EDINBURGH NAPIER UNIVERSITY SCHOOL OF COMPUTING

MSc RESEARCH PROPOSAL

The process of completing and reviewing the contents of this form is intended ensure that the proposed project is viable. It is also intended to increase the chances of a good pass. Much of the material produced while completing this form may be reused in the dissertation itself.

1. **Student details**

|  |  |
| --- | --- |
| First name | Nnamdi |
| Last (family) name | Nwosu |
| Napier matriculation number | 40224579 |

2. **Details of your programme of study**

|  |  |
| --- | --- |
| MSc Programme title | Computing |
| Year that you started your diploma modules |  |
| Month that you started your diploma modules | January |
| Mode of study of diploma modules | Full-time |
| Date that you completed/will complete your diploma modules at Napier |  |

3. **Project outline details**

Please suggest a title for your proposed project. If you have worked with a supervisor on this proposal, please provide the name. You are strongly advised to work with a member of staff when putting your proposal together.

|  |  |
| --- | --- |
| Title of the proposed project | Privacy Preservation of Blockchain |
| Is your project appropriate to your programme of study? | Yes |
| Name of supervisor | Liam Bell |
| I do not have a member of staff lined up to supervise my work |  |

4. **Brief description of the research area - background**

Please do not describe your project in this section. Instead, provide background information in the box below on the broad research area in which your project sits. You should write in narrative (not bullet points). The academic/theoretical basis of your description of the research area should be evident through the use of citations and references. Your description should be between half and one page in length.

|  |
| --- |
| The dissertation is about the preservation of private blockchain in healthcare. Blockchain technology is a game-changer with the potential to positively affect many industries. Blockchain has the potential to push transformation in preventive care and community-based healthcare systems. The capacity (IBM Blockchain, 2017).  The blockchain innovation has made its way to the healthcare sector, and it’s only the beginning of what is obtainable. Healthcare Rallies for Blockchain is a study from IBM which found that 16% of surveyed healthcare executives had concrete plans on implementing a commercial blockchain solution this year, whilst 56% percent expected to by 2020 (Bernard Marr, 2017).  The concept of “private blockchains” has become very popular in the wider blockchain technology discussion. Essentially, instead of having state machine secured by crypto-economics (e.g. Proof of work, proof of stake) and fully public and uncontrolled network, it is doable to create a system where access permissions are more tightly controlled, with some rights restricted to blockchain users, whilst continue maintaining many kinds of decentralization and partial guarantees of authenticity and decentralization that blockchains provide (Vitalik Buterin, 2015).  Zero Knowledge Proofs (ZKPs) were first conceptualized in 1985 in a paper “The knowledge Complexity of Interactive Proof Systems”. It is a cryptographic technique that makes it possible for two parties (a prover and a verifier) to prove that a proposition is true, without disclosing any information about it apart from it being true (George Samman, 2016).  The aim of this projects is to design and implement a healthcare application that can save patients’ records in a decentralized and immutable model using Ethereum smart contracts to demonstrate the usefulness of blockchain in healthcare system. |

5. **Project outline for the work that you propose to complete**

Please complete the project outline in the box below. You should use the emboldened text as a framework. Your project outline should be between half and one page in length.

|  |
| --- |
| **The idea for this research arose from:**  I am a blockchain enthusiast, and I had done some research on Neo formerly Antshare, Lisk, Dash (Privacy blockchain) and Ethereum Smart contracts.  Finally, Prof Bill Buchanan (OBE) enthusiasm in blockchain also made me believe that it is the future and will be disruptive like the internet.  **The aims of the project are as follows:**  The aim of this project is to demonstrate the need for private blockchain in healthcare system, and the coverage of different blockchain technologies such as Ethereum, Zk-Snarks, Neo, Hyperledger and Lisk, and finally, an application will be designed to demonstrate the application of Ethereum smart contract in healthcare.  **The main research questions that this work will address include:**   * How does zero knowledge proof help in privatization of blockchain? * What are the needs for using private blockchain in healthcare system, why not public blockchain? * How can distributed ledgers be used for the sharing of medical data between organisations and how can this affect patient care?   **The software development/design work/other deliverable of the project will be:**  The software will deliver a demo application that demonstrates the use of Ethereum’s smart contracts in healthcare using liver cancer risk factors as a use case.  **The project deliverable will be evaluated as follows:**  The application is expected to have a web interface for personal information inputs.  Ethereum’s smart contract will power the backend which will accept patients’ information from the frontend and saves it on blockchain. Test server maybe used in hosting it as I don’t think I can afford to invest in gas (Ether).  **The project will involve the following research/field work/experimentation/evaluation:**   * Smart contracts. * Private Blockchain in healthcare * Zero knowledge proof. * Other blockchain technologies.     **This work will require the use of specialist software: YES**  **This work will require the use of specialist hardware:NO**  **The project is being undertaken in collaboration with: Initial report week 8** |

6. **References**

Please supply details of all the material that you have referenced in sections 4 and 5 above. You should include at least three references, and these should be to high quality sources such as refereed journal and conference papers, standards or white papers. Please ensure that you use a standardised referencing style for the presentation of your references, e.g. APA, as outlined in the yellow booklet available from the School of Computing office and <http://www.soc.napier.ac.uk/~cs104/mscdiss/moodlemirror/d2/2005_hall_referencing.pdf> .

|  |
| --- |
| IBM unleashed, (2017). Blockchain in healthcare: Patient benefits and more. Retrieved from: ttps://www.ibm.com/blogs/blockchain/2017/10/blockchain-in-healthcare-patient-benefits-and-more/  Marr, B. (2017). This is why blockchains will transform healthcare. Retrieved from: <https://www.forbes.com/sites/bernardmarr/2017/11/29/this-is-why-blockchains-will-transform-healthcare/#35094c11ebe3>  Buterin, V. (2015). On public and private blockchains. Retrieved from: <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>  Samman, G. (2016). The trend towards blockchain privacy: Zero knowledge proofs. Retrieve from: <https://www.coindesk.com/trend-towards-blockchain-privacy-zero-knowledge-proofs/> |

7. **Ethics**

If your research involves other people, privacy or controversial research there may be ethical issues to consider (please see the information on the module website). If the answer below is YES then you need to complete a research Ethics and Governance Approval form, available on the website:   
<http://www.ethics.napier.ac.uk> .

|  |  |
| --- | --- |
| Does this project have any ethical or governance issues related to working with, studying or observing other people? (YES/NO) | NO |

8. **Confidentiality**

If your research is being done in conjunction with an outside firm or organisation, there may be issues of confidentiality or intellectual property.

|  |  |
| --- | --- |
| Does this project have any issues of confidentiality or intellectual property? (YES/NO) | NO |

9. **Supervision timescale**

Please indicate the mode of supervision that you are anticipating. If you expect to be away from the university during the supervision period and may need remote supervision please indicate.

|  |  |
| --- | --- |
| Weekly meetings over 1 trimester | This is preferable. |
| Meetings every other week over 2 trimesters |  |
| Other (what?) |  |

10. **Submitting your proposal**

1. Please save this file using your surname, e.g. macdonald\_proposal.docx, and e-mail it to your supervisor, who will discuss it with you and suggest possible improvements.
2. When your supervisor is content with your proposal, email it to your internal examiner, who will provide feedback and possibly suggestions for improving your idea.
3. Discuss your feedback from the internal examiner with your supervisor and if necessary make final changes to your proposal.
4. Upload the final version to the dissertation learning space on Moodle.
5. When you produce your dissertation, add your finalised proposal as an appendix.