Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technologies

Bachelor Thesis

A blockchain based e-voting system: a case of Nepal

Sanij Shrestha

© 2021 CULS Prague

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

BACHELOR THESIS ASSIGNMENT

Sanij Shrestha

Informatics

Thesis title

A blockchain based e-voting system: a case of Nepal

Objectives of thesis

The main objective of the thesis is to examine the possible application of blockchain based e-voting system in Nepal.

The partial objectives of the thesis are such as:
- to make an overview of the core concepts of blockchain technology and the current state of the art of e-government in Nepal;
- to analyse the prerequisites to implement blockchain technology in the Nepalese e-government;
- to propose and evaluate a solution of blockchain based e-voting system in Nepal.

Methodology

The methodology of the thesis is based on the review of the literature and practical part. At the beginning, a literature review of blockchain and the current state of the art of its use in e-government will be done. Secondarily followed on the implication of the economic, social, geographical and other sectors in Nepal, a concept of blockchain adoption in Nepalese e-government will be proposed. Software engineering methods such as data flow diagram, use case diagram as well as scientific methods such as analysis, synthesis, comparison, induction and deduction will be used. Based on the results of the literature review and practical part, final recommendations and conclusions will be formulated.

The proposed extent of the thesis

30 – 40 pages

Keywords

Blockchain, e-Government, e-voting, e-Government services,

Recommended information sources

Atzori, M., 2015. Blockchain technology and decentralized governance: Is the state still necessary?.

Howard, M., 2001. E-government across the globe: how will'e'change government. e-Government, 90, p.80.

ØLNES, S., 2016, September. Beyond bitcoin enabling smart government using blockchain technology. In International Conference on Electronic Government and the Information Systems Perspective (pp. 253-264). Springer, Cham.

STEVE CHENG, MATTHIAS DAUB, AXEL DOMEYER, AND MARTIN LUNDQVIST. Using blockchain to improve data management in the public sector. McKinsey & Company.25.02.2018. Available from: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector

Tough, A., 2011. Accountability, open government and record keeping: time to think again?. Records Management Journal, 21(3), pp.225-236.

Expected date of thesis defence

2021/22 WS – FEM

The Bachelor Thesis Supervisor

Ing. Miloš Ulman, Ph.D.

Supervising department

Department of Information Technologies

Electronic approval: 11. 9. 2018

Ing. Jiří Vaněk, Ph.D.

Head of department

Electronic approval: 19. 10. 2018

Ing. Martin Pelikán, Ph.D.

Dean

Prague on 27. 11. 2021

Declaration

I declare that I have worked on my bachelor thesis titled "A blockchain-based e-voting system: a case of Nepal" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the bachelor thesis, I declare that the thesis does not break any copyrights.

In Prague on 30.11.2021 _____

Acknowledgment

The author would like to thank the supervisor of this paper Ing. Miloš Ulman, Ph.D. for providing the necessary assistance for the completion of this work

A blockchain-based e-voting, a case of Nepal

Abstract

This bachelor thesis examines the possibility to adopt blockchain in the e-government of Nepal and proposes an approach to implement blockchain-based e-government in Nepal. Although the idea of e-voting has not been commonly practiced by many countries, some attempts of a few countries have proven its efficiency and accuracy while maintaining trust among their citizens. The theoretical part of this thesis assesses the current state of e-government in Nepal and provides some detailed information on the blockchain and its components. It also provides some examples of the implementation of blockchain technology by different countries across the globe. The practical part analyses the electoral system in Nepal and proposes an approach to adopt blockchain-based e-voting in Nepal, this section also includes data flow diagrams, a use case diagram, and cost analysis of the proposed approach. Furthermore, SWOT analysis of the proposed system is performed to assess the system.

Keywords: E-government, E-government services, Blockchain, Decentralized Voting, E-Voting, Nepal. Smart contracts, Hyperledger Fabric, blockchain in Nepal

Table of content

List of pictures

List of tables

List of abbreviations

IT	Information Technology
ICT	Information Communication Technology
PoS	Proof-of-Stake
PoW	Proof-of-Work
BEV	Blockchain-based Electronic Voting
AWS	Amazon Web Services

1 Introduction

In the world of infinite possibilities, we came across many eras from the stone age to the technological. With the boom of ICTs, e-mails, e-commerce, and e-government were introduced. The electronic government began with the motive of providing simple, effective, and convenient interactions between the government and the citizen by utilizing the ICTs. E-government has been gaining massive attention and popularity among the countries and is adopted by many governments. Over 90 countries now have a single entry platform for public records, online services, or both, and 148 countries have at least one type of online transactional service (United Nations 2020). Government, by going online and delivering public services and information through the internet to its citizen can enhance the service level and public participation. Affective, efficient, and accessible by the public 24/7 affects the function related to document management and processing.

In developing countries like Nepal, the implementation of e-government is very challenging due to various reasons. The first reason is the e-readiness followed by the low-connectivity and design-reality gaps. E-readiness refers to the measure of the ability of a country or organization to use the information and communication technology benefits whereas the other reason design-reality gap means the existing size of the gap between current realities and the design of e-government projects. The smaller the gap, the great chance of success. If these issues are not taken into consideration, the e-government projects will only benefit the skilled people and not the ordinary people. Although the e-government is being adopted by many governments of developed countries, the biggest challenge is data security and trust.

Blockchain, the underlying technology beyond cryptocurrency Bitcoin, has already proved its capability with the success of bitcoin. Many countries in Europe have successfully implemented blockchain in e-government. Blockchain securely stores the data of the transactions between the government bodies and citizens carried out in a very vulnerable environment, like the internet. without the need of any third party. Blockchain in e-government aids to bring trust and transparency in e-government projects. The core benefits of adopting blockchain in e-government are security, public participation, and intermediary less transaction recognized internationally without breaking the bank.

2 Objectives and Methodology

2.1 Objectives

This thesis is focused on the implementation of blockchain technology in e-government. The primary goal of the thesis is to examine the possible application of blockchain based e-voting system in Nepal

The partial goals are as follows:

- to make an overview of the core concept of blockchain technology and the current state of the art of e-government in Nepal
- to analyze the prerequisites to implement blockchain in the e-government of Nepal
- to propose and evaluate a solution for a blockchain based e-voting system in Nepal.

