



HN/BSC COMPUTING PORTFOLIO

Changemakers: Creativity and Value Creation



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: Ideation & Mind Map	2
Financial Empowerment via Secure Blockchain Nodes	3
Eliminating Single-Point Failure: The Multi-Device Vault Evolution	3
Personal Interests	3
The Selected Project	4
Universal IoT Security & Physical Trust Hub	4
Task 2: Aim & Objectives and Research area	5
Project Aim and Objectives	5
Research Philosophy	6
Search Tools and Research Databases	6
Task 3: Research Strategies	7
Validity, Reliability and Ethical Considerations	7
Research Strategies and Pilot Design	7
Quantitative and Qualitative Analysis	8
Conclusion.....	8
References	9
Appendix	10
Section 1: Pilot Survey Design and Ethical Consent	10
Section 2: Quantitative Data Analysis (Statistical Results)	11
Section 3: Qualitative Data Analysis (Open-Ended Responses).....	13

Introduction

In this assessment, the Changemakers: Creativity & Value Creation module will help me to develop skills for identifying opportunities and creating real value in society. My goal is to understand the link between design thinking and research, and how these methods can create useful ideas that help both individuals and the wider community.

Through this portfolio, I will carry out research analysis and use critical thinking to explore different ideas and possible solutions. This process helps me learn how to evaluate information, question assumptions, and develop stronger concepts. These skills are important for my future modules, especially Emerging Trends and the Independent Project in my final year. My focus is on the process of ideation and research. I am using this module to turn my personal interests into a clear and structured project plan that could create positive value and benefit society.

Task 1: Ideation & Mind Map

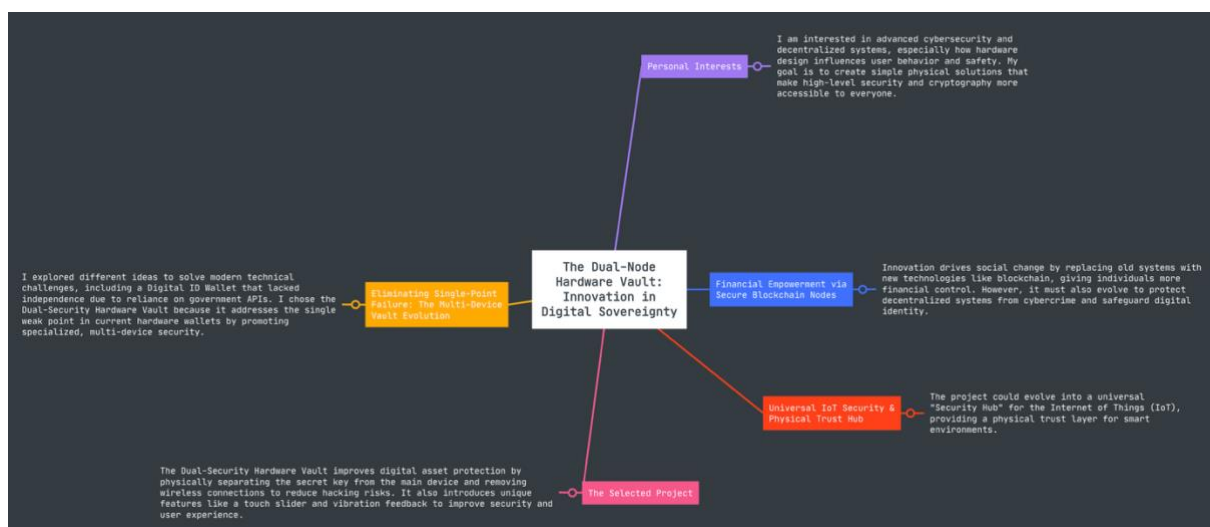


Figure 1: Mind Map

Financial Empowerment via Secure Blockchain Nodes

Innovation is the main driver of social change, acting as a force that replaces outdated systems with better and more efficient solutions for everyone. Throughout history, progress has happened because new ideas challenged old structures and improved the way society functions. It explains how modern technologies, such as blockchain, are transforming traditional financial systems by reducing the need for intermediaries and increasing transparency, creativity is essential to balance easy online access with strong asset protection. As more services move online, risks also increase. By shifting power from central institutions to individuals, innovation promotes real financial independence and personal control over data and assets. However, as decentralized systems become more widely used, innovation must also focus on advanced security measures to reduce cybercrime, prevent identity theft, and protect digital identity on a global scale.[1]

Eliminating Single-Point Failure: The Multi-Device Vault Evolution

To arrive at my final project, I explored several concepts focused on solving modern technical challenges.

