Blockchain: The Future of Voting

Project Proposal: Using blockchain technology in order ensure complete security, and auditability of the voting system

Jonathan Clark
University of Cape Town
CLRJON005@myuct.ac.za

Jason Smythe
University of Cape Town
jason@smythemail.za.net

CCS CONCEPTS

- **Computer methodologies → Blockchain**
- **Computer networks→ Decentralized network**
- **Mathematical methodologies → Cryptography→ Zero-knowledge proofs→ ZK-snarks**

KEYWORDS

Voting, Blockchain, Security, Cryptography, Ethereum, Smart Contracts, zero-knowledge proofs

1 PROJECT DESCRIPTION

Blockchain[1, 4, 10, 22] has received considerable attention in recent times from a multitude of entities due to its numerous possible applications. Key to Blockchain is its ability to provide perceivably superior security over traditional systems primarily attributed to its completely distributed nature. It is becoming increasingly apparent that Blockchains benefits extend far beyond its initial and most famous implementation “Bitcoin” (a cryptocurrency payment system) into the economic, political, humanitarian, social and scientific realms [1, 22].

One particular arena that stands to significantly benefit from Blockchain is the traditional voting system. Current voting systems heavily depend upon a trusted central authority to ensure the correctness of the voting tally and the eligibility of voters whilst also ensuring complete voter privacy [3, 21]. Voting has also historically been the subject of numerous other difficulties with many points of weakness that would be attackers could potentially exploit [5, 8, 9, 12]. Certain electronic voting systems have been introduced in an attempt to curb some of these traditional problems, and although succeeding in some areas, they have magnified problems in other areas [11]. As such no voting system has yet managed to provide a complete solution to the numerous problems faced by voting.

The aim of our project is to leverage the technology presented by Blockchain to create a more secure and completely auditable implementation of an electronic voting system. The most significant advantage behind the Blockchain based electronic voting system we plan to implement is that its distributed nature takes control away from the central authority in facilitating the voting process, thus removing the possibility of the central authority manipulating the outcome.

We will explore Blockchain technology in great detail in order to further our understanding regarding the security benefits it provides. We will examine the topics of census and cryptography which are cornerstones to the high level of security afforded through Blockchain. Notably we also examine key attacks on Blockchain networks in the past, Mt Gox and the 2015 Ethereum attack [23], in order to understand the security vulnerabilities that were exploited.

Lastly, the project will examine how identity systems can be created and registered on the Blockchain. This problem is significant, firstly because of the inherent ease that Blockchain systems give to users to create new identities (addresses) at will, and secondly to help users control and manage their identities (their private/public key pairs), which is not trivial from a security perspective [20, 22].

Through gaining a significant insight into both Blockchain and current voting systems, we aim to determine the feasibility of Blockchain based voting systems. This will be further augmented via the creation of a number of prototypes and comparing their advantages along a number of criteria. These include privacy of the voter, tamper resistance, possible cyber attacks, scalability, cost and ease of use.

Two core concepts are that of smart contracts and zero knowledge proofs. Smart contracts are small pieces of code that can be executed safely, securely, trust-lessly and predictably in the Blockchain [25]. Zero knowledge proofs are a mathematical and cryptographic method and set of algorithms that allow the correctness of certain information to be proven to be correct without giving away information as to what that information really is [26]. These two concepts will form the cornerstones for this project, and their conjunction will provide the security, safety and

2 PROBLEM STATEMENT

2.1 Aims and Research Question

The aim of our Blockchain voting project is to provide a secure trustless voting system that will circumvent the problem associated with traditional voting, trusting a central authority. This will allow small organisations and entities to facilitate fair elections at ease with little to no cost. This could be extended to full scale government elections in due course. Overall, through extensive research and an implementation of such a system we aim to determine the feasibility and likelihood of success of the above mentioned Blockchain based voting system.

- **Question 1.** What key theoretical aspects of Blockchain technology provide a significant security advantage over current voting systems? Jonathan will address this question.

- **Question 2.** What actual Blockchain architecture can we currently harness in order to implement a voting system that provides superior security? Jason will address this question.

2.2 Requirements

Our project takes the form of a research project as we attempt to determine the feasibility of Blockchain based electronic voting, through a theoretical analysis of the security Blockchain and the implementation of a small scale prototype. Aspects of the Blockchain voting system need to meet certain requirements in order to satisfy the stringency posed by the voting process, and furthermore the actual voters.