2.2 Methodology

The methodology of the thesis is based on the review of the literature and practical part. In the beginning, a literature review of blockchain and the current state of the art of its use in e-government will be done. Secondarily, followed by the implication of the economic, social, geographical, and other sectors in Nepal, a concept of blockchain adoption in Nepalese e-government will be proposed. Software engineering methods such as data flow diagrams, use case diagram as well as scientific methods such as analysis, synthesis, comparison, induction, and deduction will be used. Based on the results of the literature review and practical part, final recommendations and conclusions will be formulated.

3 Literature Review

3.1 Blockchain

In 2008, ‘Satoshi Nakamoto' conceptualized and introduced blockchain as the key component of the cryptocurrency bitcoin, where it serves as the public ledger for all network transactions. Bitcoin was the first digital currency to address the double-spending issue without the need for a trusted authority or intermediary, thanks to the use of blockchain technology (HILL, WALLNER, FURTADO 2010).

Blockchain is a decentralized and distributed database of records, or public ledger, of all transactions or digital events that have been executed and exchanged among the participating parties (Baars, Kemper 2015). Every ledger from a transaction is verified and apostilled by the consensus of many of the members in the framework. When entered, the data can never be adjusted or deleted. Any transaction that ever occurred is recorded on the blockchain.

Dissimilar to the customary bookkeeping methods which are centralized and stored in a solitary book or database system, blockchain technology is decentralized and distributed among an enormous network of computers making data tampering exceptionally difficult.

Blockchain is a cumulation of two unique words ‘block’ which alludes to a bunch of databases and ‘chain’ alluding to the connection between the accessible set of blocks. Each block contains the cryptographic hash, timestamp, and transaction data of the previous block (generally addressed as a Merkle tree) (Benbya, McKelvey 2006). To adjust a record each existing block has to be modified.

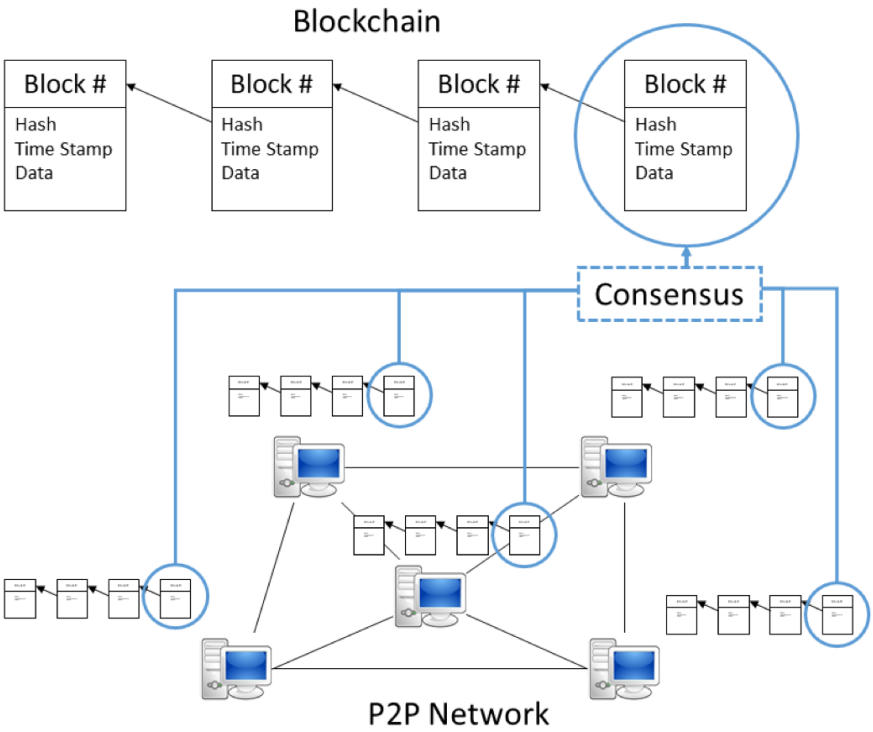
3.1.1 Blocks and hash

A block is made up of two sections: a block header and a block body. Block header data incorporates block edition, parent block hash, Merkle tree root hash, Timestamp, nBits, and Nonce. The block body comprises transactions and a transaction counter.

Hash is a computerized cryptographic signature used to validate the authentication of the transaction (Zheng, Xie, Dai, Chen, Wang 2017). The blocks are linked utilizing unique hashes. When there is an endeavor to alter the block a new block is created with an alternate hash which would be invalid because of the mismatch in the hash.

Hashing was executed by Satoshi Nakamoto as the ‘Proof of Work' in bitcoin, a process that connects consensus with computational power, rendering participant duplication influential to consensus outcomes. The proof work done by the ‘miners.' There is rivalry among miners in the mining process (Aste, Tasca, Matteo 2017).

Figure 1: Key elements of blockchain systems
(Cai, Wang, Ernst, Hong, Feng, Leung 2018)



Blockchain disposes of the requirement for a trusted third party to serve as a middleman in a transaction. It will function like a trusted third party, approving each transaction with a digital time stamp, safeguarding, and maintaining the transactions without charging a transaction fee, and preventing fraud. After the transaction is completed, a copy is distributed to everybody on the network.

3.1.2 Digital Signature

Every user on the network has a pair of private key and the public key stored in a database known as "Wallet." These keys are utilized in two distinct stages: signing and authentication. The private key generates a unique digital signature that is used in signing the transactions. The public key is used to access the digitally signed transactions and create a publicly shareable address for the user which empowers to spread of the transaction throughout the network.
If we were to use the currency analogy, a single unit of any blockchain is a digital token. Following this comparison, it is being utilized using similar methods as a dollar would. Regulators are in this case the designers of the blockchain, as it's via their design that the amount of digital tokens in circulation is regulated (Spielman, Supervisor 2016).

The three core functions of blockchain technology are as follows:
1. Check for errors in entries.
2. Keep entries secure
3. Preserve historical documents

Hashing was implemented by Satoshi Nakamoto as the ‘Proof of Work' in bitcoin, a process that connects consensus with computational power, rendering participant duplication influential to consensus outcomes. The evidence of work is carried out by the ‘miners.' There is rivalry among us in the mining process (Aste, Tasca, Matteo 2017).

3.1.3 Permissionless blockchain vs Permissioned blockchain

A permissionless blockchain is a very first generation of Distributed Ledger Technology (DLT) to provide decentralized ledger rather than centralized databases where anybody with a blockchain fundamental can run a node and read, write, or participate within the blockchain. The consensus mechanism element of public blockchain keeps the network running in a decentralized manner offering greater transparency. A well-known example of permissionless blockchain is Bitcoin and Ethereum. (Hedgetrade 2019).

