



Changemakers: Creativity and Value Creation

Assignment 2: Project Management & Innovation



Name: Lucas Adouko

Student ID: 2424749

Course Name: BSc Applied Computing

Module Name: Changemakers: Creativity and Value Creation

Module Code: ACCA5033

Table of Contents

Introduction	2
Task 1: Project Management.....	2
Q1. Project Management & Planning:	2
Project Scope and Proposed Solution	2
Technologies and Resources Required	3
Project Constraints	3
Development Methodology.....	3
Project Timeline & Gantt Chart	4
Q2. Project Design:	4
Industrial Design & Product Aesthetics (Physical Render)	4
Hardware Security Architecture & Data Flow (Diagram)	5
Task 2: Enterprise.....	7
Q1. PEST & SWOT Analysis	7
PEST Analysis	7
SWOT Analysis.....	7
Legal & Ethical Considerations	7
Q2. Tech Start-up Profile: GenVault	8
Start-up Name & Logo:	8
Business Type:	8
Business Strategy:	8
Funding Initiatives:.....	8
Task 3: Project reflection	9
Skill Development and Personal Growth.....	9
Positive Impact on Society.....	9
Risks, Challenges, and Mitigation	10
Conclusion.....	10
References	11

Introduction

The development of digital security and decentralised asset management is constantly changing, showing important weaknesses in current storage solutions. This report presents the development project for a “Dual-Node Hardware Vault,” an innovation designed to remove single points of failure by physically separating cryptographic secret keys from the main user interface. By applying the principles of creative thinking and value creation, this project aims to not only improve technical security but also enhance Human-Computer Interaction to provide real financial control for users in a decentralised economy.

The objective of this document is to explain the strategic planning of the project, including its scope, development method, and market analysis using tools such as PEST and SWOT. By exploring areas of project management and business innovation, this report shows how a practical approach can turn a creative idea into a realistic and secure solution that meets the high standards of today’s technology industry.

Task 1: Project Management

Q1. Project Management & Planning:

Project Scope and Proposed Solution

The purpose of this project involves the end-to-end design and conceptualisation of the Dual-Node Hardware Vault. The proposed solution addresses the "single point of failure" in existing digital asset wallets by physically decoupling the cryptographic signing environment (The Secret Node) from the internet-facing user interface[1]. The project scope includes the architectural design of the air-gapped communication protocol, the selection of secure hardware components, and the integration of a capacitive touch-slider for enhanced Human-Computer Interaction. The final deliverable is a comprehensive technical blueprint and a non-functional physical prototype focused on security and usability.

Technologies and Resources Required

To build this hardware-focused solution, the following tools and technologies are needed:

- **Hardware Components:** Dual microcontroller units such as the ESP32 or STM32 for separate node processing.
- **Communication Interface:** A physical USB-C or Lightning interface for the temporary connection between the UI Node and the Secret Node, allowing for secure data transfer during the signing process (Air-gap technology).[2]
- **Interaction Hardware:** Capacitive touch sensors for the slider and haptic vibration motors for tactile confirmation.[3]
- **Software Tools:** CAD software for the aluminium casing design and UML modelling tools for system architecture.
- **Security Libraries:** Open-source cryptographic libraries for secret key generation.

Project Constraints

The project must navigate several critical constraints:

- **Technical Isolation:** Ensuring zero electrical leakage between the UI node and the Secret node.
- **Usability vs Security:** Maintaining a high level of security without making the transaction process too slow for the average user.
- **Material Costs:** Keeping the prototype within a reasonable budget for a potential tech start-up.

Development Methodology

I have selected the Agile (Scrum) development method for this project. Unlike the traditional Waterfall model, Agile allows for iterative development, which is essential for a security-focused hardware project. By working in two-week sprints, I can continuously test the HCI elements (like the touch slider) and the physical USB connection reliability. This method provides the flexibility to pivot based on feedback from the Pilot Data Collection phase, ensuring the final product effectively meets user needs while maintaining strict security standards.[4]