The requirements for the application should be as follows:

- *Voters maintain complete privacy.* Voters should be able to cast their vote in a manner such that no party except themselves can determine the exact entity which they voted for.
- *Votes are completely auditable.* The Blockchain should facilitate a complete auditable trail of every vote cast to promote the integrity of the election at question.
- *Voting is mobile.* Voters can cast their vote from any location provided they are eligible to vote in the election in question.
- *Voting is cheap.* The voting process should comprise of little to no cost
- *Voters can confirm their vote was included in the final count.*
- *No outside manipulation is possible.*
- *The voting record is permanent and immutable, so it can be examined any time in the future should disputes arise.*

We plan to implement the voting application on a small scale (less than 1000 voters) to determine the nature of the outcome and major feasibility issues before considering implementing our voting system in a national context.

Due to the significant ramifications associated with its outcome, extensive testing and prototyping will be required to ensure that our voting application meets the stringent requirements inherent to any voting process.

3 PROCEDURES AND METHODS

We will be using the public Ethereum Blockchain for all our development and the Solidity programming language for the smart contract implementation.

3.1 Blockchain security principles: Cryptography and Consensus

The implementation of our project will leverage the existing consensus mechanism of the Ethereum network [23]. The Ethereum Virtual Machine (EVM) will also handle the safe execution of all of the code in our Solidity smart contracts. However, there is no existing mechanism built into Ethereum for privacy. We will have to implement all aspects of the zero-knowledge proof/ZK-Snarks system [3] in code ourselves.

3.2 Development Procedures

The implementation of our project will leverage the existing consensus mechanism of the Ethereum network [23]. The Ethereum Virtual Machine (EVM) will also handle the safe execution of all of the code in our Solidity smart contracts. However, there is no existing mechanism built into Ethereum for privacy. We will have to implement all aspects

of the zero-knowledge proof/ZK-Snarks system in code ourselves.

3.3 Development Methods and Practices

The plan is to start development very early, and work continually and iteratively on it. Initial work has already determined that the truffle [27] framework will be used for all web3 integration, and smart contract compilation and deployment. Any front-end work will be done in react [28]for its ease of use.

The Blockchain network used in development will be a local testnet for speed and convenience. However, for any substantial testing the ethereum testnet will be used, this is a fully functional clone of the live net, just without the associated transaction fees.

3.4 Evaluating Measures and Acceptance Testing

Evaluation of the system will take the form of basic use case testing in the form of mock elections. Thereafter we will look at a series of edge cases that truly test the effectiveness of the voting system.

Thereafter a series of basic user trials will allow us to gather feedback about the use of our system and help us potentially discover and patch any issues we may have missed. The focus of these user trials will be less on user experience and more on practical or even conceptual issues with the system.

3.5 Case Studies of Historical Blockchain Security Attacks: Mt Gox, Ethereum Security Attack

The case studies will be done purely for research and give us a firm backdrop as to considerations for our own system. We will relate any security related decisions for our own system back to these concrete examples of security exploits and their solutions.

4 ETHICAL, PROFESSIONAL AND LEGAL ISSUES

The following ethical, professional and legal issues pertaining to testing, software and personal data is briefly described below:

Testing:

Within the Blockchain domain testing is not only standard practice as it is in software development, but ethically mandatory due to the immutable and irrevocable nature of the Blockchain. When users use a smart contract they are doing so in the knowledge that it operates as promised. Any variance can cause great loss to those involved, be it financial losses or otherwise. Liability in such cases may lie with the developer, who delivered something different to what was promised to be binding. Therefore it is essential that all smart contracts go through large amounts of testing and peer review before being considered for a live network.

Software:

Our final research, voting system and report will belong to the University Of Cape Town. The application will initially be open source in the beta phase, freely downloadable to all UCT related parties. Subject to the successfulness of the application, UCT, Jason Smythe and Jonathan Clark may look at the potential of outside distribution of the application.

The source code will be released under GNU GPL, and the source will be open to the public via a github repository.

Public adoption of application:

Users may feel skeptical towards this new technology deciding the outcome of an election that has possible extensive financial or political ramifications. It may be an issue convincing the larger community that the voting system development is indeed completely safe as mentioned.

