can provide immutable audit trails, granular consent controls, and GDPR-compliant data governance. WELL extends and generalises this model to the broader landscape of electronic health records, integrating a cloud-of-clouds repository (for high availability) with a permissioned distributed ledger (for tamper-evident logging and consent enforcement via smart contracts).

Consent Lifecycle and Audit Trail

Drawing on the PrivacHer consent model, WELL implements a *dynamic consent lifecycle* in which a patient's preferences can be updated at any time; every version is preserved on-chain. Figure 10 traces the five stages of this lifecycle and the blockchain events that accompany each transition, ensuring that both patients and regulators can reconstruct a complete provenance chain for any EHR access.

Performance and Scalability Trade-offs

The PrivacHer prototype, evaluated under load using Locust, revealed that blockchain-backed data retrieval introduces measurable latency—peaking near 13 000 ms under heavy load—while

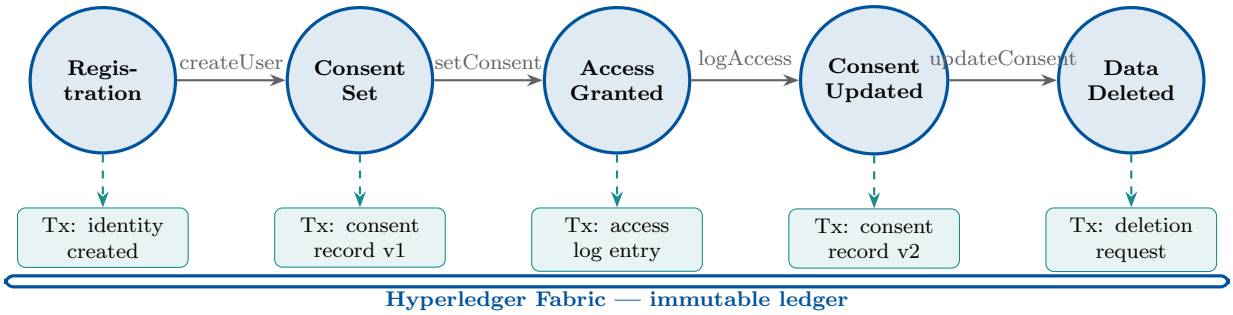

Figure 10: Dynamic consent lifecycle in WELL. Every state transition triggers a blockchain transaction, producing an auditable, tamper-proof history of patient consent and data access.

simpler operations such as consent updates remained well below 2 000 ms. WELL acknowledges these trade-offs and targets optimisations at the repository level (caching, off-chain data with on-chain pointers) to keep routine clinical access within acceptable bounds. Figure 11 compares the indicative latency profiles of the key WELL operations.

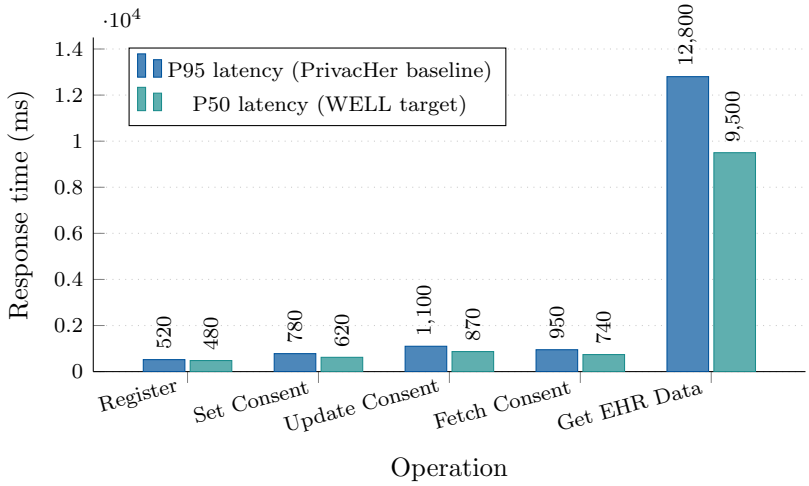

Figure 11: Indicative latency profiles for key WELL operations. P95 figures are based on PrivacHer prototype measurements; P50 figures represent WELL design targets after repository-level optimisation. The *Get EHR Data* operation dominates due to multi-service and blockchain interaction.

Transparency as a Trust Enabler

Trust in a health data system is not solely a technical property—it is a social contract between patients, clinicians, and institutions. The WELL project operationalises this contract through four mutually reinforcing mechanisms:

1. **Immutability.** Once an access event or consent record is written to the Hyperledger Fabric ledger, it cannot be silently altered, giving patients and regulators a reliable ground truth.
2. **Verifiability.** Patients can inspect their own access logs via the WELL Wallet at any time, without dependence on the goodwill of any single institution.
3. **Accountability.** Every data request is attributed to an authenticated identity, creating non-repudiation for both authorised and unauthorised accesses.

