School of Computing

Year 4 Project Proposal Form

SECTION A

Project Title :	Applications of Electoral Systems using Ethereum Blockchain
Student Name :	Patrick H Morris
Student ID :	14759021
Stream :	Computer Applications and Software Engineering
Project Supervisor Name :	Dr. Geoff Hamilton

SECTION B

General area covered by the project:

The purpose of this project is to enable election administrators generate custom-made electoral systems and easily hold these elections using the Ethereum blockchain providing immutability, security and transparency for all actors involved.

Outline of the proposed project

- *Background*
The idea for this project spawned out of my interest for blockchain technology. Blockchain is the technology that underpins cryptocurrencies like Bitcoin and Ethereum and functions to provide decentralized consensus of transactions between users of the currency. What I propose is an e-voting system that can allow voters to use this technology to securely and verifiably vote in elections.

- *Justification*
Current e-voting systems are not deemed secure enough. Implementations of centralised e-voting systems which involve processes of casting, transporting and tallying votes were found to

- leave opportunities for grand-scale fraud
- did not provide assurance to the voter that their vote was cast correctly
- proved no better than the traditional paper-ballot models

By using a decentralised implementation, the level of fraud is minimised. The total transparency of the election can be achieved in that the blockchain is publicly viewable like a global ledger while still keeping voter anonymity.
Other ways it is useful is that it can provide this level of security across different electoral systems. My intention is to allow electoral administrators as much flexibilty as possible in the initial set-up of the election.

- *Achievements*
The user's of the system is anyone who wishes to generate and/or take part in an election system that is entirely trustless. With the dynamic nature of it's intended design stage, the scope of user's will be any general voters. These voters may include:

- Board of Directors deciding on business decisions
- People voting in local/national elections
- Members of Government deciding on motions
- Members of non-profits deciding on investment projects
- Any members of organizations where voter anonymity is warranted

Programming Languages & Tools

Ethereum is the blockchain technology which the application will run on. The Ethereum blockchain network is analagous to a global virtual computer. This Ethereum Virtual Machine (EVM) executes software known as Smart Contracts which are written in a language called **Solidity**. This language allows us to interact with the blockchain programatically.
The Ethereum blockchain itself comes in multiple strains with versions written in Go, C++, Java, Javascript, Python, Ruby and Haskell to name a few. I will primarily use **Go** unless I feel more advantaged using a different version. These programs are called ‘clients’ and represent the node on network.
For the user interface application I will use web3js which can be used to generate in-browser applications to interact with smart contracts. **Web3js** is a javascript implementation of the web3 library which can be used to locally communicate from a frontend to a user’s Ethereum client.
Truffle is a framework that is used to set-up, build and deploy smart contracts to the blockchain and can also integrate with the test networks **Ropsten** and **Rinkeby**. It can also use a local blockchain with ten user accounts called **TestRPC**.
The **Mist** browser is an application called a wallet which stores Ether, it also functions as a client node like I mentioned earlier and can deploy Smart Contracts. It also comes with a Solidity IDE called **Remix**.
Lastly, **MetaMask** is a plugin feature for Chrome and Firefox browsers that allows browsers bridge onto decentralized networks without needing to use an Ethereum client.

Learning Challenges

The main learning challenge is going to be understanding the Ethereum blockchain. As of writing I would say I have a mediocre level of knowledge of how it works and I would hope that with this project that a deeper understanding of it is achieved. My opinion of blockchain is that it is going to be a major technology in the near future and an e-voting system is a well matched application for it.
I have touched on the all technologies mentioned in the above section but none to a level of familiarity.

Hardware/Software

At some stage during the development, there will be a necessity to emulate the election process which would mean I would need fake voters. Implementing tests of voter numbers could be a challenge and may require heavier computing equipment to model such instances.
Development of the software can be done on a single machine.