Legal liability:

Despite any asserted confidence we may have for our system and the way we are freely distributing them, we will make it clear that we hold no legal liability for damages any third party may incur while using our application.

We also have no intention of using our product on any election of consequence, and will keep it our project within the bounds of simulated elections for testing purposes.

5 RELATED WORK

In lieu of the many problems faced in facilitating an election process, attempts at creating secure electronic voting systems have been made [14, 15, 17]. These solutions have perhaps improved voting efficiency and minimized the risk of voting corruption to some extent, yet the core problem remains of trusting a central authority to facilitate this process [6, 9, 18].

Direct-Recording Electronic (DRE) is one such system. This voting system functions much like a traditional electronic voting system as they require In-person voting at polling stations that require a central authority to regulate and supervise the process [8], the difference being that instead of users recording their vote on paper, they press a button on an electronic machine to cast their vote. This process has demonstrated significant security vulnerabilities; and subsequently led to the retraction of many of these voting systems in an array of nations.

Remote Electronic Voting (REV) refers to the process of voting where users can vote “without having to be physically present in a supervised environment” [8]. This requires that the voters use and trust a unsupervised system to record and transmit their vote to the relevant authority. Although REV systems have demonstrated some small degree of success, core security vulnerabilities underpinning the system, relating to the transmission of votes across an inherently risky domain (the internet), have been the downfall of this system.

The first type of Blockchain voting system to be devised uses a trusted third party (TTP) to count the votes, jumble up the identities of voters, coordinate with the organisation holding the election and publish an auditable roster after the election.[8] This is also the approach all Blockchain voting startups that we know of use: Blockchain Voting Machine, FollowMyVote and TIVI[3]. None of these systems have achieved any notable level of adoption.

The second type of Blockchain voting system was devised by McCorry et al at Newcastle University and utilises zero-knowledge proofs instead of a trusted third party. This makes the voting system entirely *on chain* and decentralized and autonomous[10]. The zero-knowledge proofs ensure voters interact with the system in a valid and correct manner, whilst still remaining anonymous[10].

The reader is referred to the following two literature reviews for further detail regarding the above mentioned voting systems.

6 ANTICIPATED OUTCOMES

6.1 System

We are expecting an operational system to work with a limited pool of voters. We are not focussing on issues of scalability, and have no expectations with regards to applicability for large scale elections.

6.2 Expected Project Impact

We expect the project to be useful in contained settings where a small number of participants all vote and want a irrevocable and immutable record of the results of the vote for future reference. The anonymity of the vote also adds to the appeal as a tool to resolve certain local and contentious issues.

We also believe that our system will greatly reduce the costs associated with elections since security and anonymity is built in. Additionally online remote voting removes the need for staff to monitor voting stations, nor is there a need to rent or find space to hold these voting stations.

6.3 Key Success Factors

Success will be measured when a voting system that is functional and Blockchain based is produced according to our specification. If objective comparisons can be made between the implementations then the project will be a success. Any other discoveries or breakthroughs will be a bonus.

7 PROJECT PLAN

7.1 Risks and Risk Management Strategies

The risks and risk management strategies for this project can be found in Appendix A1. Overall, the project is of moderate risk, due to the fact that we are using Blockchain technology in the Alpha stage of its development.

7.2 Timeline

The Blockchain voting project will run for the majority of the year from the 28th of March till the 23rd of October 2017. Exact details regarding the timeline can be found in our Gantt chart and Tasks and Milestones table in Appendix A2 and A3 respectively.

7.3 Required Resources

We required a number of academic papers and other online sources to formalise this concept. We will continue to require these resources to solidify our concept and aid us in our design.

All we require is a laptop for development. The public ethereum testnet (an environment used for Blockchain development) is hosted for us when we wish to work on a live network. For development purposes we will use a local test network, for speed and convenience. We may decide to test a private ethereum network which will require additional machines, however this is not necessary for our project.

7.4 Deliverables

The overarching deliverable for our project will be the Blockchain based voting application. The features contained in this system have previously been outlined and will serve to guide the development of this deliverable. We will also be delivering a comprehensive analysis of the security of Blockchain technology and the cryptographic and consensus steps needed in order to ensure complete safety.