Permissioned blockchains accomplish an incredible bargain of decentralization; be that as it may, they cannot ensure the protection and security required for touchy citizens and government information. Only a verified or predefined list of entities is limited to accessing blockchain data and submitting transactions. One or more entities control the network (BitFury 2017) and participants are strictly controlled by a central authority in permissioned blockchain. Private blockchains are more suitable for government and businesses where they want privacy in their data. Blockchain policies exist on the framework to confer authorizations to stakeholders needed to operate specific activities. For case, when a public administration requests a specific piece of data, the individual must be notified, and the individual must assent for access to be granted. However, decentralization is impacted when a central authority is created to authorize the private network's participants, and a controlling authority acquires access to the network (Terzi, Votis, Tzovaras, Stamelos, Cooper 2019). The Best-known examples are Hyperledger and Ripple.

Table 1: Permissionless blockchains vs permissioned blockchains
(Metaco 2020)

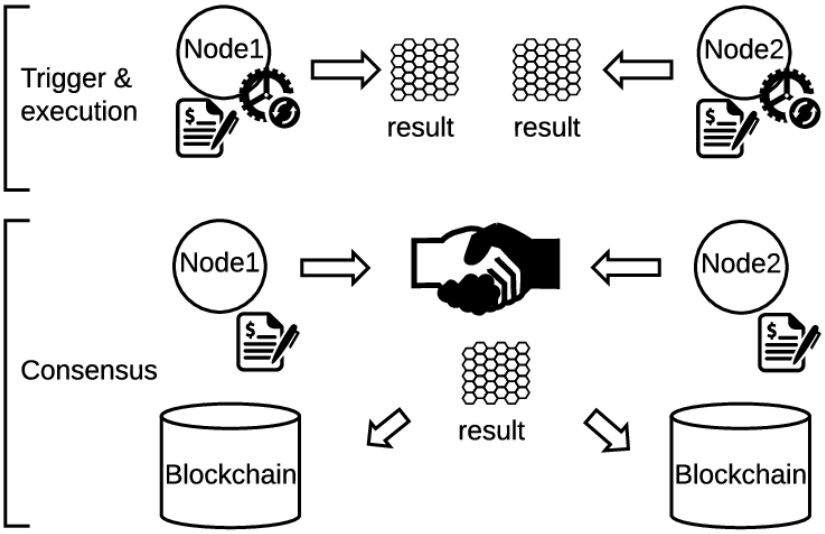
Permissionless blockchain	Permissioned blockchain
Open, Public	Closed -only approved users can access
No gatekeepers	Only governing authority acts as a gatekeeper
Trustless -the math is the proof	The governing authority provides an inherent level of trust
Consensus take longer time due to complex computations	Consensus is quick due to limited number of users means the required computations are relatively less complex
More Mindshare	Less mindshare

3.1.4 Smart Contract

Smart Contracts are blockchain-chain-based computer programs that blockchain participants can execute. Smart contracts add automation and control flow logic to any system that is

supported by blockchain. Smart contracts engines must be stochastic and should be considered in any and every situation as software functions. The deterministic property of smart contracts retains consistency and stability, regulates transaction permanence, and discourages soft and hard forks. Usually, the developer oversees deciding the determinism of smart contract's actions. As a result, he/she must ensure that automated actions are implemented as planned so that the results of these actions end up leaving the data in a consistent state, despite the node(s) on which they are conducted. The action of the smart contract must produce the same result for every time the smart contract is executed (Terzi, Votis, Tzovaras, Stamelos, Cooper 2019).

Figure 2: Smart contract execution and consensus
(Diallo, Shi, Xu, Gao, Chen, Lu, Shah, Carranco, Le, Surez, Turner 2018)



3.1.5 Decentralized Application (dApp)

Th majority of the current blockchain-based applications are yet restricted to utilizing smart contracts for core data and functionality that is liable to risks. Smart contract clients still ought to run their applications locally to complete the application. One of the primary reasons is the execution confinement of present blockchain technology. This poses a challenge concerning operational security and application maintenance. For example, there could be deliberate cheating behaviors hidden from the public audit in the local components (Cai, Wang, Ernst, Hong, Feng, Leung 2018).

Decentralized applications are just like other applications that we use in our daily life however, there are a few key features that make dApp stand out from regular applications. DApp backend code runs in a decentralized peer-to-peer network. In contrast, consider an app where the backend code is hosted on centralized servers. Like an app, a dApp can contain front-end code and a user interface written in any language that can call the back end. In addition, the front end can be hosted on a distributed storage system (Ethereum 2021).

DApps are decentralized, deterministic, Turing complete, and isolated. Advantages of dApp developments are zero downtime, privacy, resistance to censorship, complete data integrity,

trustless computation/verifiable behavior. However, due to its code and data being published in blockchain it can be harder to maintain and modify and release updates if some security bugs are identified in previous versions. Also, there can be issues with network congestion if a single dApp consumes too many computational resources, the entire network suffers. The network can currently only process about 10-15 transactions per second; if transactions are sent in faster than this, the pool of unconfirmed transactions will quickly grow. These are some of the implications of the dApp development (Ethereum 2021).

3.1.6 Proof of Work vs Proof of Stake

Satoshi Nakamoto used Proof-of-Work (PoW) to unravel the double-spending issue. The PoW includes a scientific calculation to filter for a numeric value that when hashed, the hash result starts with a particular number of zero bits. With PoW, each peer within the P2P network must compete in tackling the puzzles, which is additionally called mining. The champ of each competition will have the privilege to make a block and broadcast it to their peers. However, proof-of-work demands a massive amount of energy and investment on computational devices to achieve consensus for each new block; a quantify so large that the supported blockchains struggle to maintain and grow to the performance requirements of global networks. Despite that, the peers who effectively make a few blocks will get coin rewards for their work (Cai, Wang, Ernst, Hong, Feng, Leung 2018).

Proof-of-stake overcomes the performance and energy-use issues that plague proof-of-work, resulting in a more long-term solution. Rather than depending on ‘miners' to solve computationally hard equations to produce new blocks — and rewarding those who do it first – Proof of stake allows members to construct new blocks based on how much of the network's stake they own. This allows networks to extend horizontally, rather than vertically, by adding more powerful hardware, enhancing performance by including extra nodes. The difference in energy use results can be compared to the difference between a household and a small country. proof-of-stake is geared toward the mass market, but proof-of-work is not (Cardano 2020).

