BLOCKCHAIN WEB-BASED E-VOTING SYSTEM FOR UMS STUDENT COUNCIL

STANLEY PAUL DAVID

FACULTY OF COMPUTING AND INFORMATICS
UNIVERSITI MALAYSIA SABAH

2022

UMS
UNIVERSITI MALAYSIA SABAH

BLOCKCHAIN WEB-BASED E-VOTING SYSTEM FOR UMS STUDENT COUNCIL

STANLEY PAUL DAVID

THESIS SUBMITTED AS PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE DEGREE OF BACHELOR OF NETWORK ENGINEERING

FACULTY OF COMPUTING AND INFORMATICS
UNIVERSITI MALAYSIA SABAH

2022

UMS
UNIVERSITI MALAYSIA SABAH

PENGAKUAN

Karya ini adalah hasil kerja saya sendiri kecuali nukilan, ringkasan dan rujukan yang setiap satunya telah saya jelaskan sumbernya.

23 APRIL 2021

STANLEY PAUL DAVID

BI18160301

PENGESAHAN

NAMA : **STANLEY PAUL DAVID**

NO MATRIK : **BI18160301**

TAJUK : **SISTEM E-UNDI BERASASKAN *BLOCKCHAIN* UNTUK MAJLIS PERWAKILAN PELAJAR UMS**

IJAZAH : **IJAZAH SARJANA MUDA SAINS KOMPUTER DENGAN KEPUJIAN (KEJURUTERAAN RANGKAIAN)**

DISAHKAN OLEH;

1. PENYELIA UTAMA

Dr. Chin Pei Yee

Tandatangan

Pei Yee

PENGHARGAAN

Terlebih dahulu, saya ingin merakamkan setinggi-tinggi penghargaan dan mengucapkan terima kasih kepada penyelia projek akhir tahun saya, Dr Chin Pei Yee yang banyak memberi bimbingan dan nasihat sepanjang penulisan tesis ini. Segala bimbingan dan tunjuk ajar beliau membolehkan saya memahami tentang penulisan laporan penyelidikan dengan lebih mendalam. Saya juga ingin mengucapkan terima kasih kepada semua pensyarah dan kakitangan Fakulti Komputeran dan Informatik yang membantu saya sepanjang kajian ini. Ucapan terima kasih juga kepada ahli panel yang terlibat dalam kajian ini atas sumbangan yang diberikan.

Saya ingin mengambil kesempatan untuk mengucapkan ribuan terima kasih kepada ahli keluarga saya yang tidak pernah putus doa dan semangat serta motivasi yang diberikan sepanjang pengajian saya. Kepada rakan-rakan seperjuangan, terima kasih atas bantuan, idea dan semangat yang diberikan semasa menjalankan dan menyiapkan tesis ini. Akhir sekali, saya ucapkan terima kasih kepada semua pihak yang terlibat sama ada secara langsung dan tidak langsung dalam menjayakan tesis ini.

Sekian, terima kasih.

Stanley Paul David
23 April 2021

ABSTRACT

In the current status quo there are many innovations that are being brought forward to existing systems. These innovations help to provide a better functioning application. One particularly emerging field in innovation are blockchains. Blockchain technology offers an array of benefits from the field of economics to data storage. A blockchain is a data storage method that connects blocks with a chain. The blocks data cannot be modified once it has been stored as a block. The blockchain application in e-voting provides a open, fair and immutable. By storing the votes onto the blockchain the data is then safe and unmodifiable. Current systems use a database to store the votes. This paper proposes a system for e-voting that incorporates a blockchain as the main method for storing votes. This system is designed to fulfill the requirements of a democratic voting system and offers a degree of decentralization. The objective of this paper is to investigate and research blockchain security features, design and develop the proposed blockchain based e-voting system and evaluate the security that this system provides. The blockchain is built using Python programming language. A waterfall methodology approach is used to develop, analyze, and design the proposed system. Implementation of the system was done locally using XAMPP and testing was done locally. To conclude, this paper has shown that it is a viable alternative to traditional e-voting systems.