4. **Revocability.** SSI-backed consent can be withdrawn at any moment; smart contracts immediately enforce the updated preferences, preventing further access by previously authorised parties.

Taken together, these mechanisms transform transparency from a regulatory checkbox into an active trust-building tool—one that the PrivacHer work validated in the Femtech context and that WELL extends to the full spectrum of electronic health record management.

5 Comparison with Related Work

Table 1: Comparison of WELL with related EHR blockchain systems

System	Cloud	Blockchain	Mobile Wallet	ZKP	SSI
MedRec [2]	✓	Ethereum	–	–	–
MeDShare [18]	✓	Permissioned	–	–	–
ACTION-EHR [5]	✓	Hyperledger	–	Partial	–
Health-zkIDM [3]	–	Hyperledger	–	✓	–
PR Wallet [7]	–	Generic	✓	–	Partial
WELL Wallet	✓	**ETH L2**	✓	✓	✓
WELL Repository	✓	**Hyperledger**	✓	✓	✓

WELL is, to the authors' knowledge, the first system to combine all five desiderata: cloud-of-clouds storage, blockchain auditing, a patient-facing mobile wallet, ZKPs applied to clinical data (not merely identity), and SSI-based identity management.

6 Implementation Status and Outputs

Figure 12 shows the WELL project timeline, spanning January–December 2025.

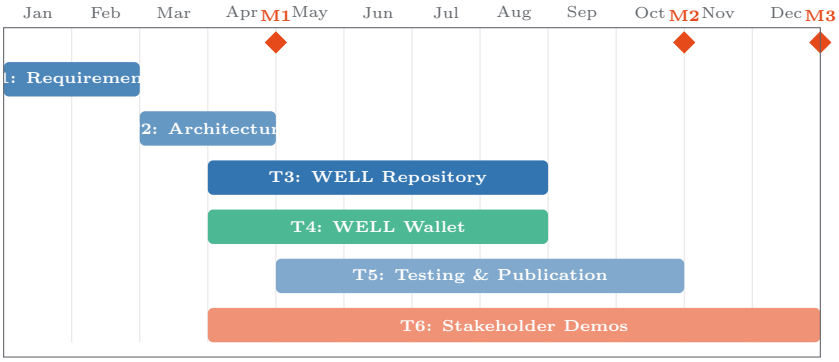

Figure 12: WELL project timeline. Three milestones: M1 (feasibility, April 2025), M2 (full prototype, October 2025), M3 (stakeholder validation, December 2025).

The project has delivered the following tangible outputs:

Scientific Papers. Four peer-reviewed papers were published.

- Melita, Matos, and Pardal presented [10] *Bonsai: A Recovery Approach for Ethereum ERC-20 Transactions* at the 23rd International Symposium on Network Computing and Applications (NCA 2025).

- Pedro, Ramos, and Matos presented [12] *Rûm: Multivalued Loss-Tolerant Byzantine Consensus for Mobile Ad-Hoc Networks*, at the 23rd International Symposium on Network Computing and Applications (NCA 2025).
- Tomaz, Matos, and Almeida presented [17] *Trust Through Transparency: Blockchain for Consent and Accountability in Femtech Applications* at the 2025 International Conference on Information Technology for Social Good.
- Finally, Rodrigues, Silva, and Avritzer published [15] *Assessment of Performance and its Scalability in Microservice Architectures: Systematic Literature Review* in the *Journal of Systems and Software*.

Completed MSc Theses. Two MSc theses were completed under the project.

- Beatriz Militão concluded *Healthy Wallet: Blockchain Wallet for Electronic Health Records* [11], advised by David R. Matos and Hugo Macedo.
- Diogo Melita concluded *Bonsai: A Recovery Approach for Ethereum ERC-20 Transactions* [10], advised by David R. Matos and Miguel Pardal.

Prototypes. Three open-source prototype components were developed and are publicly available.

- The Well Wallet mobile application is available at `https://github.com/INESC-ID-Project-WELL/Well-Wallet`.
- The Well Repository is available at `https://github.com/INESC-ID-Project-WELL/Well-Repository`.
- The Well Smart Contracts are available at `https://github.com/INESC-ID-Project-WELL/Well-Contracts` and `https://github.com/INESC-ID-Project-WELL/Well-Wallet-ChainCode`.

7 Future Directions

Progressive web app. The current implementation of the Well Wallet can be extended to a Progressive Web App, enabling clinician access from any device.