3.2 E-government

E-government is no longer a completely new term. E-government is a natural evolution of how government services respond to broader economic and social changes. E-government enables people to participate in government services and initiatives through low-cost collaboration and interaction, and time-efficient features, benefiting both government services and their citizens. As the number of Internet users grows, governments and citizens raise and investigate issues affecting their communities and similar community impacts, influencing discussions within Congress without visiting the city has become a very efficient (Howard 2001).

E-government refers to the use of information technology by government agencies (wide area networks, the Internet, mobile computing, etc.) that can transform relationships with citizens, businesses, and other government agencies. These technologies serve a variety of purposes, including improving the provision of government services to citizens, improving interactions with businesses and industries, empowering citizens with access to information, and more effective government management. The resulting benefits are reduced corruption, increased transparency, increased convenience, increased sales, and/or reduced costs (Bank 2013).

Some people define it simply to make digital government information or digital transactions with customers. For others, e-government simply creates websites that provide information on political and government issues. These narrow definitions and conceptualizations of e-government limit the possibilities it offers. One reason numerous e-government projects fall flat is identified with the restricted definition and absence of comprehension of e-government ideas, cycles, and capacities. E-government is a multidimensional and complex concept that requires extensive definition and understanding to design and implement an effective strategy.

Analyzing these definitions can identify the main aspects and components that characterize the e-government framework, including:

1. Transformation areas (internal, external, relational).
2. Users, customers, actors, and their interrelationships (citizens, businesses, government organizations, employees).
3. E-government application domains (e-services, e-democracy, e-administration) (Ndou 2004).

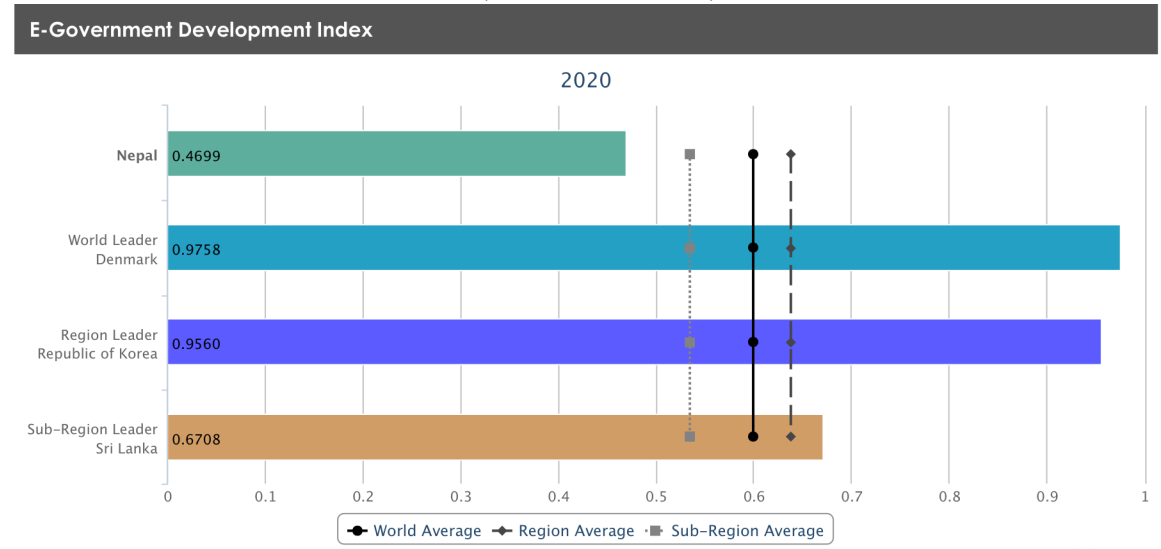
3.2.1 Status of ICTs and current scenario of e-government in Nepal

United Nations have been conducting surveys to measure the development of the national e-government capabilities. The E-Government Development Index (EGDI) is a composite index consisting of three equally weighted indexes (Online Services Index, Telecommunications Index, and Human Capital Index) (Камерницкий, Левина 2005). The human capital index is used to measure the ability of citizens to use e-government services.

Nepal is lacking behind in the south Asian region and has a middle EGDI level and ranks 132 out of 193 in 2020 compared to EGDI from 2018 where Nepal ranked 117. Nepal is declining

its rank whereas neighboring countries like Bhutan have been able to incline its rank ahead of Nepal. The world average EGDI is 0.5988 in the 2020 (United Nations 2020).

Figure 3: E-Government Development Index
(United Nations 2020)



E-Government Development Index	2020	2018	2016	2014	2012	2010	2008	2005	2004	2003
Nepal (Rank)	132	117	135	165	164	153	150	126	132	130
Nepal (Value)	0.46990	0.47480	0.34581	0.23442	0.26644	0.25677	0.27250	0.30211	0.28074	0.26839

To lay the establishment for e-government, the government of Nepal has arranged the e-Government Master Plan Counselling Report (e-GMP) as a team with the Korea IT Industry Promotion Office (KIPA). Following a study of ICT methodologies, law, and laws associated with e-Government, the advisory group discovered some repercussions. The group also organized several gatherings with experts and various governments, as well as driving appraisal discussions with residents, corporate representatives, and government officials. KIPA also held several workshops in Nepal to form visions and missions for e-government.

The vision of e-government is 'The Worth Systems administration Nepal' through:

- Citizen-focused assistance
- Transparent Administration
- Networked government
- Knowledge-based society

According to Nepal government (Nepal 2020), the current government's goals through e-government is such as:

- Becoming more proactive
- Improve internal efficiency and service levels of members Greater transparency
- More service-oriented
- Reduction of operating costs
- Change people`s view of the government as bloated, wasteful, and unable to meet urgent needs

- Develop new sources of growth and ways to reduce vulnerabilities
- Better public services and quality of life
- Electronic communication between government agencies
- Citizens can conduct frequent and complex administrative procedures with agencies electronically

During and after the COVID-19 pandemic, e-governance has become a major focal point of government initiatives in Nepal. Nepal is one of the least developed countries that has embarked on an e-governance effort that has been fraught with difficulties. It is argued that e-governance can cut administrative and development issues. However, in undeveloped or underdeveloped countries like Nepal, extra effort is required to achieve e-governance. In this regard, e-governance facilitates democratic contact between the government and its citizens by increasing efficiency and transparency in government transactions (Sharma 2020). Table 3 includes the challenging factors found in the implementation of e-governance in Nepal.