Idea A: Digital ID Wallet. This concept offered great societal value for privacy but relied too heavily on third-party government APIs, which limited its independence and security.

Idea B (Selected): The Dual-Security Hardware Vault. This idea was chosen because it solves a clear known problem: the single weak point found in current all-in-one hardware wallets. It shows a move toward specialized, multi-device security.[2]

Personal Interests

My interests are in advanced cybersecurity and the complex structure of decentralized systems. I am especially interested in how hardware design affects user behaviour and overall safety. I want to understand how the physical form of a device can influence the way people interact with security tools and reduce human error. My goal is to use creative thinking to design practical physical solutions that make high-level security accessible to a wider audience, not just experts. This project allows me to explore how hardware development, including strong metal machining and secure component design, can solve real-world security weaknesses.

I aim to connect complex cryptographic systems with simple, intuitive, and user-friendly physical interfaces.

The Selected Project

The Dual-Security Hardware Vault is a new solution made to change how we protect digital assets. Unlike market leaders that keep everything on one device, this project creates a physical split between the “Secret Key” (stored on a simple USB device) and the “Brain” (the main device).[3]

Novel Features: It includes a touch slider on the side for navigation, keeping the main screen clear for transaction checks. It also has a vibration system to give physical feedback, so the user feels every approval step.

Value Creation: By using air-gapped communication through QR codes and removing Bluetooth and Wi-Fi, the device removes the main wireless attack risks. This makes sure the user’s private keys never connect to the internet, offering a higher level of security than current standard solutions.[4]

Universal IoT Security & Physical Trust Hub

The final stage of this idea process focuses on the long-term future of the Hardware Vault in a rapidly changing digital world. As quantum computing continues to develop, current cryptographic systems may become vulnerable, making post-quantum cryptography a key area for future research and development. For this reason, the project is designed to be scalable and adaptable over time. It can evolve from a simple digital asset wallet into a universal “Security Hub” for the Internet of Things (IoT). By creating a strong physical layer of trust, the device could provide secure authentication, identity protection, and safe communication for smart homes, devices, and connected environments.[5]

Task 2: Aim & Objectives and Research area

Project Aim and Objectives

The main aim of this research project is to design and conceptualize a “Dual-Node Hardware Vault.

Which is a special security device specifically made to remove the single point of failure that is so common in current digital asset storage solutions. Most wallets store everything on one chip, which creates a huge risk. By physically separating the sensitive cryptographic “Secret Key” from the main "Brain" or user interface, this project aims to provide a brand-new solution for people who want full financial control and digital sovereignty in a decentralized economy. This separation ensures that even if one part of the device is compromised, the actual funds remain untouchable.

To achieve this ambitious goal, I have set several clear objectives.

The objectives are:

- Carry out a detailed analysis of existing hardware weaknesses found in popular wallets, focusing specifically on how wireless attack methods like Bluetooth and Wi-Fi can be broken or intercepted by hackers.[6] Understanding these flaws is vital to building a better system.
- Create a strong and reliable system design using “Air-Gapped” communication methods. This includes using encrypted QR codes to transfer data between the two nodes, which makes sure that private data never actually touches an internet-connected device or a wireless signal.[7]

The project aims to include advanced physical features to improve the user experience and security. This involves a touch slider for smooth navigation on the side of the device and a haptic system to give the user a clear, tactile transaction confirmation.[8] This physical interaction adds a layer of safety that software alone cannot provide. Finally, the success of the vault will be tested through rigorous security checks and stress tests. These evaluations will make sure the prototype stays completely safe against both remote cyber-attacks and direct physical damage or tampering, proving it is a reliable tool for long-term asset protection.