ZKP for population-level analytics. The meeting with SPMS revealed an opportunity to integrate a ZKP verification layer into the national health message bus, enabling privacy-preserving statistical queries (e.g., average glycaemia values across patient cohorts) without exposing individual records.

On-chain access control. Access control logic currently delegated to MedPlum will be migrated fully on-chain, increasing transparency and removing dependence on a trusted middleware layer.

Hardware security enclaves. Key management will be hardened through TEE (Trusted Execution Environment) integration, protecting private keys from OS-level compromise.

GDPR Right-to-Erasure tooling. Formal tooling for on-chain reference invalidation and cloud-data deletion will be developed, providing verifiable erasure audit trails.

8 Conclusion

The WELL project demonstrates that a patient-centric EHR wallet combining cloud-of-clouds storage, blockchain auditing, and Zero-Knowledge Proofs is technically feasible, practically de-

ployable on commodity hardware, and architecturally aligned with Portugal's national health infrastructure.

Experimental results establish that Layer 2 blockchain networks (Arbitrum) provide latency acceptable for real-time clinical workflows (≈2 seconds), while the Well Repository backend sustains over 1,300 requests per second — sufficient for national-scale deployment.

Beyond the technical contributions, WELL establishes a governance model for sensitive health data: patients hold cryptographic keys, every access is logged, and consent is enforced by code rather than policy. This model is generalisable to any personal data domain — from Femtech applications to agricultural health records — wherever individuals seek meaningful control over data that directly affects their lives.

Acknowledgements. This work was supported by national funds through Fundação para a Ciência e a Tecnologia, I.P. (FCT) under projects UID/50021/2025 and UID/PRR/50021/2025 (INESC-ID) and 2024.07494.IACDC (WELL).

References

[1] Elli Androulaki et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the 13th EuroSys Conference*, pages 1–15, 2018.

[2] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman. MedRec: Using blockchain for medical data access and permission management. In *2nd International Conference on Open and Big Data*, pages 25–30, 2016.

[3] T. Bai et al. Health-zkIDM: A healthcare identity system based on Fabric blockchain and zero-knowledge proof. *Sensors*, 22(20), 2022.

[4] V. Buterin. Ethereum: A next-generation smart contract and decentralized application platform. https://ethereum.org/en/whitepaper/, 2013.

[5] A. Dubovitskaya et al. ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care. *Journal of Medical Internet Research*, 22(8):e13598, 2020.

[6] European Parliament and Council of the European Union. Regulation (EU) 2016/679 (General Data Protection Regulation), 2016.

[7] M. Gupta. PR wallet-based blockchain access protocol to secure EHRs. In *Blockchain and IoT Integration*. Auerbach Publications, 2021.

[8] D. R. Matos, M. L. Pardal, G. Carle, and M. Correia. RockFS: Cloud-backed file system resilience to client-side attacks. In *Proceedings of the 19th International Middleware Conference*, pages 107–119, 2018.

[9] M. Mehrnezhad and T. Almeida. Caring for intimate data in fertility technologies. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 2021.

[10] D. Melita, D. R. Matos, and M. L. Pardal. Bonsai: A recovery approach for Ethereum ERC-20 transactions. In *2025 23rd International Symposium on Network Computing and Applications (NCA)*, pages 286–294. IEEE, 2025.

[11] B. Militão, D. R. Matos, and H. D. Macedo. Healthy wallet: Blockchain wallet for electronic health records. In *ACM Conference Proceedings*, October 2025.

[12] J. Pedro, G. Ramos, and D. R. Matos. Rûm: Multivalued loss-tolerant Byzantine consensus for mobile ad-hoc networks. In *2025 23rd International Symposium on Network Computing and Applications (NCA)*, pages 115–122. IEEE, 2025.

[13] A. Preukschat and D. Reed. *Self-Sovereign Identity*. Manning Publications, 2021.

[14] I. Rocha. SNS começa em breve a partilhar dados de saúde dos utentes com o grupo CUF. *Público*, July 2024.

[15] H. Rodrigues, A. R. Silva, and A. Avritzer. Assessment of performance and its scalability in microservice architectures: Systematic literature review. *Journal of Systems and Software*, 230:112500, 2025.

[16] L. Shipp and J. Blasco. How private is your period?: A systematic analysis of menstrual app privacy policies. *Proceedings on Privacy Enhancing Technologies*, 2020(4):491–510, 2020.

[17] L. Tomaz, D. R. Matos, and T. Almeida. Trust through transparency: Blockchain for consent and accountability in femtech applications. In *Proceedings of the 2025 International Conference on Information Technology for Social Good*, pages 33–40, 2025.

[18] Q. Xia et al. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access*, 5:14757–14767, 2017.