ABSTRAK

SISTEM PENGUNDIAN BERASASKAN BLOCKCHAIN DAN WEB BAGI JAWATANKUASA PILIHAN RAYA UMS

Pada zaman sekarang terdapat banyak inovasi yang dibawa ke hadapan kepada sistem yang sedia ada. Inovasi ini membantu menyediakan aplikasi yang berfungsi dengan lebih baik. Satu bidang terutamanya yang muncul dalam inovasi ialah rantaian blok. Teknologi Blockchain menawarkan pelbagai faedah daripada bidang ekonomi kepada penyimpanan data. Blockchain ialah kaedah penyimpanan data yang menghubungkan blok dengan rantai. Data blok tidak boleh diubah suai setelah ia disimpan sebagai blok. Aplikasi blockchain dalam e-undi menyediakan yang terbuka, adil dan tidak berubah. Dengan menyimpan undian pada rantaian blok, data itu kemudiannya selamat dan tidak boleh diubah suai. Sistem semasa menggunakan pangkalan data untuk menyimpan undian. Kertas kerja ini mencadangkan satu sistem untuk e-undi yang menggabungkan blockchain sebagai kaedah utama untuk menyimpan undi. Sistem ini direka bentuk untuk memenuhi keperluan sistem pengundian demokratik dan menawarkan tahap desentralisasi. Objektif kertas ini adalah untuk menyiasat dan menyelidik ciri keselamatan blockchain, mereka bentuk dan membangunkan sistem e-undi berasaskan blockchain yang dicadangkan dan menilai keselamatan yang disediakan oleh sistem ini. Blockchain dibina menggunakan bahasa pengaturcaraan Python. Pendekatan metodologi air terjun digunakan untuk membangunkan, menganalisis dan mereka bentuk sistem yang dicadangkan. Pelaksanaan sistem dilakukan secara tempatan menggunakan XAMPP dan ujian dilakukan secara tempatan. Sebagai kesimpulan, kertas kerja ini telah menunjukkan bahawa ia adalah alternatif yang berdaya maju kepada sistem e-undi tradisional.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Over the recent years electronic voting has started to become a trend and is preferred by many as a means of carrying out democracy. The vote is usually cast via a device or through the internet or more commonly denoted as online voting. Online voting has seen a growing number of users in the past years especially when it comes to colleges and schools. Due to the recent disruption in social activities caused by the COVID-19 pandemic, traditional voting methods are not encouraged as it may increase the likelihood of spreading the virus when in close proximity with others. Furthermore, electronic voting helps to speed up the process of counting votes and reduces the hassle of managing traditional voting ballots. However, there are major concerns that come into play when using online voting as a method of democracy. Election's fraud and other fraudulent attempts will leave a standard voting system at risk. These systems are required to be secure and tamper proof in order for it to function as intended to.

1.2 Research Background

Online voting systems have come to a rise and has recently been favored upon due to the COVID-19 pandemic. Being able to vote securely from anywhere in the world with a secure connection is becoming essential. Current voting systems on UMS portals are also inefficient at times especially when loading graphics from the websites. Efficiency will also be monitored to provide a faster user experience by reducing the graphics on the page so that low bandwidth users will be able to cast their votes. The blockchain system will have asymmetrical keys for better security and the user will be assigned a public key before voting. The private keys are stored on a blockchain that is secured and tamper proof. This will allow heightened security.

1.3 Problem Statements

As the pandemic has changed our social lifestyle it is crucial to find a new system that can accommodate the democratic process of voting in UMS. The existing system implements a system that uses a basic database which is susceptible to unauthorized tampering which can affect the integrity of the results. It also needs to accommodate all the students and their democratic needs. There are some issues with current deployments of e-voting systems, and they are listed below.

1. Lack of transparency in vote counting – Current voting systems are not transparent when it comes to keeping count of the votes. The score is only announced in the end and only 1 party has full access to the database.

2. Lack of security in data storage – Current voting systems that use a database to keep track of votes are not tamper proof. The database is also centralized. Nonrepudiation is also required.

3. Lack of voter anonymity – Current systems do not guarantee the anonymity of the user and the database method still requires a user to interact with it using their name. Blockchain will not store user data but instead the vote sent.

1.4 Project Objectives

Primary goal is to help provide a system that is secure and efficient to be used by UMS for their e-voting system.

• To investigate and research on blockchain security features and methods to implement.

• To design and develop a blockchain based e-voting system for the student council of UMS for use in their general elections.

• To evaluate the blockchain's performance in an e-voting system environment.

1.5 Project Scope

This project aims to develop an e-voting system which uses a blockchain as a data structure to store votes. The target users will be the voting council and the voters. This project will implement a blockchain as the data storage method for an e-voting application. The voting council will act as the systems administrator while the voters will act as the users. The project is divided into modules as shown in Table 1.1 .