Research Philosophy

Identifying a suitable research philosophy is important for guiding the development of this technical project. For the Hardware Vault, I have chosen a Pragmatic research philosophy. Pragmatism is well suited for applied computing because it focuses on practical, real-world solutions instead of complex theoretical ideas. [9] In this context, the value of the research is judged by “what works” to solve the main problem of cyber-theft in the blockchain environment. This approach allows me to use a mixed-methods strategy, combining quantitative technical data from cryptographic performance with qualitative evaluation of Human-Computer Interaction (HCI). In the context of my Hardware Vault, the relationship with HCI is central, a security device is only effective if a human can operate it without making fatal errors. For example, many crypto losses happen because of "human error" during complex transactions. By focusing on the practical use of design thinking, the pragmatic approach ensures that the final product is not only technically secure but also simple, clear, and easy to use for the end user, creating real value for society.

Search Tools and Research Databases

To find the right information for my research, I will use several professional search tools and databases. I will use IEEE Xplore and the ACM Digital Library to find high-quality papers on hardware security and how to build secure circuits. I will also use Google Scholar to look for the latest studies on blockchain vulnerabilities and Air-Gap technology. To make sure my project follows official safety rules, I will check the NIST Digital Library for government security standards. My strategy is to use specific keywords like "Hardware Wallet Security" and "QR code encryption" to filter out useless info and find exactly what I need to make my Dual-Node Vault a success.[10]

Task 3: Research Strategies

Validity, Reliability and Ethical Considerations

To ensure the academic integrity of my project, I must focus on the validity and reliability of my research data. Validity means how accurately a method measures what it is meant to measure for my Hardware Vault, this means making sure that my survey questions really test a user's security habits rather than just their basic tech knowledge [11]. To achieve reliability, I will standardize my data collection process so that if another researcher repeats my study, they will get similar results.

I must consider generalisability, which is the extent to which my findings from a small group of students can be applied to the wider global crypto community. On the ethical side, I will follow strict ethical rules by making sure all participants give informed consent. Their data will be kept anonymous and stored safely, and they will have the right to withdraw from the study at any time, making sure that my research respects privacy and follows university guidelines.[12]

Research Strategies and Pilot Design

For this project, I have selected a Survey (Questionnaire) as my main data collection method. This quantitative method is ideal for collecting data from many people about their fears of cyber-attacks and their willingness to use a physical "Air-Gapped" device. To improve my research, I created a pilot data collection method with a short 5 questions survey. I shared this pilot with a small group of three computing classmates to test the clarity of my technical terms.

As shown in the Appendix, the feedback I received suggested that terms like "Dual-Node" and "Asymmetric Encryption" were too difficult for non-experts. Based on this feedback, I improved the focus of my project by adding simple explanations and visual diagrams to my final survey. This pilot phase was important to avoid confusion and ensure that the final data collected is clear, reliable, and useful for the development of the vault. [13]

Quantitative and Qualitative Analysis

Understanding the different types of data analysis is important for interpreting my results. Quantitative analysis involves looking at “the numbers” and using simple statistics, such as percentages and averages, to identify trends. For example, I can calculate what percentage of users prefer a physical touch-slider instead of a touch screen for security reasons. If I ask open-ended questions about why people do not trust current wallets, I will use thematic analysis to group their answers into common themes like “fear of hacking” or “difficulty of use.” By combining both numerical data (quantitative) and theme-based insights (qualitative), I can get a full understanding of market needs and technical requirements for my project, making sure the Hardware Vault provides real value to its users. [14]

Conclusion

In conclusion, this project has allowed me to apply the principles of the Changemakers: Creativity & Value Creation module to an important real-world problem in digital security. By moving through the stages of ideation, research, and method design, I have turned a personal interest in blockchain technology into a clear proposal for the Dual-Node Hardware Vault.

This process has shown me that true innovation is not only about technical complexity, but about solving real problems in a practical way. By focusing on Human-Computer Interaction and removing single points of failure, my project aims to give individuals the tools they need for financial control and data protection. In addition, the research methods I have developed including the use of a pilot study to improve my data collection ensure that the project is based on reliable data and ethical standards.

