Coventry University
FACULTY OF ENGINEERING AND COMPUTING

Coursework Cover Sheet

Please ensure that you complete all relevant sections legibly
First Copy: *Attach top copy to the front of your assignment.*
Second Copy: *Keep safety as your receipt*

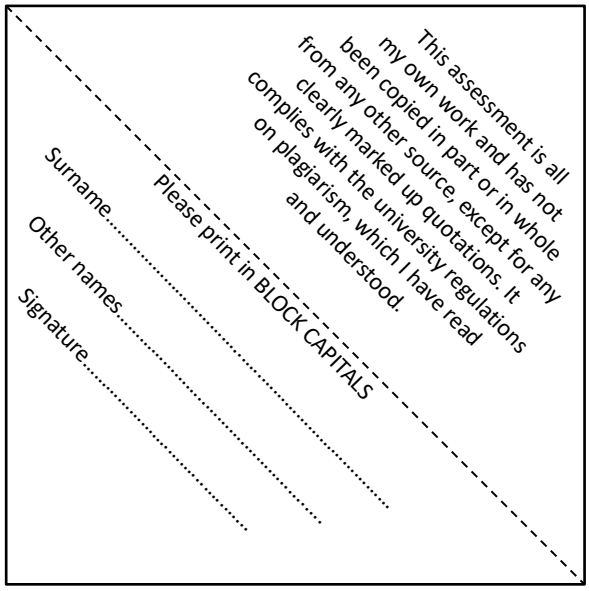
Module Code	**Student Card ID Number**
VTC303COM	**197101307**

Module Title

Individual Project

Deadline date	**Actual word Count**	**Tutor**

Coursework Title/Number



FEEDBACK ON MARKED WORK: *Lecturers will complete this section when work is marked.*
NB. All marks notified during the year are provisional until confirmed by the end of year Assessment Board

STRENGTHS

WEAKNESSES

ADVICE ON HOW WORK COULD BE IMPROVED AND FURTHER COMMENTS

If you require more feedback, please contact your tutor or see module web.
See assignment sheet for assessment criteria for this assignment.

MARKED AWARDED	
Less any late penalty	-
Adjusted mark if penalty	

Marker's Signature …… **Date** …….

Students are reminded that reference must be given for any previously published work used to gather information to help write assignments, including internet sources, but these sources should not be copied directly.

Second Marker Additional comments Signature …… **Date** ……

ABSTRACT

With the progress of this society, the rapid economic development, polling and opinion collection are becoming more and more important in social life. The digital voting system is environmentally friendly and efficient. However, there are still some problems that cannot be ignored in digital systems. For example, the administrator of the system may maliciously modify the data in order to use it, and the user's voting information is easy to be leaked. Blockchain is a distributed database technology behind Bitcoin. It seems to be very suitable for digital voting systems. Blockchain has decentralization, which provides a method to keep transactions private and a mechanism to prevent data tampering. Therefore, blockchain technology is the best way to ensure fairness.

This article first studies the advantages of blockchain technology and the feasibility of its application in voting systems. Then understand the operating process of the blockchain. In analyzing system requirements and data management storage, the system is divided into an application layer and a blockchain layer.

This article aims to design a novel electronic voting system based on blockchain, which can solve all the limitations we found. Make full use of the decentralization of the blockchain, the data cannot be tampered with, the characteristics of security and trustworthiness, and reduce the cost of holding elections. Moreover, the system also has a variety of functions, including user registration, user login, identity information modification, account cancellation, frozen information query, registered user query, transfer and bill query. Finally, we will complete the functional test of each module of the system to ensure the availability and stability of the voting system.

KEYWORDS

Blockchain, Electronic Voting System; e-Voting; I-Voting; Electronic Ballot; Decentration;

1 INTRODUCTION

Elections are a fundamental pillar of democracy, enabling the public to express their opinions in the form of votes. Because of the importance of the election process to society, elections must be trustworthy, and people's privacy and the security of voting must be ensured.

At present, the traditional voting method is to use paper voting, which has become the most commonly used method for holding national elections worldwide. Voters usually need to go to a polling center, show the government identity card to be verified, and then continue to vote on a completely anonymous paper ballot. The process is complicated. In addition, the staff responsible for counting the votes will spend a long time on counting because waiting for the results for a long time will increase voters' concerns about the manipulation of the results. All these reasons have caused a lot of controversial issues. In particular, paper ballots are managed by a central authority, and there is a risk of manipulation of ballot papers and ballot paper results.