Table 2: Identified factors influencing implementation of e-governance in Nepal during and after the pandemic

(Sharma 2020)

Factors	Challenges of e-governance adoption
Technical factor	Power supply, digital gap, e-readiness, privacy, and security
Education and public participation	Internet availability, low ICT literacy and education
Political factor	Frequent changes in regulation and legislation, political instability, government priorities, and political leaders
Cultural factor	Employees resist amendment, corruption
Human resource factor	Insufficient human resources, lack of government awareness
Training on human resources	Public sector awareness, lack of training, information sharing, and transparency are still restricted
Financial factors	Investment problems, sustainability

The below table contains the list of the available e-government portals of Nepal.

Table 3: List of e-government portals of Nepal
(Nepal 2020)

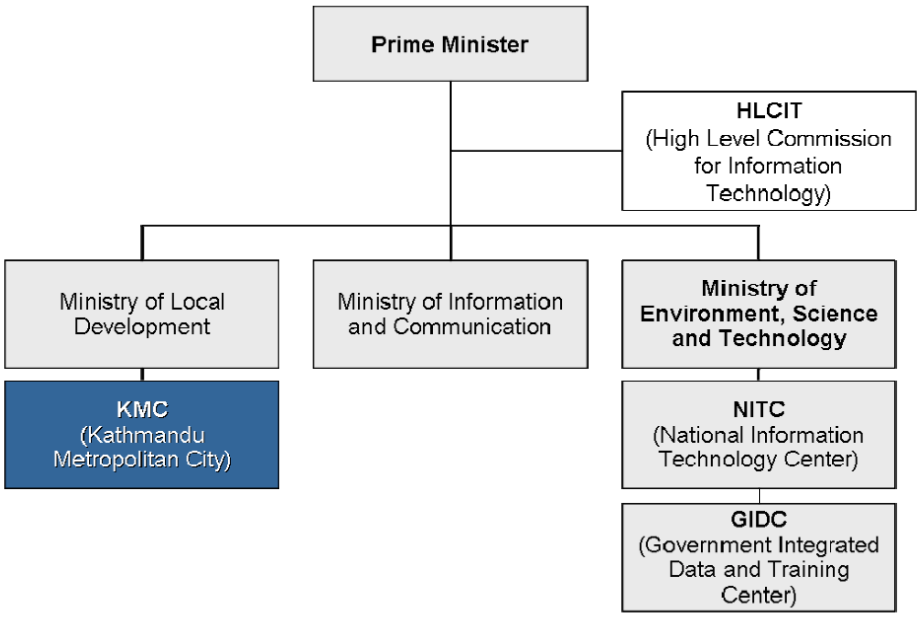
Portals	URLs
Inland Revenue Department (e-VAT, e-PAN, e-Fillings, e-TDS)	https://nepal.gov.np:8443/NationalPortal/irdService
Hello Sarkar (OPMCM)	https://nepal.gov.np:8443/NationalPortal/gunasoService
Public Service Commission	https://nepal.gov.np:8443/NationalPortal/pscService
IMEI check	https://nepal.gov.np:8443/NationalPortal/ntaService
Reconstruction progress	https://nepal.gov.np:8443/NationalPortal/privateHousing
Land Property Owner Details (DOLRM)	https://nepal.gov.np:8443/NationalPortal/lPDetailsService
Property Detail Submission Status (DOCPR)	https://nepal.gov.np:8443/NationalPortal/pdssService
Building Permit Tracking System (KMC)	https://nepal.gov.np:8443/NationalPortal/bptsService
Passport Status (OOP)	https://nepal.gov.np:8443/NationalPortal/pStatusService
Department of Foreign Employment (DoFE (Pre-permission details))	https://nepal.gov.np:8443/NationalPortal/dofeService
Department of Foreign Employment (DoFE (Passport))	https://nepal.gov.np:8443/NationalPortal/dofePassportService
Department of Passports	https://online.nepalpassport.gov.np/PreEnrollment/home.html
Department of Passports (MRP Status)	https://nepalpassport.gov.np/choose/district/?post_type=receivedstatus
Department of Consular Services (Attestation Verification)	https://nepalconsular.gov.np/attestation/public/
Department of Consular Services (Diplomatic and Exemption)	https://nepalconsular.gov.np/diplomatic/public/
Election Commission Nepal	http://www.election.gov.np/election/np/voter-list.html
Ministry of Health and Population (List of Doctors)	http://moh-doctors.herokuapp.com/
Department of Immigration (Online Application)	http://online.nepalimmigration.gov.np/
Department of Land Management and Achieve	https://public.dolma.gov.np/dolma/#/auth/login

3.2.2 IT Policy of Nepal

Nepal's most recent ITC policy paper is the IT Policy of 2015. According to the policy, it is "intended to lay the foundations for an overall vision of Digital Nepal." It focuses on the concept of PPP, sustainable development, net neutrality, environmental effect, and climate change. The agenda also includes objectives such as achieving 100 percent internet connection in Nepal by 2020 and making 80 percent of government services available through digital methods.

To formulate the IT policy, the government of Nepal formulated High-Level Commission for Information Technology (HLCIT).

Figure 4: Major ICT governance organization
(Government 2009)



The use of information and communication technology will continue to support the flow of information to make public service delivery more effective. In this context, the e-Government Master Plan by 2016 Amendments and modifications will be implemented.

3.2.3 Overview of implementation of blockchain technology in e-government

In April 2016, Bitfury and the Republic of Georgia entered a partnership to construct a one-year pilot project to migrate the country's land registry system to a Blockchain Platform. As part of the first phase of the project, Bitfury built a blockchain-based timestamping layer on top of the National Agency of Public Registry's (NAPR) existing digital land registry system (Shang, Price 2019). Most of the changes were made to the system's backend, where certificates are timestamped and hashed in the Bitcoin Blockchain while the login procedure remained the same for the end-users to avoid confusion. Users can view records that have been cryptographically confirmed to be legitimate by logging into the NAPR website on their PC or mobile device. The project has expanded to include the processing of land title purchases and

sales, new land title registration, property demolition, mortgages and rentals, and notary services (New America 2020). The new system helped citizens to register the property in just one day also bringing the cost to only 0.1 percent of the property value (Shang, Price 2019).