Other deliverables for the project include:

- Literature review
- Project Proposal
- Presentation of Project Proposal
- Notes from Important Meeting and Brainstorming sessions
- Software Feasibility Demonstration
- Iterations of Software
- Project Website
- Project Poster
- Draft of Final Report
- Final Report
- Report Reflection

7.5 Milestones

The milestones for this project are listed our Gantt chart and Tasks and Milestones table (In Appendix A2 and A3 respectively). Here we outline the timing related to our honours project deliverables, as well as our design and development iterations.

7.6 WorkAllocation

The workload for this project will be divided into a more practical/implementation aspect, and a more theoretical part. Jason will deal with the implementation part, this includes the smart contract code, related user interfaces, and any networking considerations. Jonathan will focus more with the theory, the cryptography involved at a lower level and the overall security of the system at a higher level.

The implementation of this project will include minimal viable products of the two main types of voting system that seem feasible on the onset of this project from the literature. There will also likely be some variations or improvements that will be uncovered in the theory aspect of the project that will be detailed and found by Jonathan.

ACKNOWLEDGMENTS

This work was supported by our supervisor Tommie Meyer (Computer Science) and co-supervisor Christine Swart (Mathematics) of the University of Cape Town, South Africa.

REFERENCES

[1] Swan, M. 2016. Blockchain: Blueprint for a new economy. DOI: http://w2.blockchain-tec.net/blockchain/blockchain-by-melanie-swan.pdf

[2] Atzori, M. 2015. Blockchain Technology and Decentralized Governance: Is the State Still Necessary?

[3] McCorry, P., Shahandashti, S. and Hao, F. 2016. A Smart Contract for Boardroom Voting with Maximum Voter Privacy. School of Computing Science, Newcastle University UK.

[4] Mattila, J. 2016. 'The Blockchain Phenomenon', in Editor (Eds.): 'Book The Blockchain Phenomenon' (Berkeley Roundtable of the International Economy, edn.)

[5] IEFS, 2014. International Foundation for Electronic Voting Systems Pakistan Fact Sheet. DOI: https://www.ifes.org/sites/default/files/electronic_voting_machines.pdf

[6] USA, 2014. A Sampling Of Election Fraud Cases From Across The Country. The Heritage Foundation. DOI: https://thf_media.s3.amazonaws.com/2015/pdf/VoterFraudCases-8-7-15-Merged.pdf

[7] Jones, D. 2006. Technologists as Political Reformers: Lessons from the Early History of Voting Machines. Department of Computer Science, The University of Iowa. DOI: http://homepage.divms.uiowa.edu/~jones/voting/SHOTpaper.pdf

[8] Gibson, P., Krimmer, R., Teague, V. and Pomares, J. 2016. A review of E-voting: the past, present and future. Institut Mines-Telecom and Springer-Verlag France. DOI: http://www-public.tem-tsp.eu/~gibson/Research/Publications/E-Copies/GibsonKPT16b.pdf

[9] Karayumak, F., Olembo, M. Kauer, M. and Volkamer, M. 2017. Usability Analysis of Helios - An Open Source Verifiable Remote Electronic Voting System. Technische Universitat Darmstadt. DOI: http://static.usenix.org/events/evtwote11/tech/final_files/Karayumak7-8-11.pdf

[10] Kambo, G. and Mehta, R. 2016. Blockchain A revolutionary

technology too important to ignore. J.P. Morgan Cazenove.

[11] Hao, F., Ryan, P. and Halderman, A. 2016. Real-World Electronic Voting: Design, Analysis and Deployment. University of Michigan. DOI: https://jhalderm.com/pub/papers/ch7-evoting-attacks-2016.pdf

[12] Prasad, H., Halderman, A. and Gonggrijp, R. 2009. Security Analysis of India's Electronic Voting Machines. The University of Michigan.

[13] A. W. Appel, M. Ginsburg, H. Hursti, B. W. Kernighan, C. D. Richards, G. Tan, and P. Venetis. 2009.The New Jersey voting-machine lawsuit and the AVC Advantage DRE voting machine.

[14] D. Bowen et al. 2007. "Top-to-Bottom" Review of voting machines certified for use in California. Technical report, California Secretary of State. DOI: http://sos.ca.gov/elections/elections vsr.htm.

[15] R. K. Kumar. 2004. The business of 'black-marking' voters. The Hindu. DOI: http://www.hindu.com/ 2004/03/17/stories/2004031700571300.htm.

