Student Name: George Chavady	**Student ID: 19305272**	**Stream: M.Sc. Computer Science I.S.**	**Supervisor Name: Donal O'Mahony**

1. Research Question/Aim:

To implement an Oracle system for the QTUM blockchain considering aspects of security and integrity.

2. Research Objectives

- Understanding Bit-Coin core
- UTXO model
- Proof-of-stake consensus algorithm
- Ethereum smart contract
- Examine work on Oracles – principally on the Ethereum blockchain
- Research on QTUM blockchain eco-system
- QTUM vs Ethereum
- Information Logistics Orchestration
- Ways of implementing an oracle system to allow smart contracts to access information from the outside world for the QTUM eco-system.
- Aspects related to security and integrity of the oracle system and information logistics orchestration with the smart contracts.

3. Approach/Method to achieve objectives

- Literature review of various topics on Bit-Coin and bitcoin core.
- Understand the state of the art technologies in blockchain.
- Read literature on Ethereum smart contract.
- Understand UTXO model by reading literature.
- Read and understand information available on the QTUM blockchain ecosystem
- Research on methods that could help automate cross-organisational information logistics.
- Usage of lite wallets.
- Use of Solidity (An OOP language, used for implementing smart contracts. It targets the Ethereum Virtual Machine)
- Read literature on Oracle implementation in Ethereum blockchain.

4. Evaluation

Ask -

- Is there a logical flow in the literature review done?
- Does the knowledge gained and the literature review help us fulfil our aim/goal?
- Have we been able to achieve our aim/goal? i.e., Have we implemented a system that communicates with a smart contract from the outside world?
- Is the Oracle system secure?

Methods:

- Unit testing
- Integration testing
- System testing

5. Contribution

- Review of the various blockchain technologies. E.g., UTXO, Proof of Work, Proof of Stake, QTUM eco-system etc.
- Create an application that acts as an oracle provider to smart contract/contracts.
- Discusses aspects of security and integrity in the oracle systems.

Student Name: George Chavady	**Student ID: 19305272**	**Stream: M.Sc. Computer Science I.S.**	**Supervisor Name: Donal O'Mahony**