In March 2017, the Ddabok Community Support Project was voted on using a Blockchain-based Electronic Voting (BEV) system in the South Korean province of Gyeonggi-do. A blockchain platform established by the Korean financial technology startup Block that featured smart contracts was used to vote by 9,000 citizens. A blockchain was used to store the votes, results, and other pertinent data. This approach involves no management or central authority. This was the first time a technique like this was used in South Korea. (Kshetri, Voas 2018)

A member of the Ukrainian election team logged into Facebook in August 2018 to reveal his involvement with the blockchain. According to the report, the country is in the testing phase and is considering all the logistics necessary for the pilot voting system of the NEM blockchain.

The administration of the province of Zug, Switzerland, through the registry department, began issuing digital IDs based on ETH on November 15th, 2017. The country's involvement in the blockchain sector has earned it the moniker "crypto valley." Below are some examples of successful implementation of blockchain in e-government. (ALISON MCGUIRE 2018)

The government of Estonia has introduced several incentives like blockchain-based E-Residency and Digital Health Services.

The National Energy department of Chile launched the use of blockchain in energy on April 19th. To establish accountability in the industry, the government employs the Ethereum blockchain to track data and finances. The results of the energy blockchain project, “Energy Abierta” will be researched and shared with other fields to further exploit the blockchain.

The Brazilian government is looking to move petitions that require voting and popular vote to Ethereum intending to increase accountability. If it passes Congress and the bill is signed, it will address the nation's inefficient system.

Venezuela declared the Petro coin to be their primary currency at the start of 2018. This was done to phase out the Bolivar, which was experiencing record-breaking inflation.
Petro coin is an oil-based coin, with each coin backed by the country's oil reserves. Even though the whitepaper states that the coin is an ERC-20 token on the Ethereum blockchain, the coin runs on the NEM blockchain. The coin has been chastised for its grey areas, and expectations that it will be able to save a failing economy are being called into question. However, business analysts believe the Petro coin has growth potential.

West Virginia has decided to use the blockchain-based mobile application in all the 55 counties during the midterm election after a successful pilot in the two states.

Nevertheless, eSatya a private company in Nepal has been working on several private blockchain-based applications such as land registry, aid distribution, identity management, and more on a private blockchain network.

3.3 Challenges of implementing blockchain in e-government of Nepal

After reviewing several works of literature about the state-of-the-art e-government and blockchain technology and its implementation by governments of various countries in several aspects. Blockchain technology in e-government proves to be beneficial which can provide greater transparency, cut the bureaucracy, provide trustworthy, flawless, and cost and time-efficient services to its citizen.

The developing countries must be motivated and build a stable infrastructure for the digitalization of public services. For successful implementation of such technology in various industries, blockchain and e-government concepts and challenges need to be analyzed and evaluated. For a government to prosper, it must first overcome many challenges, including overcoming national financial, social, and technical barriers.

- Low Internet penetration
- Infrastructure constraints
- Digital gaps
- Privacy and security concerns
- A limited number of qualified IT specialists
- Unavailability of Payment Gateway
- Lack of Digital Signature
- Lack of IT literacy among the citizens

Besides these challenges of e-government, there are regulations from Nepal Rastra Bank which states that "It is illegal to trade bitcoin or any other sort of cryptocurrency in Nepal".
After conducting a comprehensive literature study to identify current research and possible uses of blockchain technology in e-government applications, given the relevance of the potential usage of blockchain in the public sector. To do this, we devised the following research question:

1. *What are the issues related to the current electoral system of Nepal?*
2. *How should Nepal approach the adoption of blockchain technology in e-voting?*

4 Practical Part

4.1 Elections in Nepal

Voting systems have existed for hundreds of years and, despite differing opinions on their effectiveness, have always been regarded as secure due to a few basic security and anonymity principles. Various electronic frameworks have been proposed and implemented, but some concerns have been expressed about the integrity of decisions because of security flaws discovered in these systems. Electronic voting requires a more easy and secure technique than current frameworks provide to be successful (Tarasov, Tewari 2017).

The newly elected Constituent Assembly declared Nepal the Federal Democratic Republic on May 28, 2008, putting an end to the country's 240-year monarchy. According to Article 245 of the constitution of Nepal, an Election Commission is shaped of five Election Commissioners, one of them is Chief Election Commissioner and acts as the chairperson. They serve one term of six years and are named by the President at the suggestion of the Constitutional Board. It plans a voter's list for the election on subjects of national as per the law. During the federal election, Nepal is divided into 165 constituencies.

There are three sorts of the constituent framework in Nepal:

- Parallel voting for House of Representatives and provincial assemblies.
- Single Transferable Vote (STV) for National assembly.
- First Past the Post (FPTP) for local elections.

To participate in the election, the individual should be a Nepalese citizen and should be at least 21 years for local government, 25 years for Parliament assembly, and 35 years for national assembly who are not holding any post of profit and punished for criminal cases and moral disgrace.

The voting process is as follows:

- Eligible citizens are required to register in the respective constituency by proving required documents to obtain a voter identity card.
- On the election day, the voter should visit the polling station of the constituency and prove his identity and sign a voter list.
- The voter will receive a ballot paper and use the stamp to select the preferred candidate.
- After the end of the election, the vote ballots are transferred for the counting of the vote manually and declared a winner.

Table 4: Voting data according to 2017 general election of Nepal

(Election Commission of Nepal 2017)

Valid votes	9,544,744	90.15
Invalid/blank votes	1,042,777	9.85
Total votes	**10,587,521**	**100.00**
Registered voters/turnout	15,427,731	68.63

4.1.1 Problem formulation

It is not new to our ears that we hear the news about manipulation of votes and vote frauds in elections. Even if there has not been any it is hard to prove. Within the general election of Nepal in 2013, the pioneer of Nepal's biggest Maoist party requested a stop to the country's vote checking due to what he called a widespread voting fraud (Gardiner Harris 2013). It is also known that the traditional election costs a lot of taxpayer money. The state's election expenses are anticipated to exceed NPRs 20 billion (approximately USD 200 million) there in the upcoming parliamentary election of Nepal. When the costs of candidates and parties are added together, the overall cost could approach NPRs 100 billion (approximately USD 1 billion). In an interview with APEX, former Chief Election Commissioner Neel Kantha Upreti states, "Elections in Nepal are getting increasingly expensive, with election-related expenses of both state and party candidates increasing at rates higher than market inflation." In a poor country like Nepal, this poses a threat to democracy's long-term viability (The Annapurna Express 2021).

