**MSc. in Computing**

**Practicum Approval Form**

# Section 1: Student Details

|  |  |
| --- | --- |
| Project Title: | Towards Trustworthy AI: Blockchain-based Architecture Design for Internet of Things (IoT)" |
| Student ID: | 21268168, 21267549 |
| Student name: | Vishal Padwal, Vipul Popat, |
| Student email | [vishal.padwal2@mail.dcu.ie](mailto:vishal.padwal2@mail.dcu.ie), [vipul.popat2@mail.dcu.ie](mailto:vipul.popat2@mail.dcu.ie), |
| Chosen major: | MCM - M.Sc. in Computing - Blockchain |
| Supervisor | Irina Tal |
| Date of Submission | 11/11/2022 |

# Section 2: About your Practicum

Please answer all questions below. Please pay special attention to the word counts in all cases.

**What is the topic of your proposed practicum? (100 words)**

Very little research has been conducted on applying trustworthy AI principles to the Internet of Things (IoT). For IoT to be implemented with Trustworthy AI principles, there is a need for a generic architecture. The aim of this study is to propose an architecture that incorporates the seven principles of Trustworthy AI, as well as to apply this architecture to a concrete use case involving an IoT vertical. Additionally, we aim to demonstrate the end-to-end application of trustworthy AI through a proof of concept of this architecture.

**Please provide details of the papers you have read on this topic (details of 5 papers** expected).

References

[1] D. Svetinovic, ‘Keynote 3: Blockchain — IoT — AI Trust Nexus; Keynote 3: Blockchain — IoT — AI Trust Nexus’, SNAMS, 2019.

[2] S. C. Ch, S. Puli, K. L. Viveka, και M. V. B. T. Santhi, ‘Machine Learning Based Data Security Model Using Blockchain for Secure Data Transmission in IoT’, 8 2021, σσ. 1521–1527.

[3] C. A. Ardagna, R. Asal, E. Damiani, N. E. Ioini, M. Elahi, και C. Pahl, ‘From trustworthy data to trustworthy IoT: A data collection methodology based on blockchain’, ACM Transactions on Cyber-Physical Systems, τ. 5, 1 2021.

[4] N. Petrovic, Model-Driven Approach to Blockchain-Enabled MLOps. 2022.

[5] Z. Gong-Guo και Z. Wan, ‘Blockchain-based IoT security authentication system’, Proceedings - 2021 International Conference on Computer, Blockchain and Financial Development, CBFD 2021. Institute of Electrical and Electronics Engineers Inc., σσ. 415–418, 2021.

[6] ‘HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE SET UP BY THE EUROPEAN COMMISSION ETHICS GUIDELINES FOR TRUSTWORTHY AI’. .

[7] S. K. Lo κ.ά., ‘Towards Trustworthy AI: Blockchain-based Architecture Design for Accountability and Fairness of Federated Learning Systems’, IEEE Internet of Things Journal, 2022.  
  
**How does your proposal relate to existing work on this topic described in these papers?** (200 words)

Despite our efforts, we could only observe one keynote [1] published on blockchain - AI - IoT nexus, nor could we find any evaluation of Trustworthy AI principles [6] [2] on this nexus in any of the journals we reviewed.

Much research has been done on the interconnection but in isolation between blockchain technology, the Internet of Things (IoT) [5], and artificial intelligence (AI). However, this nexus should be explored more extensively using trustworthy AI principles [6].

It is important to remember that there is a need to apply Trustworthy AI principles on this nexus for the consumers to have more confidence and trust in the solutions leveraging these platforms. There has been a lot of research done in various research papers, but it has yet to be done in conjunction with a nexus of these technologies. This proposal aims to produce fresh architecture design [7] and to link all three technologies together for future development using trustworthy AI principles defined by the European Union.

**What are the research questions that you will attempt to answer?** (200 words)

Cryptocurrencies, such as Bitcoin, use blockchain technology as part of their underlying technology, and it is being used in many new software systems. In the same way that the Internet revolutionised the development of software systems in a way similar to what the blockchain has done, the blockchain's innovative approach to decentralised computation and asset management could solve a number of system scaling, reliability, security, and privacy problems. As a result of the alignment of blockchain, artificial intelligence (AI), and the Internet of Things (IoT), a promising new research and development pathway has been created, attracting significant investment and funding. In terms of why one might not be able to trust today's AI algorithms because they do not explain the rationale behind their decisions can be seen as one of the main concerns.

A blockchain - AI - IoT system can be more trustworthy and explainable by leveraging smart contracts, trusted oracles, and decentralised storage. The framework discussed here addresses the problem of applying trustworthy AI principles to complex AI systems that use federated or centralised learning systems. In conclusion, we discuss key application areas and their practical applications. We aim to develop a proof of concept using this generic framework.

Research Question’s:

1. How have the trustworthy AI Principle been Applied to the modern technologies such as Blockchain, Artificial Intelligence (AI) and Internet of things (IoT).
2. What are the different frameworks available where trustworthy AI Principles have been applied.
3. How would you apply the trustworthy AI Principles using a generic Framework on a concrete use case.
4. What effect would Application of Trustworthy AI Principles will have on end user’s

How will you explore these questions? (Please address the following points. Note that three or four sentences on each will suffice.)

* What software and programming environment will you use?
* **Amazon Sagemaker for MLOps, Decentralized storage IPFS or Arweave,**
* What coding/development will you do?
* **Smart contracts to push models and their metadata to blockchains. Invoke smart contract from MLOps**
* What data will be used for your investigations?
* **Once we define a concrete use case, we will furnish details on the data**
* Is this data currently available, it not, where will it come from?
* ***Kaggle***
* What experiments do you expect to run?
* ***Brief outline of Trustworthy AI Principle to Proposed Architecture***
* What output do you expect to gather?
* ***The new Architecture with a combination of Three technologies using 7 trustworthy AI Principles.***
* How will the results be evaluated?
* ***New Architecture with nexus of three technologies against 7 trustworthy AI principles.***