Project Timeline & Gantt Chart

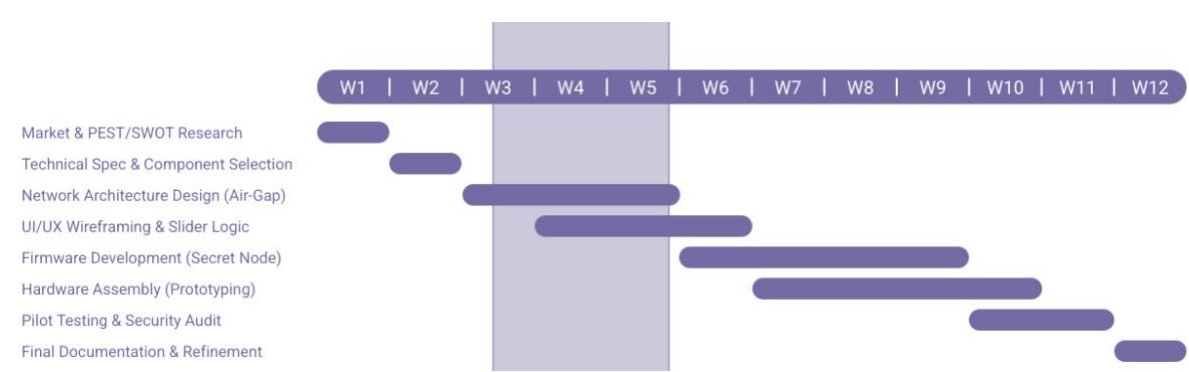


Figure 1: 12-Week Development Grantt Chart for the Dual-Node Hardware Vault.

Q2. Project Design:

To ensure both the technical viability and the market appeal of the Dual-Node Hardware Vault, I have developed two distinct design components. These designs bridge the gap between the aesthetic "Pragmatic" philosophy and the rigorous security requirements.

Industrial Design & Product Aesthetics (Physical Render)

The first piece of design work focuses on the physical form factor and user interface of the device.



Figure 2: Physical Render

- **Design Description:** The render illustrates a premium aluminium chassis, chosen for its durability and electromagnetic protection properties. The minimalist interface features a high-contrast screen for displaying transaction QR codes and a dedicated physical area for haptic interactions.
- **HCI Integration:** The ergonomic design is intended to inspire user trust. The placement of the internal sensors allows for intuitive handling, ensuring that the "Physical Slider" validation described in the scope is easily accessible for the user, reducing the risk of accidental input errors.

Hardware Security Architecture & Data Flow (Diagram)

The diagram illustrates the internal hardware architecture and secure data flow of the system. It highlights the physical air-gap isolation between the "Secret Node" (where private keys are stored) and the "UI Node" (the internet-connected interface). This design ensures that sensitive cryptographic signatures remain offline, protected from remote network attacks.

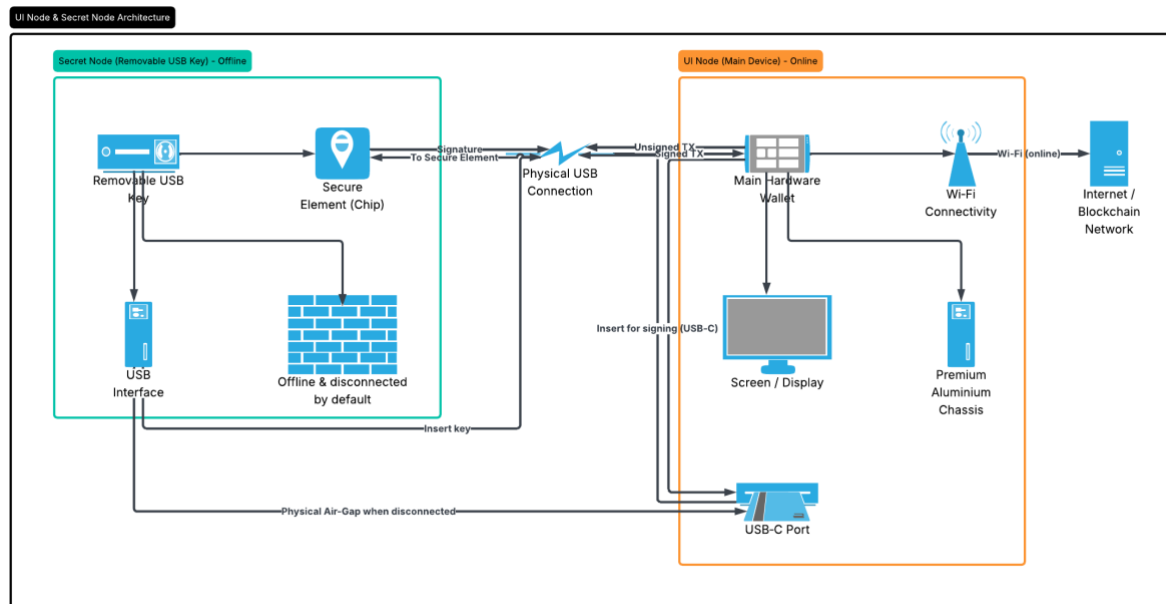


Figure 3: Hardware Security Architecture (Diagram)

UI Node (Main Device) – The Online Interface

The right-hand section represents the UI Node, which serves as the primary gateway for user interaction and network synchronisation.