People need to build trust in their government and for sustainability, a trusted voting system should exist. The emerging technology of blockchain has been proving its potential in decentralized finance and other sectors. There are no doubts that blockchain can simplify identification, registration, authentication, and secure and validate transactions while maintaining anonymity and transparency. Although there are many beneficial features of blockchain, there are still critical challenges of blockchain:

- Election Integrity: a center issue of e-voting frameworks
- Consensus mechanism: Since trade and transactions of any sort of cryptocurrency are illegal in Nepal, it is almost impossible to use native coins of public blockchain which is required to complete the transactions using PoW and PoS consensus.
- Scalability: Public blockchain requires many nodes to mine the blocks and validate them, also it consumes an enormous amount of energy and computing resources.

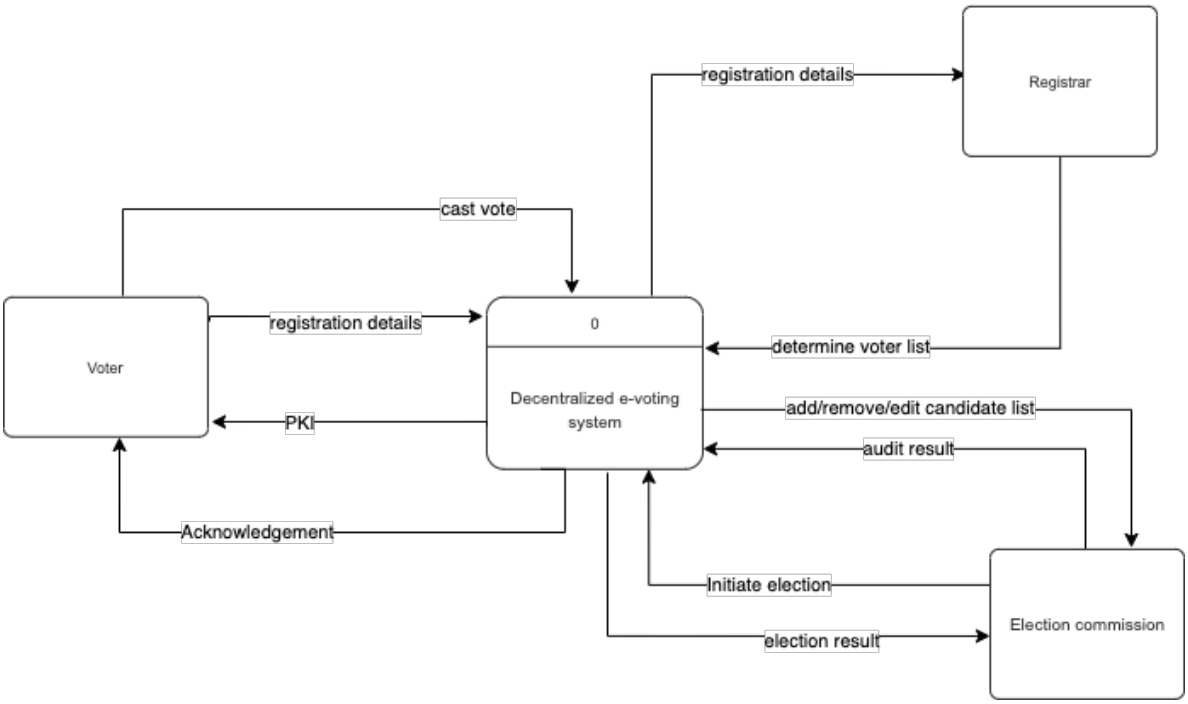
The proposed approach is designed to address these challenges, the development of DApp and smart contracts in private blockchain can eliminate the need for consensus. The private blockchain like Hyperledger Fabric features plug-and-play of components like consensus and membership services.

4.2 The proposal of implementation of blockchain-based e-voting in Nepal

The idea proposes a decentralized e-voting application built on Hyperledger Fabric permissioned blockchain network which eliminates the use of PoW and PoS consensus mechanism since all the nodes in the network are known to each other. This feature of Hyperledger fabric will overcome the issue that may arise with gas fees or transaction costs. The permissioned blockchain can manage different roles and control access to the system. The decentralized application consists of smart contracts to automate the transaction processes and

generate the same result on the execution of an action and store the digital ballot with cryptographic hash on a block. The smart contract will regulate and process the transactions. The system will allow voters to vote anonymously only one time i.e., once a voter has cast a ballot his status change to vote hence not allowing the same voter to vote multiple times.

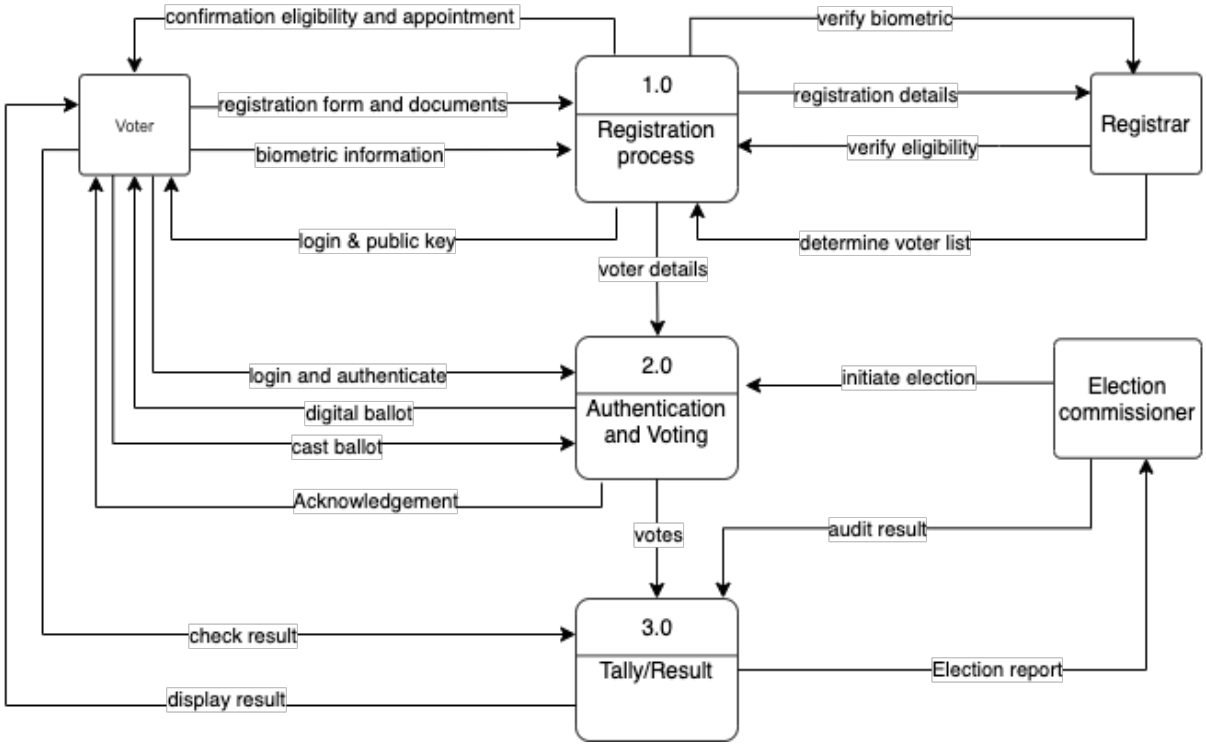
Figure 5: System architecture of the blockchain based e-voting system
(Author)



