College Dublin
Computing • IT • Business

Assessment Cover Page

Student Full Name	Carlos Eduardo Borges Torres de Menezes Neto Renan de Castilhos da Silva
Student Number	2023252; 2023211
Module Title	Distributed Digital Transactions
Assessment Title	Decentralized
Lecturer/Supervisor	Muhammed Iqbal
Assessment Due Date	21/11/2025 @ 11:59pm
Date of Submission	24/11/2025

Use of AI Tools

I acknowledge the use of CopilotAI for the purpose of Structuring the texts, correcting the grammar and making it concise with 500 words. The use of RemixAI assistant for the purpose of bug fix and deep explanation of the code in order to have a better understanding of the subject.

Declaration

By submitting this assessment, I confirm that I have read the CCT policy on academic misconduct and understand the implications of submitting work that is not my own or does not appropriately reference material taken from a third party or other source.

I declare it to be my own work and that all material from third parties has been appropriately referenced.

I further confirm that this work has not previously been submitted for assessment by myself or someone else in CCT College Dublin or any other higher education institution.

Abstract

The use of AI was mainly for making the text concise and correcting grammar along with brainstorming and helping with design principals in order to use the best practices to get a clean and well structured code.

Contents

Introduction

This report describes the smart-contract–centric DApp we developed as a pair. It outlines the core functionalities of the application, a focused reflection on encryption and cryptographic choices, and the design principles that guided our implementation. The content is written so it can be pasted directly into an MS Word document and used as the project reflection.

Functionalities of the Application

- On-chain Business Rules

The smart contract is the single source of truth and enforces all critical business rules. It handles creation, modification, and termination of primary on-chain entities and ensures atomic state transitions.

- Role-Based Access Control

Roles are defined on-chain with minimal trusted authorities. Administrative operations require multi-step confirmation or multi-signature approval to reduce single-point compromise.

- Commitment and Reveal Flow

The contract supports commit-reveal patterns using hashed commitments for privacy during the commit phase, followed by on-chain reveal and verification.

- Signature-Based Off-Chain Authorization

Off-chain actions are authorized by ECDSA signatures. The contract verifies signatures to accept delegated transactions and meta-transactions, enabling gas abstraction patterns.

- Event-Driven Observability

Every meaningful state change emits structured events to facilitate off-chain monitoring, auditing, and replicated state reconstruction.

- Emergency Controls and Recovery Paths

A guarded pause mechanism and clearly defined recovery functions permit safe intervention during crises while preserving an auditable trail.

Encryption and Cryptography Reflection

- Primitive Choices

We used ECDSA for signature verification and Keccak-256 for hashing, aligning with broad ecosystem support and deterministic gas behavior. These primitives provide authentication, integrity, and succinct commitments.

- Canonicalization and Domain Separation

Messages are canonicalized and include explicit domain separators and nonces. This prevents signature replay across contexts and ensures signed payloads map unambiguously to on-chain actions.

- Off-Chain Computation with On-Chain Verification

Heavy cryptographic computation and batch processing are performed off-chain. The contract verifies compact cryptographic artifacts such as hashes, signatures, and succinct proofs. This hybrid model reduces gas cost while maintaining verifiability.

- Replay and Expiry Protection

Nonces and explicit expiry windows are enforced for signed payloads. This reduces risk from leaked signatures and ensures time-bound validity of off-chain authorizations.

- Threat Trade-offs

We acknowledge advanced primitives (e.g., full zero-knowledge proofs) provide stronger privacy or compression but are costly. Our approach prioritizes pragmatic, verifiable proofs and cryptographic commitments that fit within gas constraints while enabling future upgrades to stronger proofs.

Design Principles

- Minimal Trusted Surface

Expose only the essential API and restrict capabilities to what must be on-chain.

- Modularity and Composability

Contracts are small and focused: core logic, storage, and utility libraries. This improves auditability and reusability.

- Determinism and Observability

State transitions are deterministic; structured events make the system reconstructible and auditable off-chain.

- Fail-Safe Defaults

Default behaviors prioritize safety: failed actions revert cleanly, and emergency pause/rollback patterns exist where possible.

- Gas Awareness and Efficiency

Storage packing, batched operations, and moving heavy work off-chain were applied to control gas costs.

- Security by Design

Checks-effects-interactions, least-privilege roles, explicit invariants, and guarded admin flows minimize attack surface.

Conclusion

This pair project prioritized a contract-first architecture with clear, auditable functionality, pragmatic cryptographic choices, and design principles that balance security, cost, and upgradeability. The DApp demonstrates how careful cryptographic integration and modular contract design produce a system that is verifiable, maintainable, and prepared for incremental hardening and formal verification.