[16] Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten. 2007. Security analysis of the Diebold AccuVote-TS voting machine. In USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'07)

[17] Edward W. Felten. 2006. "Hotel minibar" keys open Diebold voting machines. Freedom to Tinker blog.DOI: https://freedom-to-tinker.com/blog/felten/hotel-minibar-keys-open-diebold-voting-machines/

[18] R. Mercuri. 2001. Electronic Vote Tabulation: Checks and Balances. PhD thesis, University of Pennsylvania.

[19] Wallach, D. 2011. The Risks of Electronic Voting. Rice University. DOI: https://www.cs.rice.edu/~dwallach/talks/e-voting-risks.pdf

[20] Narayanan, A., Bonneau, J. and Felten, E. 2016. Bitcoin and cryptocurrency technologies. Princeton University Press.

[21] Kremer, S., Ryan, M. and Smyth, B. 2009. Election Verifiability in Electronic Voting Protocols. School of Computer Science, University of Birmingham, UK.

[22] Franco, P. 2015. Understanding bitcoin. John Wiley & Sons.

[23] Buterin, V. 2014. Ehtereum Blockchain project founded in 2014. DOI: https://www.ethereum.org/

[24] Coin Market Cap. 2017. List of current Cryptocurrencies. DOI: https://coinmarketcap.com/currencies/ethereum/

[25] M. GREEN. 2014. Zero Knowledge Proofs: An illustrated primer. 2017, .
M. REPORT. 2016. Switzerland : IDENTITY protection app with blockchain technology released by WISeKey. Academic OneFile 2017, go.galegroup.com/ps/i.do?p=AONE&sw=w&u=unict&v=2.1&id=GALE%7CA462752291&it=r&asid=38fbc5a4ba6700523fdfca49eb577d52. .

[26] A. NARAYANAN, J. BONNEAU, E. W. FELTE, A. MILLER, S. GOLDFEDER, S. CLARK. 2016. Bitcoin and Cryptocurrency Technologies. Princeton University Press, New Jersey.

[27] The Ethereum Development framework. DOI: http://truffleframework.com/

[28] Development environment for multi platform applications. DOI: http://www.reactnative.com/