Table 1.1 : Project Modules and Description

Modules	Description	Authority
Blockchain management	• Creates the genesis block for the blockchain and initializes the data • Acts as a starting point for the blockchain	Voting council
User management	• Administrative page to manage current users and voters	Voting council
Candidate management	• Administrative page to manage candidates	Voting council
Poll management	• Administrative page to manage the polling date.	Voting council

Cast vote	• Page to cast the vote to the corresponding candidate (creates new block into blockchain)	Voters
Dashboard	• Displays and prints the results of the elections	Voting council and Voters

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

A blockchain based e-voting system will require insight on how to implement a blockchain and link it together with an e-voting system. This link will be crucial in the functioning of the blockchain. This section will outline what is a blockchain and e-voting system. It will also outline previous papers and applications that have been used in the past.

2.2 Blockchain

Blockchains are an append-only data structure that was first envisioned by Stuart Haber and W Scott Stornetta in 1991. It was a cryptographically secured chain of blocks, or data, where timestamps of documents could not be tampered with. In 2008 it gained relevance when an entity, either a group or a person, named Satoshi Nakamoto released a paper about Bitcoin where blockchain technology was used to for a peer-to-peer (P2P) e-commerce system that allows users to exchange currency without the need of a central institution like a bank (Nakamoto, 2017). This makes it suitable for the recording of events, transactions and proving provenance. Blockchains such as the Ethereum blockchain is used for cryptocurrency to keep track of transactions.

The blockchain works by linking blocks together in a long line of data where each block will have a hash that is calculated, usually SHA-256 (Nakamoto, 2017). The block is then set to point to the previous block's hash in the chain of blocks. The first block in the chain is called the genesis block. This block does not have a previous block linked to it making it the first block in the chain. This process then carries on as new blocks are added into the chain. This type of data structure allows it to be tamper free as each block is linked to another block in the chain. When a block has its values changed, the hash for the block will also change. This will then cause the chain to break and make it invalid. Due to it being a P2P network of blocks, each node in the network will have a copy of the chain (Bolfing, 2020). When a chain loses one piece of data due to tampering it can always get the chain back by referring to other chains in the network. Blockchains grow stronger when there are more nodes in the network. As new blocks are added the hash value will be calculated.

Blockchain also serves as a decentralization point where the blockchain itself is distributed among members of the network in order for it to be held. There is no single owner that holds the blockchain and all new blocks are distributed via broadcast method to all the nodes of the P2P network. This allows for better reviewing of the data as the data is not held by one owner. Users may view the transactions that have taken place by going through the blocks in the chain. This benefits the stakeholders as data is transparent and available to all nodes.

Blockchain makes it very difficult for the chain to be tampered with due to its nature of using hashes and pointers. The chain can only be disrupted if the attacker can rewrite all the blocks in the chain to accommodate the tampered data. This will require an immense amount of processing power to recalculate all the hashes in the block and the other nodes in the P2P environment (Duong, 2020). Blockchain does come with certain challenges that needs to be faced. The processing requirements of calculating hashes is considerably low when calculating for few blocks, but the requirements will increase exponentially when multiple newer blocks are added into the chain. The diagram below shows the structure of a blockchain and how the link is crucial in ensuring the blockchain is tamper proof. Figure 2.1 explains the rudimentary structure of a blockchain. Each block has 3 major components. The previous hash is a pointer that refers to the previous block's hash in the chain.

Encrypted data is the data that is being held in the blockchain. This data is encrypted in SHA-256 and is stored in the block. The block hash is the current block's hash. This hash is crucial as it determines the integrity of the current block. If the current block is modified the hash value will change. This change in value will cause the chain to break as the next block is unable to point back to the previous block (Patidar , 2019).

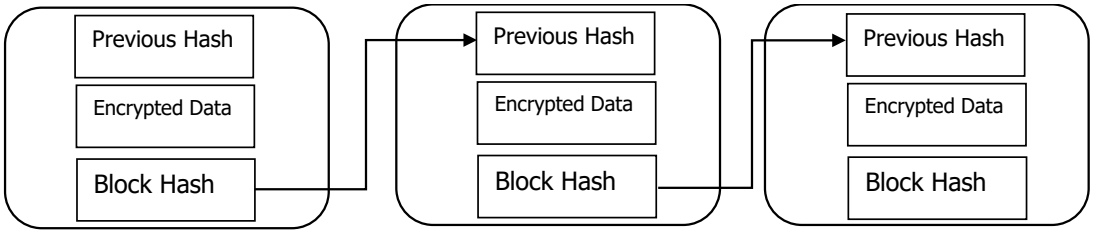

Figure 2.1: A blockchain's rudimentary structure and the linkage to the previous block

2.2.1 Security features in blockchains

There are multiple security features that are useful in a blockchain. This allows them to be a secure, append only data structure that is reliable enough to be used in cryptocurrencies (Wen, 2021).