As I move toward my final year of study, the knowledge gained during this module will provide a strong foundation for my Emerging Trends and Independent Project. I am now better prepared to identify opportunities, carry out detailed research, and create long-term value for society through innovative computing solutions.

References

- [1] L. Westcott. "How does innovation impact society?" Digital Leaders. (-02-242021). Accessed: Feb 24, 2026. [Blog]. Available at: <https://digileaders.com/how-does-innovation-impact-society/>
- [2] Dylan Yaga, Peter Mell, Nik Roby and Karen Scarfone, "Blockchain Technology Overview," October 2018, Accessed: Feb 24, 2026. Available at: <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf>
- [3] Ledger. "What Is a Hardware Wallet?" Ledger. (Oct 242025). Accessed: Feb 24, 2026. [Blog]. Available at: <https://www.ledger.com/academy/crypto-hardware-wallet>
- [4] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Accessed: Feb 24, 2026. Available at: <https://bitcoin.org/bitcoin.pdf>
- [5] CLOUDFLARE. "What is post-quantum cryptography (PQC)?" Accessed: Feb 26, 2026. [Online]. Available: <https://www.cloudflare.com/learning/ssl/quantum/what-is-post-quantum-cryptography/>
- [6] Sergei Volokitin, "Software attacks on hardware wallets," 2018, Accessed: Mar 18, 2026. Available at: <https://i.blackhat.com/us-18/Wed-August-8/us-18-Volokitin-Software-Attacks-On-Hardware-Wallets-wp.pdf>
- [7] A. G. Khan, et al., "Security Of Cryptocurrency Using Hardware Wallet And QR Code", pp. 1–10. [Online].doi:10.1109/ICIC48496.2019.8966739.Available: <https://ieeexplore.ieee.org/abstract/document/8966739/citations>.
- [8] D. R. Agrawal and E. Agrawal, "User Authentication Based on Haptic: A Systematic Review." Accessed: Mar 18 2026. [Online]. Available: <https://www.researchsquare.com/article/rs-6543696/v1>
- [9] D. L. Morgan, "Pragmatism as a Paradigm for Social Research," vol. 20, no. 8, pp.1045–1053, October 1 2014, Doi: 10.1177/1077800413513733. Accessed: Mar 18, 2026. Available at: <https://doi.org/10.1177/1077800413513733>.
- [10] Boris Chigarev *, "Analysis of the Use of Author Keywords and IEEE Terms in IEEE Xplore Data to Identify Current Research Topics in Energy Technology and Existing Limitations," 2 October 2025, Accessed: Mar 18, 2026. Available at: https://www.preprints.org/frontend/manuscript/ec53caa9357d935eab2d504cdefb413c/download_pub.
- [11] Christopher D. Mellinger and Thomas A. Hanson, "View of Methodological considerations for survey research: Validity, reliability, and quantitative analysis," 20-01 2021, Accessed: Mar 24, 2026. Available at: <https://artojs02.uantwerpen.be/index.php/LANS-TTS/article/view/549/548>.
- [12] ELIZABETH A, BUCHANAN and ERIN E. HVIZDAK, "ONLINE SURVEY TOOLS: ETHICAL AND METHODOLOGICAL CONCERNS OF HUMAN RESEARCH ETHICS COMMITTEES," 5/14/09 Accessed: Mar 24, 2026. Available at: https://sites.pitt.edu/~peterb/papers/JER0402_05.pdf.
- [13] Edwin R., Teijlingen and Vanora Hundley, "The importance of pilot studies," 2001, Accessed: Mar 24, 2026. Available at: https://eprints.bournemouth.ac.uk/10149/1/SRU35_pilot_studies.pdf.

[14] YOLANDE DE E. CHAN, "IT Value: The Great Divide Between Qualitative and Quantitative and Individual and Organizational Measures," 2000, Accessed: Mar 24, 2026. Available at: https://www.floppybunny.org/robin/web/virtualclassroom/chap11/s3/articles/it_value_qual_quant_2000.pdf.

Appendix

Section 1: Pilot Survey Design and Ethical Consent

This section shows the initial design of the survey used for the pilot study. As mentioned in Task 3, the survey includes an informed consent statement to ensure all participants are aware that their data is anonymous and used strictly for academic purposes.