- **Connectivity:** It features a dedicated Wi-Fi module for real-time connection to the Internet and Blockchain networks.
- **HCI Components:** It houses the main display for transaction review and is encased in a premium aluminium chassis for physical protection.
- **Bridge:** It includes a physical USB-C port, which remains inactive for data transfer until the Secret Node is inserted.

2. Secret Node (Removable USB Key) – The Offline Vault

The left-hand section documents the Secret Node, a self-contained environment designed to protect private keys from remote exploitation.

- **Air-Gap Integrity:** This node is "Offline & disconnected by default," creating a physical airgap that prevents any wireless or remote access to the internal data.
- **Cryptographic Core:** It contains the Secure Element (Chip), which processes cryptographic signatures locally. This ensures that sensitive signing operations never take place on the internet-facing UI Node.

3. Data Flow and Interaction Logic

The architecture defines a strict protocol for transaction signing to mitigate human and technical error:

1. **Unsigned Transaction:** The UI Node prepares transaction data and requests a signature via the physical USB connection.
2. **Physical Insertion:** The user must manually insert the USB key, providing a layer of physical consent.
3. **Local Signing:** The signature is generated within the Secure Element. Only the resulting digital signature is sent back to the UI Node—the private keys never leave the Secret Node.
4. **Broadcast:** Once the signed transaction is returned, the UI Node broadcasts it to the blockchain while the user removes the USB key, restoring the Air-Gap.

Task 2: Enterprise

Q1. PEST & SWOT Analysis

This strategic analysis is conducted for Ledger, the global leader in hardware security and digital asset custody. To evaluate the market environment in which a new competitor like GenVault would operate, it is essential to first understand Ledger's current position and the external factors affecting the industry in 2026.

PEST Analysis

- Political: Increasing government regulations on digital assets demand higher security standards for hardware storage providers.[5]
- Economic: Despite market volatility, there is a rising demand for "Cold Storage" solutions as institutional investors seek professional-grade security.[6]
- Social: A growing distrust in centralised exchanges is driving a massive shift toward personal financial sovereignty.[7]
- Technological: The rise of quantum computing threats is forcing hardware companies to integrate post-quantum cryptographic standards into their roadmap.[8]

SWOT Analysis

- Strengths (Ledger): Huge market share, established trust, and the "Ledger Live" ecosystem.
- Weaknesses (Ledger): Past data breaches (marketing database), and the controversy over their "Ledger Recover" firmware update which some users felt compromised the "Cold Storage" principle.
- Opportunities: Growing institutional adoption and the integration of new blockchain networks.
- Threats: New innovative competitors focusing on "Pure Air-Gap" security.

Legal & Ethical Considerations

From a legal standpoint, the company must comply with global data protection laws (GDPR) and obtain security certifications like EAL5+. Ethically, my project is committed to an "Open-Source" philosophy for its non-critical firmware to allow community audits, ensuring transparency and proving the absence of backdoors.[9]

Q2. Tech Start-up Profile: GenVault

Start-up Name & Logo:

The company is named GenVault, a brand dedicated to next-generation digital custody. The name represents the synergy between modern "Generational" tech and the reliability of a "Vault." The logo features a minimalist, premium design with a bold 'G' and a 'V' nested within its structure.

Business Type:

GenVault would be registered as a Private Limited Company (Ltd). This legal structure is chosen to provide limited liability protection, which is essential for a hardware-focused venture. Furthermore, a Ltd status is the most effective way to attract external investment and manage equity when scaling the business from a prototype to a commercial product.

Business Strategy:

Our strategy focuses on building a high-end, premium product. Unlike cheap plastic wallets, GenVault uses strong aluminium and real physical security. We will sell our products directly to customers (D2C) through our own website. This avoids middlemen and ensures that no one can tamper with or hack the device before it reaches the user. In short, we offer peace of mind through a robust physical object and a simple, manual USB connection.

Funding Initiatives:

To fund the initial production and R&D, GenVault will utilise:

- Innovation Grants: Government funding for cybersecurity infrastructure.
- Seed Investment: Capital from "Angel Investors" to transition the prototype into a production-ready product.
- Pre-orders: A crowdfunding campaign to validate market demand and fund industrial tooling.