Smart contracts are small computer programs that live inside the blockchain. It is small conditional expression code that executes when certain condition or conditions are met (Lopez Vivar, 2021). They execute automatically without user intervention and will help in authentication, verification and even enforcement. Smart contracts are advantageous because of their autonomy and ability to execute by itself. It makes certain processes faster and reduces time loss in the blockchain. This can save the executions time. In the current system the smart contract can be used to keep count in real time of the votes that are being added to the blockchain. The smart contract can automatically increase the count of the vote for the candidate in response to the block added. Smart contracts also allow for better security measures due to them being hardcoded into the blocks. Smart contracts do not need any intermediary to run thus making it decentralized.

Another important feature of the blockchain is SHA256 (Secure Hash Algorithm) encryptions (Duong, 2020). This is a cryptographical encryption that encrypts data when being stored in the blocks. It is 256-bits long. When data is stored in the blocks it is encrypted with SHA256 making it difficult to crack.

Besides that, another key feature in using open source blockchains is that they are maintained and patched very quickly. Ethereum blockchains are one example of open source blockchains. Being open source allows for transparency when it comes to using blockchains and incorporating them into other systems. (Lopez et al, 2021). Secrecy can be implemented depending on what type of data is stored in the blockchain.

2.2.2 Blockchain Technologies

Since there were few blockchain types to choose from an analysis was made on the existing open-source blockchain technologies. These include Ethereum, Bitcoin and Hyperledger. Choosing a particular blockchain required a few aspects to be considered. The first being that the blockchain has to be easily incorporated with other systems. The second is that the blockchain must support Smart Contracts. The third is that the blockchain needs to be able to support the data handling that is required by the e-voting system. Table 4.8 outlines the findings (ECCouncil, 2021) followed by the conclusion for the chosen blockchain technology.

Table 2.1 : Comparison Between Bitcoin Technologies

	Ethereum	**Bitcoin**	**Hyperledger**
Platform	Open Source		
Accessibility	Open to all	Open to all	Closed
Confidentiality	Public Network	Semi Private Network	Closed Network
Integration	Easy	Made for transactions	Easy
Smart Contract	Available	None	Available

2.3 Blockchain Applications in Other Fields

The most common use of blockchains can be seen in the financial field (Haferkorn, 2015). Cryptocurrencies use blockchain as a ledger to keep track of transactions. This is especially done due to the append only structure of blockchains. Banks and other financial institutions are also implementing blockchains for loan management schemes (Gazali , 2017) and general banking services (Cocco , 2017). The adopting of blockchains in the financial field allows for decentralized banking and financial services that are transparent and potentially cost saving (Accenture , 2017a). One application of a blockchain in banking is keeping asset ownership information on a distributed ledger. The distributed ledger is a blockchain that is distributed across other nodes which can help verify asset ownership by cross referencing the data. Image 2.1 shows the concept of the system.

Another field that is also pursuing blockchains is the IoT (Internet of Things) field. Blockchain architecture helps in enhancing the IoT while minimizing the deficiencies that are brought forward from distributed wireless sensor networks (Kshetri , 2017).IoT devices can also monopolize on the append only structure of blockchains to ensure consistent logging from devices and sensors. IoT enabled blockchains can help keep track of temperatures, locations, and contents of freight containers. The immutable nature of the blockchain allows all parties to trust the data and act on the freight quickly.

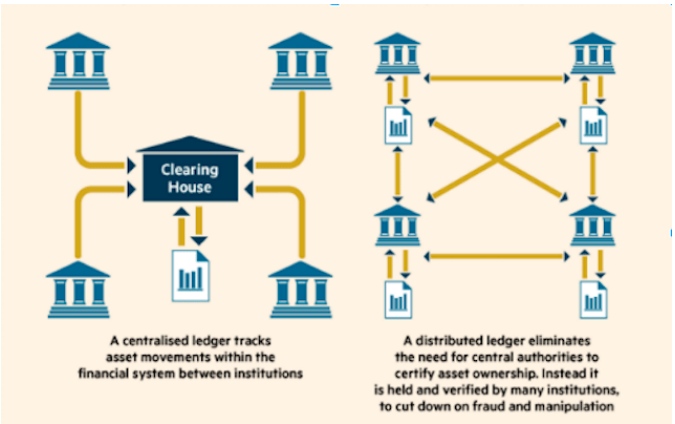

Figure 2.2 : Blockchain implementation in asset ownership verification process

2.4 E-voting systems overview

E-voting systems are being tested to be used in today's times (Petipas, 2021). The voting system relies on an electronic medium instead of the traditional paper ballot system. This system requires a machine or a web browser to cast the votes. The digital vote is then either stored on the machine itself or is sent to a central database. Then these votes are calculated and tabulated by a computer. This reduces the amount of manual work needed to count the ballot papers and manage them. Logistics problems are also solved in this manor where only the devices themselves are needed to be transported.