There are also technology companies trying to automate the entire voting system by using electronic voting in order to eliminate the problem of traditional voting systems. Although electronic voting simplifies the voting process and reduces the labor burden, privacy and security concerns continue. In order to completely eliminate the problems of traditional voting systems and electronic voting systems, blockchain technology can be used to improve electronic voting systems.

Blockchain is a system that cannot be changed and is easy to confirm. It has great potential to replace traditional voting systems. The purpose of the work described in this report is to provide a decentralized voting system using blockchain. Ballots and voter security and privacy are discussed in the proposed solution.

1.1 Problem Background

In recent years, many literatures have attempted to develop new electronic voting systems to address the shortcomings of paper ballots. Although online voting systems have been an active area of research in recent years, the results make people think that the work of electronic voting systems is still flawed, and the main motivation for designing a new system seems to be just to solve the problem of inefficient systems, such as the required manpower or large work. It is not a solution to its security problems.

1.2 Problem Statement

Online Voting reduces manual efforts and a large amount of information can be easily processed. Except for all these features there are some drawbacks with this system are, such as software failure issue, insecure access of internet and voters’ familiarity with the internet.

1.3 Scope

The main scope of the project is to verify the casting of the voter has registered correctly. We deploy Blockchain for this concept. The main advantage of the project is to provide an opportunity to cast their vote from home itself.

1.4 Research Objective

The electronic voting system is a system combining software and hardware based on the principles of cryptography and using computers, the Internet, and communications to replace traditional manual methods to implement voting functions. The system's operation process is completed through the Internet to meet the greatest demand with the least cost. The research objectives of this topic meet the following needs:
Fairness: The verification unit shall accept the votes of any legitimate voter, and all valid votes shall be correctly counted.

- Uniqueness: Legal voters can vote only once.
- Anonymity: All ballots are confidential, and no one can match a ballot with a voter to determine what a voter voted for.
- Verifiability: Any voter can check whether their votes have been counted correctly, and the voting results can be verified for fairness.
- Convenience: The system should be simple, convenient, and easy to use. For voters, the knowledge and operation required for voting cannot be too much.
- Flexibility: There should be no restrictions on the number of people voting and the venue. The voting activities of each voter are independent and unaffected, and they do not need to participate in voting at the same time.

2 LITERATURE REVIEW

2.1 Overview Current Electronic Voting Systems

As early as 1880, the great inventor Tomas Edison invented an electronic voting recorder. The function of the system was to vote by the US legislature. However, under the social and market environment at the time, this electronic voting recorder had not been practically used, and ultimately failed.

The first electronic voting scheme in the modern sense was proposed by Chaum in 1981. It uses a public cryptosystem, uses digital signatures to hide the identity of voters, and completes the entire voting process

through computers and the Internet. In 1985, Cohen and Fisher proposed an electronic voting scheme based on homomorphic encryption technology. Then Benaloh, Yung, Iverson, Sako, and Kilian also proposed electronic voting schemes based on homomorphic encryption technology.

In the course of the continuous development of electronic voting schemes over the years, some schemes are too complicated to be suitable for large-scale voting, while others have major loopholes in security. The first practical solution suitable for large-scale voting is the Foo solution proposed by Fujilka, Okamoto, and Ohta in 1992. The core of the solution uses bit commitment technology and blind signature technology. After the proposal was put forward, it received much attention from the society and was considered to be an electronic voting solution that can better realize secure voting. So far, the adoption of the electronic voting system has achieved substantial breakthroughs and has been widely used in various non-governmental departments. Subsequently, the research institutions of many universities and companies have improved the scheme and developed corresponding electronic voting software systems. Among them are the EVOX system of the Massachusetts Institute of Technology and the Sensu system of the University of Washington. In 1999, Wei-ChiKu and Wang-ShengDe of Taiwan University proposed an RSA-based electronic voting scheme, which is also an improvement on the FOO scheme.

In the research and development process of electronic voting, many researchers have proposed a variety of different solutions to the problems in the FOO protocol. Other researchers have devised other ways to design electronic voting systems suitable for different occasions and purposes.