Task 3: Project reflection

Skill Development and Personal Growth

Developing the GenVault project has been a big turning point in my academic journey. This project forced me to dive into Hardware Engineering. One of the most rewarding skills I developed was learning to manage physical security at the circuit level. Understanding how to create "Technical Isolation" between two separate nodes taught me that security is not just about code, but about how data moves physically through a device.

I used to see design as something purely aesthetic. Through the development of the GenVault touch-slider and haptic feedback system, I now understand that design is a critical part of security. If a tool is too hard to use, people will not use it correctly[10]. Mastering the balance between a simple user experience and strict technical constraints is a professional skill that will be invaluable in my future career. The Enterprise task helped me develop a Business Mindset. Learning to think like a founder considering legal structures, branding, and funding has shown me that a great technical idea needs a solid business strategy to succeed.

Positive Impact on Society

We see news of major data breaches and exchange hacks almost every week. This has created a lack of trust in digital institutions. I believe GenVault can have a positive impact on society by promoting Digital Sovereignty. By giving individuals the tools to own their own "keys" in a physical, air-gapped way, we move away from a world where people must trust massive, centralised corporations with their life savings.[11]

This project contributes to a more secure and fair digital society. When people feel safe managing their own assets, they are more likely to participate in the digital economy. Beyond financial assets, the "Dual-Node" technology could be adapted to protect other sensitive areas. For example, it could be used to secure electronic voting systems or private medical records. By ensuring that the most sensitive data is never "online" unless the user physically authorises it, GenVault helps build a foundation of privacy that is essential for a modern society.

Risks, Challenges, and Mitigation

Building a hardware security product comes with unique risks that go beyond traditional software bugs.

I have identified three major challenges:

- **The Risk of Physical Loss:** Since the "Secret Node" is a small, removable USB device, a user could lose it or have it stolen. To mitigate this, I designed a "Double-Node" strategy. The GenVault ecosystem encourages a "Master and Backup" system. Users are advised to keep a second Secret Node in a separate, secure physical location, like a safe-deposit box. This ensures that assets remain recoverable even if the primary key is lost.
- **Supply Chain Attacks:** A critical challenge is ensuring the device is not tampered with before it reaches the customer. If a hacker intercepts a device in the mail, they could modify the hardware. To remove this risk, I will implement Tamper-Evident Packaging that leaves physical marks if opened[12]. Additionally, I will develop a software protocol that checks the firmware upon the first connection to verify it is factory original.
- **Technological Obsolescence:** Technology moves fast, and what is secure today might be broken by Quantum Computing tomorrow[13]. To prevent GenVault from becoming obsolete, I am committed to a "Crypto-Agile" approach. The hardware is designed so that we can push encrypted firmware updates. This allows us to upgrade to new security algorithms without the user needing to buy a new device every year.

Conclusion

This assignment has provided a comprehensive framework for developing GenVault from a technical concept into a viable business proposition. Through the design of the dual-node architecture, I have demonstrated that physical isolation remains the most robust defence against modern cyber threats. The strategic analysis conducted in Task 2 highlights a clear market opportunity for premium, high-security hardware, while the reflection in Task 3 outlines my commitment to continuous learning and ethical innovation. GenVault is more than just a hardware wallet, it is a response to the growing need for digital sovereignty in an increasingly volatile world. This project has not only allowed me to apply my computing skills to a real-world problem but has also prepared me for the challenges of the tech industry, where security, usability, and strategic planning must work in harmony.