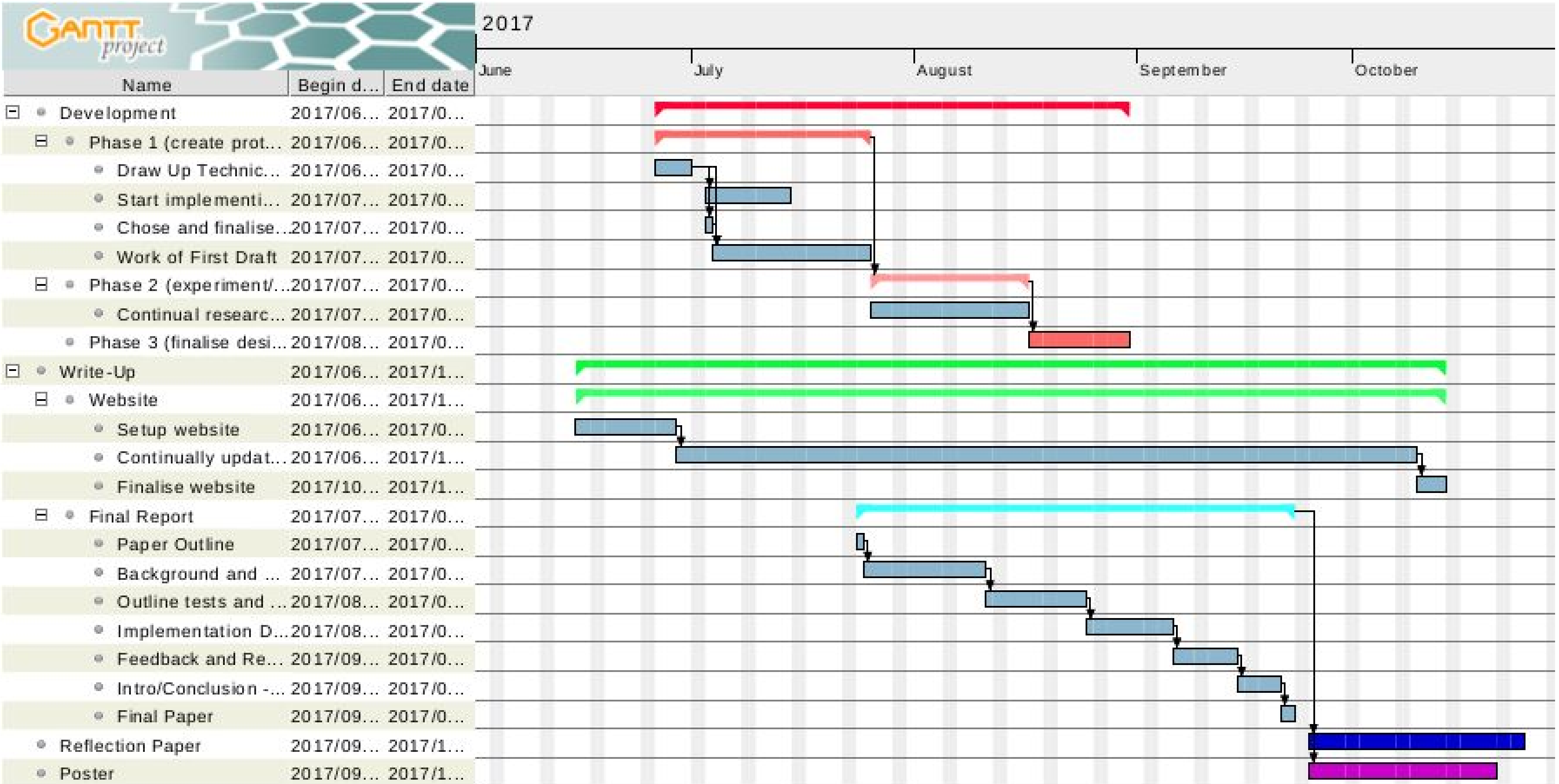
A Appendix

A.1 RIsk and Risk Management

Risk #	Risk	Probability	Impact	Mitigation/ Management
1. Unstable development environment	Technical Issues such as the test network being down or faulty.	Medium	Marginal	Use backup measures such as local development networks.
2. Missing member	Team member is unable to complete their aspect of the project due to injury, sickness or personal issues.	Low	Medium	The project is designed to be completable by a single member if need be, and the two components are self contained.
3. Scope creep (Golden Plating)	As we discover new and interesting topics relating to Blockchain we may be tempted to deviate from our original scope of project.	Medium	Marginal	Follow our Milestones to and check our research question regularly to ensure we are following our original scope.
4. Overestimate of our skills and time resource such that the	Certain deliverables in the project will not be	Medium	Critical	We must research what will be involved in all aspects of the development of the game and

planned scope of the project is unachievable.	achievable. We will have to settle with certain downgrades to the project. This may impact our code and cause us to adapt it.			factor this, with leeway into our scope calculations. We must continue doing this through development when appropriate according to our Gantt Diagram.

A.2 Gantt Chart



A.3 Tasks and Milestones

Tasks

Name	Begin date	End date
Development	2017/06/26	2017/08/30
Phase 1 (create prototype)	2017/06/26	2017/07/25
Draw Up Technical Plan	2017/06/26	2017/06/30
Start implementing Initial ideas	2017/07/03	2017/07/14
Chose and finalise technology stack	2017/07/03	2017/07/03
Work of First Draft	2017/07/04	2017/07/25
Phase 2 (experiment/compare)	2017/07/26	2017/08/16
Continual research and theoretical theoretical exploration	2017/07/26	2017/08/16
Phase 3 (finalise design)	2017/08/17	2017/08/30
Write-Up	2017/06/15	2017/10/13
Website	2017/06/15	2017/10/13
Setup website	2017/06/15	2017/06/28
Continually update website	2017/06/29	2017/10/09
Finalise website	2017/10/10	2017/10/13
Final Report	2017/07/24	2017/09/22
Paper Outline	2017/07/24	2017/07/24
Background and most of theory	2017/07/25	2017/08/10
Outline tests and comparisons	2017/08/11	2017/08/24
Implementation Discussion/Findings	2017/08/25	2017/09/05
Feedback and Revised Draft	2017/09/06	2017/09/14
Intro/Conclusion - Final pollish	2017/09/15	2017/09/20
Final Paper	2017/09/21	2017/09/24
Reflection Paper	2017/09/25	2017/10/24
Poster	2017/09/25	2017/10/20