In the 2000 presidential election in the United States, Florida and a few other places piloted elections for some voters through the Internet. Although the hot one was just an experiment, it was of great significance to the development of electronic voting systems.

In 2002, voters in two French towns became the first citizens in the country's history to use the electronic voting system. In the presidential and parliamentary elections of France, the E-POLL system was used for electronic voting. The system was developed by an association, including the R & D center of France Telecom.

In 2004, during the US President ’s High School, the electronic voting system was first used, which shows that the era of true paperless electronic voting elections has come. The general part and Texas's Diebohd company became another focus of the US presidential election in addition to the presidential candidate. The company's electronic voting system was placed at 75,000 polling points throughout the United States, and Diehold became the country's largest provider of election tools.

The electronic voting system is continuously researched and developed. Although there are still problems to be solved in security, the era of paperless voting has come to an end. The electronic voting system is constantly developing with its convenient, efficient and strict characteristics. Better service with our society.

The first electronic voting system was proposed by David Chaum in the early 1980s. The system uses public key encryption to vote and keep voters anonymous. In order to ensure that voters cast ballots electronically at a

polling station and cryptographically verify that the DRE did not modify their vote. Since the system was first introduced, many scholars have shown interest in the subject, and a lot of research has been done. Most of the research in this area has focused on the Direct Recording Electronic System and the online Voting Systems. The first system is used in polling stations instead of the paper ballot voting system, but the second system is meant to be mobile and allows voters to cast their votes from anywhere using any device with Internet connection. Obviously, an electronic voting system can make casting a vote easier and more convenient and can definitely increase the number of voters. However, technical threats of electronic voting systems have always been a concern.[2]

* Estonia I-Voting System: Estonia became the first country in the world to use the Internet and electronic ID cards for national elections. The ID card used for the election is designed to run on an integrated circuit, chip Java chip platform, and protected with 2048 bits [3]. The card can create signatures using SHA1 / SHA2 [3]. The card is easy to use for authentication, encryption and signing. Voters must download the voting application and use an electronic ID for authentication. If the voter is eligible to vote, the list of candidates will be displayed and voted. The vote will be encrypted using the elected public key and signed with the voter's private key. Once the vote is over, it is sent to the voting storage server controlled by the Estonian government [4]. Voters can vote multiple times, only the last vote is valid. This is done to prevent the purchase of votes.

* Norwegian I-Voting System: In 2011, Norway used an electronic remote voting system in the country council elections. However, due to security considerations for the country has discontinued its I-Voting project in 2014 [14]. Since, one of the main criticisms it faces was the fear of votes going public in the event of a cyber-attack.

2.1.1 Feasibility Analysis

For the feasibility analysis, one of the main problems with both Estonian and Norwegian electronic voting systems is the secrecy of critical parts of the code. The Estonian I-Voting System raise questions about transparency because the script to post the vote had been shut down. The centralization of these systems makes them vulnerable to distributed denial-of-service attack which prevent voters form voting. For credible elections to take place, there must be an open source electronic voting system.

The system we are going to propose in this paper will address all these security concerns by using few JavaScript frameworks and Libraries for the front end of the website and PHP and MYSQL for the backend to develop the electronic voting system, and rely on Blockchain technology to secure votes, and decentralize the system.

A. Security and Reliability

The security services that the blockchain provides is compared with other database solutions in Table 1. The availability and the fault tolerance of the system is high as all the nodes keep a copy of the records and check

each other to make a stable system. The blockchain provides transparency with anonymity. The privacy is not aimed but can be implemented.

Table 1 COMPARISON OF THE SECURITY SERVICES OF DIFFERENT SOLUTIONS [2]

	BlockChain	Database	Distributed Database
Integrity of the Records	High	Moderate	Moderate
Availability	High	Low	Moderate
Fault Tolerance	High	Low	Low
Privacy	Low	High	Moderate

B. Comparison Analysis

Here we summarize some of our findings in Table 2. In the analysis showed that, the potential benefits of antique blockchain-based online elections are huge and worth developing. However, there are also significant problems with implementation details, use cases, and extreme conditions.