References

- [1] I.V. Ponomarev, "ARCHITECTURE OF A SECURE CRYPTOCURRENCYWALLETBASED ON AIR-GAP AND MULTISIGNATURE MECHANISMS," 2026, Accessed: Apr 6, 2026. Available at: <https://journals.nmetau.edu.ua/index.php/st/article/view/2275/1513>.
- [2] M. Mary Shanthi Rani and K.Rosemary Euphrasia, "DATA SECURITY THROUGH QR CODE ENCRYPTION AND STEGANOGRAPHY," March 2016, Accessed: Apr 6, 2026. Available at: https://d1wqtxts1xzle7.cloudfront.net/45560032/7216acij01-libre.pdf?1463031344=&response-content-disposition=inline%3B+filename%3DDATA_SECURITY_THROUGH_QR_CODE_ENCRYPTION.pdf&Expires=1775488887&Signature=boJ8KOFajC1uVBjDUSfYOdXpTMR~FHIkvPCH~QD-rIIjlAmpSgSmdVfLV7yR~ghowh30s6NPKTdCe2KPcg7V-uBnaRYV~M7cgzSglcGzG6KaeVjlyWRIw~h3VuHlcYhDOy44~WZdu25Sju6a5bF7~7CgaANMoF7DrulHwaUX2yzgjavaxM1MZjmMhW6lUgOOon-7QdGCnNLg97z-con3U7eSgYahXtEBKww0KL5m2tvI5w4NMOoMBI6SuH2ekVITl21LVdkGISqOY72r5K8KI-ZgZvARFwPlgljKGzvpbwlw8kQG8ffn6DUgWxzBjWpiEMhupn0~WrfODru~DmZIQ_&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA.
- [3] Chutian Jiang, Emily Kuang and Mingming Fan, "How Can Haptic Feedback Assist People with Blind and Low Vision (BLV): A Systematic Literature Review," February 08 2025, Accessed: Apr 6, 2026. Available at: <https://dl.acm.org/doi/epdf/10.1145/3711931>.
- [4] SOFIA HAGLUND and CAROLINE SVENSSON, "Agile into Traditional Organizations and Hardware Development," 2016, Accessed: Apr 6, 2026. Available at: <https://odr.chalmers.se/server/api/core/bitstreams/38db68ad-78cc-4cc8-9801-58c9b38ba1f4/content>.
- [5] G. Mkrtchyan and H. Treiblmaier, "Business Implications and Theoretical Integration of the Markets in Crypto-Assets (MiCA) Regulation," vol. 4, no. 2, pp.11, /6 2025, doi: 10.3390/fintech4020011. Accessed: Apr 16, 2026. Available at: <https://www.mdpi.com/2674-1032/4/2/11>.
- [6] G. G. Battu, "AI-Driven Data Analytics in Custody Services: Enhanced Reporting, Compliance, and Risk Management," *International Journal of All Research Education & Scientific Methods*. vol. 13, pp.2455–6211, -04-17 2025, doi: 10.56025/IJARESM.2025.1304253385. Accessed: Apr 16, 2026. Available at: https://www.researchgate.net/profile/Geol-Gladson-Battu-2/publication/391229936_AI-Driven_Data_Analytics_in_Custody_Services_Enhanced_Reporting_Compliance_and_Risk_Management/links/680f40d2bfbe974b23bc8925/AI-Driven-Data-Analytics-in-Custody-Services-Enhanced-Reporting-Compliance-and-Risk-Management.pdf.

- [7] Aniruddh Vadlamani and Sarthak Sharma†, "BRIDGING THE DIVIDE BETWEEN DEFI AND REGULATORS: SHOWCASING DECENTRALIZED AUTONOMOUS GOVERNANCE AS THE FUTURE FOR SELF-CUSTODY WALLET REGULATION," Accessed: Apr 16, 2026. Available at: https://illinoisjlt.com/file/214/Vadlamani%20Sharma_2023_Issue%202.pdf.
- [8] Y. Kethepalli, R. Joseph, S. R. Vajrala, J. Vemula and N. S. Naik, "Reinforcing Security and Usability of Crypto-Wallet with Post-Quantum Cryptography and Zero-Knowledge Proof." Accessed: Apr 16 2026. [Online]. Available: <http://arxiv.org/abs/2308.07309>
- [9] Yi-Chun Yang and Ren-Song Tsay, "A Systematic Hardware Solution for GDPR Compliance," 2025, Accessed: Apr 16, 2026. Available at: https://sasimi.jp/new/sasimi2025/files/archive/pdf/p145_R2-12.pdf.
- [10] Avijit Dutta, "HUMAN FACTORS AFFECTING DIGITAL SECURITY," 31 jan 2021, Accessed: Apr 16, 2026. Available at: <https://pdfs.semanticscholar.org/6a1f/bdbe347115e8e99561e52f47842f4465621d.pdf>.
- [11] Alexandra Giannopoulou, "Digital Identity Infrastructures: a Critical Approach of Self-Sovereign Identity," 11 May 2023, Accessed: Apr 16, 2026. Available at: <https://link.springer.com/content/pdf/10.1007/s44206-023-00049-z.pdf>.
- [12] BADIS HAMMI, SHERALI ZEADALLY and JAMEL NEBHEN, "Security Threats, Countermeasures, and Challenges of Digital Supply Chains," July 2023, Accessed: Apr 16, 2026. Available at: <https://dl.acm.org/doi/pdf/10.1145/3588999>.
- [13] Stefan Heyse, "POST QUANTUM CRYPTOGRAPHY: IMPLEMENTING ALTERNATIVE PUBLIC KEY SCHEMES ON EMBEDDED DEVICES," October 2013, Accessed: Apr 16, 2026. Available at: <https://informatik.rub.de/wp-content/uploads/2021/11/thesis-stefan-heyse.pdf>.