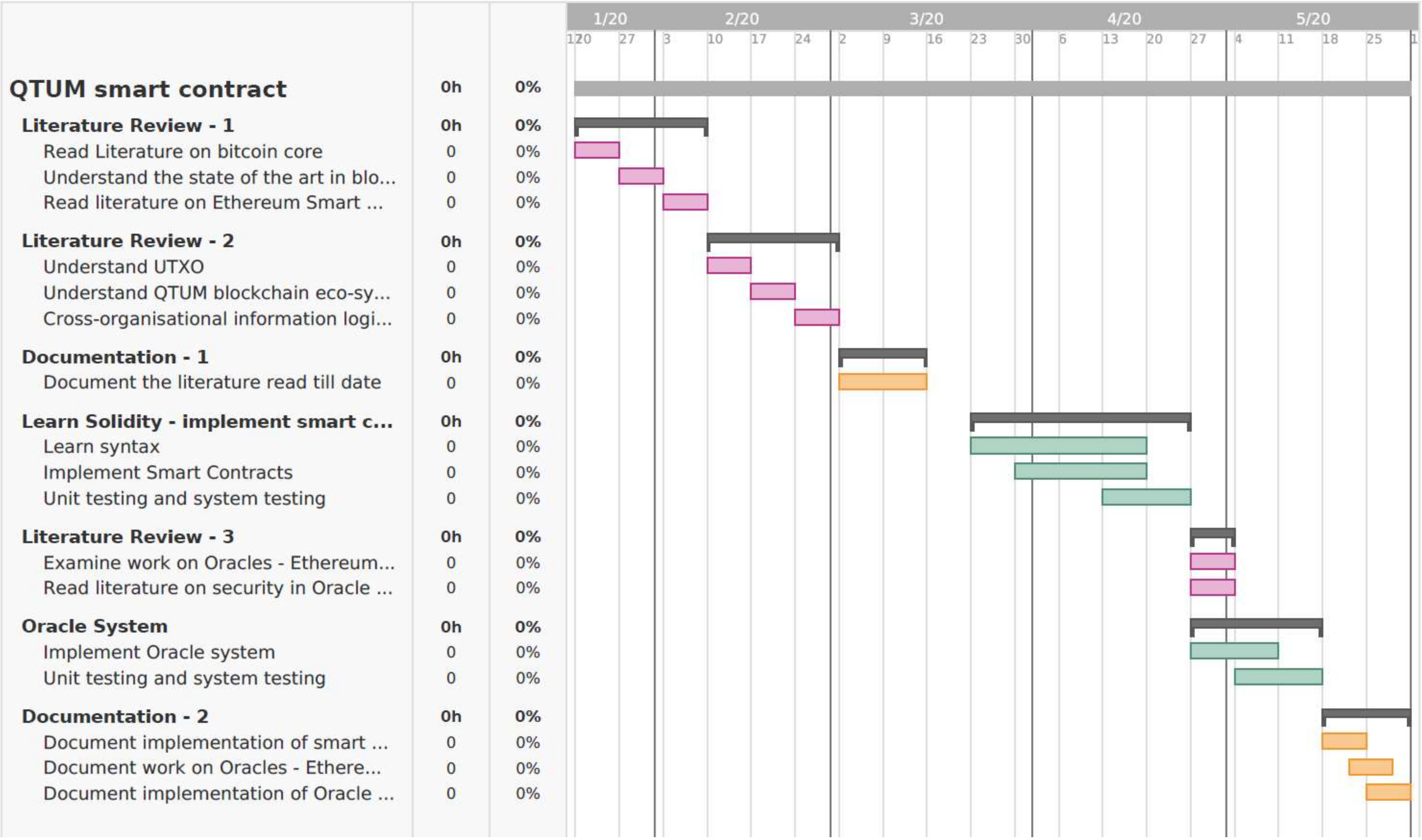
2. Motivation Statement:

Smart contracts help to digitally enforce the negotiation of contracts. They have found application in diverse domains such as financial technology, digital signing solutions etc. Smart contracts are facilitated by Ethereum Virtual Machine (EVM) and can be designed using a language called Solidity, which uses JavaScript syntax and targets the EVM. But, Ethereum uses a computationally expensive proof-of-work validation, requires downloading the entire blockchain, lacks formal semantics which is a security issue and does not facilitate cross organizational information logistics automation.

To bridge this gap the QTUM smart contract framework allows for cross organizational information logistics automation, formal semantics language expressiveness, implementation of lite wallets and use of Proof of Stake validation which is computationally less expensive. The QTUM framework also provides smart contract template libraries. Thus creation of smart contracts is made faster and secure.

The smart contracts designed using the QTUM framework requires data from the outside world to check for conditions that satisfy the contract in order to perform certain actions enforced within the contract. The data is provided to the smart contracts by so called ‘Oracles’. Through this research I aim to study the different facets related to the implementation of smart contracts using the Ethereum Virtual Machine and the QTUM eco-system. Also, I aim to research, innovate and implement a system that works as an Oracle to smart contracts developed on the QTUM smart contract framework.

3. **Gantt Chart:**



QTUM smart contract	**0h**	**0%**
Literature Review - 1	**0h**	**0%**
Read Literature on bitcoin core	0	0%
Understand the state of the art in blo...	0	0%
Read literature on Ethereum Smart ...	0	0%
Literature Review - 2	**0h**	**0%**
Understand UTXO	0	0%
Understand QTUM blockchain eco-sy...	0	0%
Cross-organisational information logi...	0	0%
Documentation - 1	**0h**	**0%**
Document the literature read till date	0	0%
Learn Solidity - implement smart c...	**0h**	**0%**
Learn syntax	0	0%
Implement Smart Contracts	0	0%
Unit testing and system testing	0	0%
Literature Review - 3	**0h**	**0%**
Examine work on Oracles - Ethereum...	0	0%
Read literature on security in Oracle ...	0	0%
Oracle System	**0h**	**0%**
Implement Oracle system	0	0%
Unit testing and system testing	0	0%
Documentation - 2	**0h**	**0%**
Document implementation of smart ...	0	0%
Document work on Oracles - Ethere...	0	0%
Document implementation of Oracle ...	0	0%