Table 2 COMPARISON BLOCKCHAIN BASED E-VOTING. E-VOTING AND TRADITIONAL VOTING

	E-Voting Systems	Blockchain-based e-Voting	traditional paper voting
Advantages	➢ There are already several demonstration models. ➢ Might bring more democracy to government units, local administrations.	➢ Immutable records. Deleting records is almost impossible. ➢ Provide transparent privacy. ➢ Provide immediate results ➢ Secure storage and records. ➢ Might bring more democracy to government units, local administrations.	➢ People trust paper-based voting and counting as long as the process is transparent. ➢ Does not rely on the Internet and computers and is suitable for areas with low Internet existence/usage. ➢ Less prone to conspiracy theories.
Disadvantages	➢ The strengths will depend on the implementation. ➢ Technology is new and there are scalability issues.	➢ The strengths will depend on the implementation. ➢ Technology is new and there are scalability issues. ➢ Internal processes and casted votes are less transparent.	➢ Costs are very high in the long term. ➢ Physical security is through and expensive. ➢ Not possible to set vote centers in small and far-away settlements.

2.2 Blockchain

2.3 What is Blockchain and how is it Commonly used:

To understand what is blockchain, it can be explained by simply divide the word into blocks and chains. The literal meaning of blockchain is a few blocks that are linked together by chains. In fact, blockchain is a time-stamped series of immutable records of data called blocks that is managed by a group of computers owned by different entities. These records of data are secured and stored in each of these computers by cryptographic principles (i.e. chains). To sum up, blockchain is a distributed database of records or public ledger of transactions that have been made and recorded among participating parties. Genesis Block is the name of the first block in the blockchain. After the construction of genesis block, more and more data are recorded, and more blocks are formed. Blockchain is formed after the sequential addition of blocks on top of the genesis block. The block is also named by the order of construction of the blocks with the genesis as the zero block.

Blockchain is first introduced by Stuart Haber and W. Scott Stornetta in 1991. In 1991, W. Scott Stornetta and Stuart Haber wrote a paper titled “How to Time-Stamp a Digital Document”. (Klein, 2019) They worked on how the date and time can be recorded at the time of the creation of the document. They tried to solve the problem by central authority, using a ‘digital safety-deposit box’ to do the records and storage. However, this solution cannot prevent the collusion of the time-stamping service provider and the client. After 3 years, Stuart and Stuart found the solution of it —the blockchain. Blockchain solved the problem by providing immutable public record. However, blockchain had not become known to the world until 2009, which a man or a group of unknown people using the name of Satoshi Nakamoto released the bitcoin whitepaper. Bitcoin is a cryptocurrency of which transactions are made and recorded in the blockchain. Satoshi Nakamoto conceptualized the first blockchain in 2008, where advanced technology made blockchain to apply in many applications beyond cryptocurrencies.

2.4 How does Blockchain work?

Table 3 STRUCTURE OF THE BLOCKCHAIN

Field	Description	Size
Block Size	The size of the whole block	4 bytes
Block Header	Encrypted almost unique Hash	80 bytes
Transaction Counter	The number of transactions that follow	1 to 9 bytes
Transaction	Contains the transaction saved in the blocked	Depends on the transaction size.

Blockchain institutions have two very important characteristics:

I. The block header of each block references the hash value of the previous block, which is used to connect the block with the previous block in the blockchain. Such connected blocks constitute a chain (Figure 2).

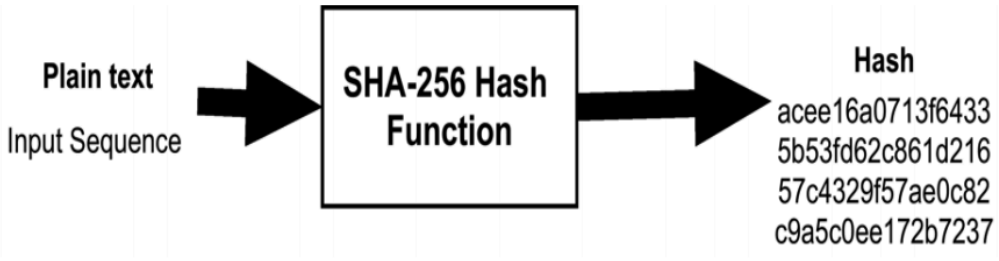


Figure 1. *Basic Function of the SHA-256 Hash*

Figure 2 *A blockchain design*

II. The transaction record on each block body is all the value exchange activities that occurred after the previous block was created. In most cases, a new block is successfully added to the chain, and the data record of the block cannot be changed or changed. This structure also ensures that the transaction information cannot be forged and tampered with.