References

Bak, Ozlem, et al. “Exploring Blockchain Implementation Challenges in the Context of Healthcare Supply Chain (HCSC).” Ebsco.com, International Journal of Production Research, Jan. 2025, research.ebsco.com/c/jzntuu/viewer/html/5ysjij5smf. Accessed 9 Nov. 2025.

“Blockchain in Healthcare: Benefits, Use Cases and Challenges.” TMA Solutions, 2022, www.tmasolutions.com/insights/blockchain-in-healthcare.

Dou, Tengyue, et al. “A Secure Medical Data Framework Integrating Blockchain and Edge Computing: An Attribute-Based Signcryption Approach.” Sensors, vol. 25, no. 9, 30 Apr. 2025, pp. 2859–2859, www.mdpi.com/1424-8220/25/9/2859, https://doi.org/10.3390/s25092859. Accessed 21 Nov. 2025.

Jabri, Abdou-Essamad, et al. “Leveraging Blockchain and Proxy Re-Encryption to Secure Medical IoT Records.” ArXiv.org, 2025, arxiv.org/abs/2509.08402. Accessed 20 Nov. 2025.

Katru Rama Rao, and Satuluri Naganjaneyulu. “Designing a Block Chain Based Network for the Secure Exchange of Medical Data in Healthcare Systems.” Applied Artificial Intelligence, vol. 38, no. 1, 11 Mar. 2024, https://doi.org/10.1080/08839514.2024.2318164. Accessed 16 Nov. 2025.

Khouzima_hamza. “Implementation of IPFS in Healthcare Projects: A Comprehensive Overview.” Medium, 14 Mar. 2024,

medium.com/@khouzimahamza20/implementation-of-ipfs-in-healthcare-projects-a-comprehensive-overview-f0afbdf7e82c. Accessed 18 Nov. 2025.

Malik, Pankaj, et al. “Integrating Blockchain and 5G Technologies for Enhanced Edge Computing: Opportunities, Challenges, and Solutions.” International Journal of Recent Advances in Multidisciplinary Topics, vol. 5, no. 2, 2024, pp. 35–43, journals.ijramt.com/index.php/ijramt/article/view/2855, https://doi.org/10.5281/zenodo.10702502. Accessed 9 Nov. 2025.

Megha, Jain, and Pandey Dhiraj. “HRCM: An Approach Using Blockchain Technology in Healthcare-Record Chain Management.” Ebsco.com, International Journal of Performability Engineering, Jan. 2025, research.ebsco.com/c/jzntuu/viewer/pdf/4adi773hvr. Accessed 20 Nov. 2025.

Mishra, Debani Prasad, et al. “Efficient Blockchain Based Solution for Secure Medical Record Management.” International Journal of Informatics and Communication Technology (IJ-ICT), vol. 14, no. 1, 22 Dec. 2024, pp. 59–59, https://doi.org/10.11591/ijict.v14i1.pp59-67. Accessed 9 Nov. 2025.

Mohanapriya, Mrs, et al. “Med-Block: Secure Health Record Management System Using Blockchain with Ipfs.” International Journal of Engineering Research & Technology (IJERT), 4 Apr. 2024.

Noor, et al. “Blockchain-Based Healthcare Records Management Framework: Enhancing Security, Privacy, and Interoperability.” Technologies, vol. 12, no. 9, 14 Sept. 2024, pp. 168–168, www.mdpi.com/2227-7080/12/9/168, https://doi.org/10.3390/technologies12090168. Accessed 3 Nov. 2025.

“Blockchain-Based Healthcare Records Management Framework: Enhancing Security, Privacy, and Interoperability.” Technologies, vol. 12, no. 9, 14 Sept. 2024, pp. 168–168, www.mdpi.com/2227-7080/12/9/168, https://doi.org/10.3390/technologies12090168. Accessed 20 Nov. 2025.

Pongallu, Darshika Ravindra. “Securing Medical Records Using Blockchain with Cryptography, Encryption, and Zero-Knowledge Rollups.” Ncirl.ie, 2024, norma.ncirl.ie/8049/, https://norma.ncirl.ie/8049/1/darshikaravindrapongallu.pdf. Accessed 21 Nov. 2025.

Singh, Murari Kumar, et al. “A Blockchain-IPFS Framework for Secure, Scalable, and Interoperable Healthcare Data Management.” SN Computer Science, vol. 6, no. 5, 17 Apr. 2025, https://doi.org/10.1007/s42979-025-03936-z. Accessed 9 Nov. 2025.

Tran, Phong, et al. “A Solution for Commercializing, Decentralizing and Storing Electronic Medical Records by Integrating Proxy Re-Encryption, IPFS, and Blockchain.” ArXiv.org, 2024, arxiv.org/abs/2402.05498. Accessed 20 Nov. 2025.