Student Name: George Chavady	**Student ID: 19305272**	**Stream: M.Sc. Computer Science I.S.**	**Supervisor Name: Donal O'Mahony**

4. Skills List:

Technical Skills:

- Understand blockchain core code.
- Understand Ethereum smart contracts
- Understand the Ethereum Virtual Machine
- Learn Solidity – a high level language used to implement smart contracts on the Ethereum Virtual Machine.
- Learn the QTUM eco-system. E.g., the opcodes used to execute transactions in the blockchain
- Learn the UTXO model
- Understand Proof of Work and Proof of Stake consensus algorithms.

Research Skills:

- Searching for the right content available out there.
- Collating content from various sources to present them in a manner that makes sense to the audience.
- Get to know of ways and methods to achieve the goal/aim.
- Learn standards used in citing sources. E.g., APA

5. Reference List:

1. Solidity. Retrieved from http://solidity.readthedocs.io/en/develop/
2. Patrick Dai, Neil Mahi, Jordan Earls, Alex Norta. Smart-Contract Value-Transfer Protocols on a Distributed Mobile Application Platform. Retrieved from https://old.qtum.org/user/pages/03.tech/01.white-papers/Qtum%20Whitepaper.pdf
3. Ghassan Karame, Elli Androulaki. (2016). Bitcoin and blockchain security. Boston: Artech House.
4. BitcoinCore. Retrieved from https://bitcoin.org/en/bitcoin-core/help
5. Cong T. Nguyen, Dinh Thai Hoang, Diep N. Nguyen, Dusit Niyato, Huynh Tuong Nguyen, Eryk Dutkie. (2019, June 26). Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities. Retrieved from https://ieeexplore-ieee-org.elib.tcd.ie/document/8746079
6. Leonor Augusto, Ruben Costa, José Ferreira, Ricardo Jardim-Gonçalves. (2019, June 20). An Application of Ethereum smart contracts and IoT to logistics. Retrieved from https://ieeexplore-ieee-org.elib.tcd.ie/document/8740823
7. Andreas M. Antonopoulos, Dr. Gavin Wood. (2018). Mastering Ethereum : building smart contracts and Dapps. CA: O'Reilly Media, Inc.
8. Xiaolong Liu, Riqing Chen, Yu-Wen Chen, Shyan-Ming Yuan. (2019, July 11). Off-chain Data Fetching Architecture for Ethereum Smart Contract. Retrieved from https://ieeexplore-ieee-org.elib.tcd.ie/document/8756348
9. Xiaolong Liu, Khan Muhammad, Jaime Lloret, Yu-Wen Chen, Shyan-Ming Yuan. (2019). Elastic and cost-effective data carrier architecture for smart contract in blockchain. Volume 100, 590-599.
10. Mik, Eliza. (2017). Smart contracts: terminology, technical limitations and real world complexity. 9(2). 269-300.
11. Oraclize. Retrieved from http://dev.oraclize.it
12. L. Luu, D.H. Chu, H. Olickel, P. Saxena, A. Hobor. (2016). Making Smart Contracts Smarter. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16, 254-269.

Student Name: George Chavady	**Student ID: 19305272**	**Stream: M.Sc. Computer Science I.S.**	**Supervisor Name: Donal O'Mahony**

6. Ethics Statement:

No, I do not need an ethics approval at this point. Because, my research doesn’t involve conducting interviews or collecting data through questionnaires. It is only the application that would be evaluated. The dissertation involves studying the state of the art in the field of Smart Contracts and implementing the same using QTUM framework. It would involve work done by me alone and would have no other authors. Moreover, QTUM is an open source platform and all the references to resources will be cited.