A. Do not forge. The blockchain record principle requires all participating and recording nodes to jointly verify the correctness of the transaction record. Because all nodes are recording every transaction on the entire network, once the information recorded by a node is inconsistent with other nodes, other nodes will not recognize the record and the record will not be written into the block.

B. Don't make up. When the sender broadcasts the transaction information, what the participating nodes in the blockchain need to do is to verify the sender's ability to perform the transaction through the historical record, instead of verifying whether the broadcasted transaction is true. Through the verification function of historical data, the blockchain establishes the foundation of trust and also guarantees the non-fiction of information.

C. Cannot be tampered with. It is almost impossible to change a certain block and the transaction information in the block. If the block is changed, every subsequent block will be changed. Therefore, people who

attempt to tamper with the data must simultaneously invade at least 51% of the global participating records to tamper with the data. Technically, this is almost impossible.

2.5 Digital encryption

Digital secrets, Bitcoin addresses, and digital signatures determine Bitcoin ownership. Among them, the digital key is generated by the user and stored in a file or database, called a "wallet".

Bitcoin is not included in the wallet; only secret keys are included. A user's digital secret is completely independent of the Bitcoin protocol, generated by the user's wallet and managed with confidence, without the need for a blockchain or network connection.

Each transaction requires a valid signature to be stored in the block. A valid signature is generated by a valid digital key, so having a key is equivalent to having control of Bitcoin in the account.

Secrets appear in pairs, consisting of a private key and a public key. Among them, public key is public, which is equivalent to the bank account number in the traditional currency transaction scenario and is used to accept bitcoin: private key is only visible and used by the owner and is used for transaction signatures during payment to prove ownership.

The private key is a randomly selected number, a public key is generated by an irreversible encryption function, and then the public key is used to generate a Bitcoin address through a hash function. A Bitcoin address is a string of letters and numbers that can be shared with anyone.

2.6 Distributed structure

The distributed structure of the blockchain makes data not recorded and stored on a centralized computer or server, but allows each node participating in the data transaction to record and store all data information. To this end, the blockchain system uses an open source, decentralized protocol to ensure the complete recording and storage of data.

- Propagation. Each transaction information in the blockchain is sent by a single node to all nodes in the entire network. Therefore, the information interceptor cannot intercept the information successfully by intercepting a certain information propagation path, because each node has received the information. In addition, the mathematical principle of asymmetric encryption is used, and only the owner of the transaction information can open the information reading content, ensuring the security of the information.

- Record. The blockchain has established a complete set of protocol mechanisms to allow each node in the entire network to participate in verifying the correctness of the results recorded by other nodes while

participating in recording data. Only when most nodes on the entire network confirm the correctness of the record, the data will be written into the block.

- Storage. In a blockchain-based distributed network system, the participating network nodes update and store all data in the entire network system from time to time. Therefore, even if some nodes are attacked or destroyed, it will not affect the data update and storage of this data system.

3 DATA COLLECTION METHODS

There are methods that were used to elicit requirement from the stakeholders of the system.
These stakeholders included:

- Student i.e. voters
- The candidates
- Electoral Affairs Commission

The following is a brief description of the tools used to gather data from various stakeholders in order to constitute requirements:

3.1 Questionnaire

A questionnaire is a method of collecting data from the target users in a specific knowledge domain. According to Peerce et al. Questionnaires are a well-known technique of collecting demographic data and users' opinions. The design of a questionnaire is important because it solves the research questions and hypothesis on which data is to be collected. The questions can be closed or open ended. Demographical and experiential information are mainly involved in the questionnaire. This information could be used to understand the users' experience with the current system. Some of the major areas covered by the questionnaires were:

- Views on online voting.
- The proposed system.
- Characteristics of a good output with regard to the system.

The questionnaires were administered to the students as well as the electoral commission. Fifty (50) respondents were surveyed. **Questionnaire questions are shown in Appendix A**.