User Perception of Dual-Node Security and Air-Gapped Hardware Vaults

All data collected is anonymous and used for academic purposes only. By completing this survey, you give your informed consent.

1. How often do you move your digital assets from an exchange to a private wallet? *

☐ After every transaction

☐ Monthly

☐ Rarely

☐ Never

2. On a scale of 1-5, how worried are you about wireless hacking (Bluetooth/Wi-Fi) on your current devices? *

☐ 5 (Extremely worried)

☐ 4

☐ 3

☐ 2

☐ 1 (Not worried)

3. Would you prefer using a "Dual-Node" system (two separate devices) if it meant your private keys were 100% offline (Air-Gapped)? *

☐ Yes

☐ No

☐ Maybe

4. Which physical interaction do you find more secure for confirming a transaction? *

☐ Using a physical capacitive touch-slider

☐ Clicking a touch screen

5. In your own words, what is your biggest fear when using a hardware wallet?

Enter your answer

[Add new question](#)

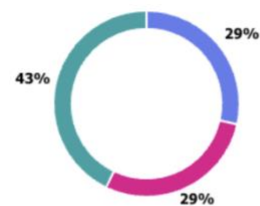
Section 2: Quantitative Data Analysis (Statistical Results)

The following charts represent the quantitative data collected during the pilot phase. These statistics help identify market trends and user preferences regarding "Air-Gapped" security and physical interaction (HCI).

1. How often do you move your digital assets from an exchange to a private wallet?

[More details](#)

After every transaction	2
Monthly	2
Rarely	3
Never	0



2. On a scale of 1-5, how worried are you about wireless hacking (Bluetooth/Wi-Fi) on your current devices?

[More details](#)

5 (Extremely worried)	4
4	1
3	2
2	0
1 (Not worried)	0



3. Would you prefer using a "Dual-Node" system (two separate devices) if it meant your private keys were 100% offline (Air-Gapped)?

[More details](#)

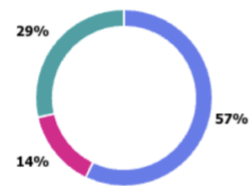
Yes	4
No	1
Maybe	2



3. Would you prefer using a "Dual-Node" system (two separate devices) if it meant your private keys were 100% offline (Air-Gapped)?

[More details](#)

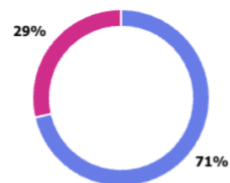
● Yes 4
● No 1
● Maybe 2



4. Which physical interaction do you find more secure for confirming a transaction?

[More details](#)

● Using a physical capacitive touch-slider 5
● Clicking a touch screen 2



5. In your own words, what is your biggest fear when using a hardware wallet?

[More details](#)

7
Responses

Latest Responses

"My biggest fear is a 'supply chain attack' where the hardware is tampered with bef..."

"I worry that a hacker could find a backdoor in the firmware if the device is connect..."

"My fear is that the battery or the screen might fail after a few years, making it imp..."

...

The data confirms a high level of concern regarding wireless vulnerabilities (Bluetooth/Wi-Fi), which validates the necessity of the "Dual-Node" hardware separation proposed in this project.

Section 3: Qualitative Data Analysis (Open-Ended Responses)

This section contains the raw feedback from the participants regarding their primary fears in digital asset storage.

r ×

5. In your own words, what is your biggest fear when using a hardware wallet?

7 Responses

ID ↑	Name	Responses
1	anonymous	I am terrified of a sophisticated remote attack through Bluetooth while I am confirming a transaction.
2	anonymous	I fear losing the physical device and not having a secure enough backup system to recover my assets.
3	anonymous	I find current wallets too difficult to use for daily transactions, which makes me feel insecure about the whole process.
4	anonymous	I am worried about 'blind signing' where I don't fully understand what the smart contract is doing with my keys.
5	anonymous	My fear is that the battery or the screen might fail after a few years, making it impossible to sign transactions.
6	anonymous	I worry that a hacker could find a backdoor in the firmware if the device is connected to a PC via USB.
7	anonymous	My biggest fear is a 'supply chain attack' where the hardware is tampered with before I even buy it.