There are some issues that can be seen with the traditional database storing method. The first being that the votes are stored on a central server which is not tamper free guaranteed. Altercations to the results can be made if the system is breached (Tajpour, 2013) and there is no transparency when it comes to these systems. The device itself could also be tampered with and this can change the outcome of the votes. India has the second most population in the world. For their general elections they have chosen to use an electronic voting system instead of the traditional paper ballot. This allows them to tally the results quicker and it also allows better participation of voters because they can reach more people and ensure the safety of the votes (Ravi S, 2019). The easy-to-use system in India helped to reduce electoral fraud and 67% voter turnout during the 2019 elections.

The increase of participation and accuracy of tallying provided by electronic voting systems is helpful (Khan, 2020). However, the system by itself is vulnerable to vote coercion, data tampering and electoral fraud. By implementing a better data storage system this method can be safer. By introducing blockchain into the system, votes will become tamper proof due to the append only nature of blockchains.

2.5 Paper Reviews

To further have insight on the field of blockchain and e-voting, some past papers and applications were reviewed and studied. These papers provided reasonable information that can be used to aid the study and development of the proposed system.

The first paper studied was Decentralized E-Voting Portal Using Blockchain by Kriti Patidar and Dr. Swapnil Jain. The paper was aimed to develop an e-voting portal using blockchain. It aimed to deliver a system where the voting is completely decentralized and open while being online. It implemented a blockchain to store the votes. There were some limitations. The system was complex due to the blockchain's nature, and it would hinder its wide acceptability among users (Patidar, 2019).

The second paper studied was Blockchain-Based E-Voting System by Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa and Gísli Hjálmtýsson. The paper aimed to develop a system that reduces cost of running an election while ensuring the integrity, security, and privacy aspects of the election. The limitations were that the system could not ensure that the votes received are coercion free. Another limitation was that large number of votes could not be supported due to the blockchain's hashing requirement (Abuidiris Y, 2019).

The third paper studied was Blockchain-Enabled E-Voting by Nir Kshetri and Jeffrey Voas. This paper highlighted some of the blockchain e-voting (BEV) implementations and the approach's potential benefits and challenges. The past systems that were used as an example was the 2018 Sierra Leone elections where a BEV was used to conduct the whole election process. Improved identity verification is very important as voting rights need to be maintained across the board and no duplicate or coerced votes can be tolerated. The downside to the system was internet connectivity being a requirement and the user's skill level in operating a computer. The scalability of bitcoin is also a concern as when the number of votes go up, the hardware requirement to calculate the hashes increase together (Kshetri, 2018). From these papers we can conclude that a blockchain can be implemented into an e-voting system and it will be able to store votes that are immutable.

Table 2.2: Blockchain Voting Systems Paper Summary

Source Info	Decentralized E-Voting Portal Using Blockchain	Blockchain-Based E-Voting System	Blockchain-Enabled E-Voting
Research topic	completely decentralized and open, online voting system based on blockchain	minimize the cost of running an election, while ensuring the election integrity by fulfilling the security, privacy and	highlight some BEV implementations and the approach's potential benefits and challenges.
Methodology	Past research	Past research	Past research
Findings	decentralized voting system	secure and cost-efficient election	improved identity verification
Limitations	blockchain systems are complex in nature which may hinder its wide acceptability	no coercion resistance and therefore could lead to false election results (forced vote)	Broadband access and digital user skills
Areas for future research	feasibility of blockchain based e-voting system for large-scale election	additonal research on methods to increase throughput of votes at larger scales	Scalability of blokchain

2.6 Application Reviews

Two applications were also reviewed that used blockchains as a medium to store the votes. The first one is TIVI Voting System followed by Agora.

2.5.1 Agora (Sierra Leone, 2018)

Agora is a blockchain based voting system that was developed by a Swiss tech-company for the Sierra Leone 2018 presidential elections. This voting system implemented a blockchain in order to tally the results. The voters however used the traditional paper ballot system to cast their votes. The ballots were then read by a group of polling station agents in order to be keyed in to the blockchain via an electronic device. This system however was only used on the side as a testing platform for the effectiveness of implementing a blockchain in a voting system. The development team of Agora ran the results through their blockchain and compared it with the traditional counting method to check for accuracy and the margin of difference was between 0.3 > 0.03 (Team A.B., 2018). This proves that the