3.2 Interviews

Interviews are used to gain more understanding into the user requirements. They involve having face to face conversations with various stakeholders in order to get more information.
They were mostly open-ended and semi-structured to allow the users provide as much information as possible without feeling stressed. One of the benefits of using interviews that a participant's unique point of view can be explored in detail. Interview questions are shown in Appendix B.
In order to do a deeper dive into this topic, I turned to Ivan Law, Co-Founder at PASSBER Limited, to answer my questions on blockchain, online voting. On LinkedIn, Mr.Law describes himself as a “A self-driven Technology Enthusiast , over 18 years of working experience in the US and Hong Kong, passionate about delivering the best digital solutions for enterprises.”
Mr. Law said that Blockchain is a permanent cryptographic record, or ledger, of digital events that’s “distributed,” or shared among many different parties. This technology provides all of the characteristics you would want in a platform that is arguably the most important part of a democratic society. The biggest issues with the current processes that blockchain technology is trying to solve is Transparency, accessibility, security, and auditability.

3.3 Observation

This involved observing the various stakeholders and their roles in the voting process. It was important in getting to know the problems that the clients mostly go through in the process of voting. The main focus was on the students because the intended software solution is aimed at making the process of voting more efficient and convenient for them. In order to anticipate software solutions that are more efficient and convenient in the voting process, the main focus was on the students or young adults.

4 EVALUATION / RESULTS

After collecting data from the questionnaires filled by 50 interviewees, where most of them are aged above 18, and are full-time workers or students, there are some results about blockchain based voting system. 42 of the interviewees are registered voters, while all of them voted at their local polling station. 37 of the voters feel struggling to find the time to vote on polling day. 36 of them responded that they would choose to use electric voting instead of normal voting system if it is possible, with reasons of convenience, fast and time saving. A lot of the interviewees thought that electronic voting would significantly increase election turnout. However, not a few of them also worried about the security of it. At last, 45 of them think that verifiability is important from an information security perspective

5 DISCUSSION

From the questionnaire result, we found out that a lot of people are very annoyed by the inconvenience caused by the normal voting system. People think that it is difficult to find the polling station, it is time consuming and they would rather use the electronic voting system than the normal voting system. However, an important issue needed to be solved is the security and verifiability as most people concerned. The main purpose of a voting system is to store the data of an election, and the data are confidential. This is the reason which affects the widespread of electronic voting system. Blockchain based electronic voting system can completely solve this problem, leaving advantages only.

6 CONCLUSION

The existing online voting system solves the problems of manpower and material waste in traditional voting system activities, limited time and space for voting activities, and inability to view the voting situation in real time. However, the existing online voting system also has many shortcomings. For example, firstly, there is a risk of leakage of user's voting information, and secondly, after voters' vote, other voters cannot verify whether the votes are recorded correctly. Finally, voting data and results can be maliciously tampered with. In order to overcome the above deficiencies, in this paper designed and implemented a fair, open and secure electronic voting system based on blockchain technology.

This paper studies the hash functions involved in the blockchain, not cryptographic knowledge such as encryption, digital signatures, and timestamps, and introduces the networking of the p2p network and its characteristics of channel centralization and scalability. Then introduce concepts such as distributed storage and in-depth understanding of the new process of blockchain, definition and decentralization, security and credibility.

Based on the analysis of system requirements and data storage characteristics, the system is divided into an

application layer and a blockchain layer. Realize the networking mode of p2p network in blockchain network, node block synchronization, data and area verification mechanism and consensus mechanism to ensure data consistency, use time stamp, asymmetric encryption and other technologies to design data blocks and use The chain structure stores data blocks.

Combined with the characteristics of the underlying blockchain to store data, a blockchain-based voting system is implemented. The web application layer is divided into a view and a data access layer. The data access layer can access local data and the blockchain. The web application layer closely combines the characteristics of the blockchain to build a fair, just and transparent voting system

7 REFERENCE

[1] Chaum, D. (2004) Secret-ballot receipts: True voter-verifiable elections, IEEE Security Privacy, vol. 2, no. 1, pp. 38{47, Jan 2004.

[2] Sos.ca.gov. (2007). Top-to-Bottom Review | California Secretary of State. Available at: http://www.sos.ca.gov/elections/voting-systems/oversight/ top-bottom-review/.

[3] Kraft, D. (2015) Difficulty Control for Blockchain-Based Consensus System, Peer-to-Peer Networking and Applications by Springer, March 2015.

[4] N. Bozic, G. Pujolle, S. Secci, "A Tutorial on Blockchain and Applications to Secure Network Control-Planes". IEEE 3rd Smart Cloud Networks & Systems (SCNS), 2016

[5] Tabora, V. (2018) Databases and Blockchains, The Difference Is In Their Purpose And Design [online]available from https://hackernoon.com/databases-and-blockchains-the-difference-is-in-their-purpose-and-design-56ba6335778b

[6] Nicholas Weaver. (2016). Secure the Vote Today. Available at:https:// www.lawfareblog.com/ secure- vote- today.

[7] T. ElGamal, "A public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Trans. Info. Theory. Vol. 31. (1985), pp. 469-472.

[8] Trueb Baltic, "Estonian Electronic ID – Card Application Specification Prerequisites to the Smart Card Differentiation to previous Version of EstEID Card Application." http://www.id.ee/public/TB- SPEC-EstEID-Chip-App-v3_5-20140327.pdf

[9] Cybernetica. "Internet Voting Solution." https://cyber.ee/uploads/2013/03/cyber_ivoting_NEW2_A4 _web.pdf.

[10] Andrey Sergeenkov, sergeenkov. 2019. Why do Voting Systems Need Blockchain? [Online]. Available from: https://hackernoon.com/why-do-voting-systems-need-blockchain-e85e747e906d

[11] Kelly, S. (2019). Voting using blockchain and smart contracts. [online] medium.com. Available at: http://www.hawking.org.uk

APPENDIX A

1. What is your age?
   - ✧ Under 18
   - ✧ 18-21
   - ✧ 22-25
   - ✧ 26-35
   - ✧ 36-50
   - ✧ 51-64

2. What is your current employment status?
   - ✧ Full-time
   - ✧ Unemployed and seeking work
   - ✧ Student
   - ✧ Part-time
   - ✧ Retired
   - ✧ Unemployed and not seeking work
   - ✧ On leave (maternity, paternity, sabbatical)

3. Are you a registered voter?
   - ✧ Yes
   - ✧ No
   - ✧ Unsure/ Don't Know

4. How have you cast your ballot in the past?
   - ✧ At my local polling station
   - ✧ By post
   - ✧ By proxy (have someone else vote on your behalf)
   - ✧ I don't vote
   - ✧ I have never voted

5. Do you struggle to find the time to vote on polling day? Choose all that are applicable.
   - ✧ Yes, because of my job commitments
   - ✧ Yes, my polling station is far away
   - ✧ Yes, because of family commitments
   - ✧ Yes, I am registered in a constituency where I do not always live
   - ✧ No, I always make sure I find the time
   - ✧ No, I usually forget to go out and vote
   - ✧ No, I vote by post/proxy incase I cannot make it

- ✧ No, I choose not to vote

6. If electronic voting is an option, would you choose to use it?
   - ✧ Yes
   - ✧ No
   - ✧ Don’t Know
   - ✧ I abstain/ do not vote

7. If yes, why would you use electronic voting? If not, why not?

8. Do you think that electronic voting would significantly increase election turnout?
   - ✧ Yes, I think they are a good idea for efficiency
   - ✧ Yes, I think they are a good idea for saving time and money
   - ✧ Yes (other, enter in comment box)
   - ✧ No, I don't trust the machines to count the votes properly
   - ✧ No, I am worried about the secrecy of the ballot
   - ✧ No, I think they are a waste of taxpayer money
   - ✧ No

9. Do you think verifiability is important, from an INFORMATION SECURITY perspective?
   - ✧ Yes
   - ✧ No
   - ✧ Maybe

APPENDIX B

- ✧ *What is blockchain technology and why is it more secure?*
- ✧ *How can voting benefit from blockchain technology?*
- ✧ *What are the biggest issues with the current processes that blockchain technology is trying to solve?*
- ✧ *What is the state of electronic or online voting in the Hong Kong. and beyond?*
- ✧ *Online voting has been happening around the world for a while; what alternate technologies have been used and how does blockchain compare to this?*
- ✧ *What can be done to make new election technology more secure?*