The proposed system will consist of three processes:

1. Voter registration process
2. Authentication and voting process
3. Votes tally and Publish results

Figure 6: Level 1 Data flow diagram of blockchain based e-voting system
(Author)



For the implementation of blockchain technology in the voting system of Nepal many efforts need to be carried out by the government and the citizens. Primarily, the government will need to build IT infrastructure and work with in-house developers or work closely with external organizations capable of building and maintaining such blockchain systems. Investment should be made in additional computational power. Alongside, awareness and hands-on experiences must be provided to citizens with low IT literacy.

Secondly, the voters will need to register themselves to the new system using biometric verification. This verification and authentication method will avoid the fraud and risks related to one person voting for someone else.

4.2.1 Voter registration process

The first process of the system is the voter registration process. It processes the eligibility verification and identity verification of the voter. This avoids misuse of someone else's identity for hacking and fraud purposes. The roles and identity for all the stakeholders and their authentication, validation, signing, and issuance will be configured in the blockchain system.

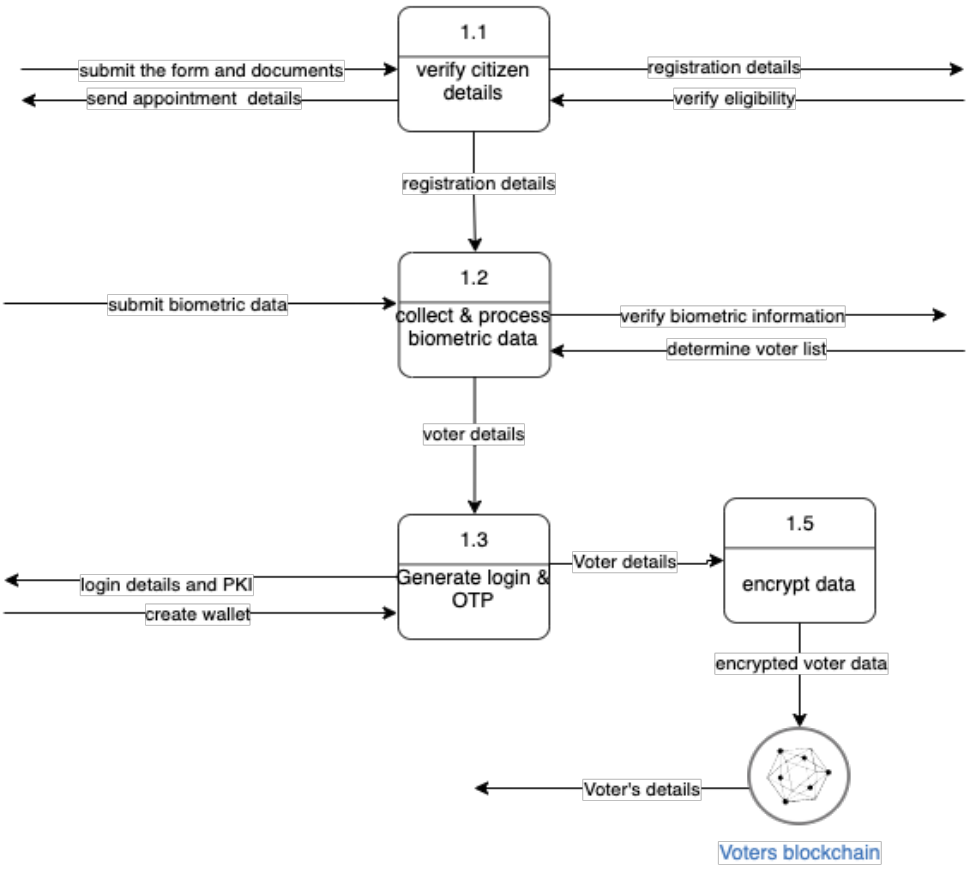
A voter blockchain is utilized during this procedure to keep track of all transactions that occur at each stage of the process for each voter. This proposal encourages one-voter-one-vote. The system will not process anything else than this.

The registration process is as follow:

1. The user would visit the web portal of the election commission or branch of the electoral commission delegated by the election commission to do such a job. Users will have to fill and submit the registration form which includes name, permanent address, date of birth, citizenship number, father's name, mother's name, and optionally email address and phone number. Alongside a copy of the citizenship of the applicant and his parents should also be attached to the form.
2. Once the voting eligibility of the citizen is verified, an appointment is given to the user to submit the biometric data like fingerprint and facial recognition to the related local government body like ward or embassy delegated by the Election Commission to complete the registration process.
3. After successful registration users will receive an OTP (One-Time Password) in their phone or email or via postal services.
4. The user would sign into the election portal by using ID number and OTP. Once signed in, the system will generate a private key (SHA-256) and a public key (SHA-256).
5. The user would be redirected to set up a wallet using the public key and set up MFA (multi-factor authentication) using biometric data.

The below diagram shows the decomposition of Process 1.0 "Registration Process".

Figure 7: Level 2 data flow diagram of voter registration and verification process (Author)



4.2.2 Authentication and voting process

Once the voting is opened, the voter either visits the web portal from a smartphone or PC or the physical polling terminal depending on their convenience. This hybrid approach can encourage voters who do not have the required infrastructure and can even be used in times of disaster.

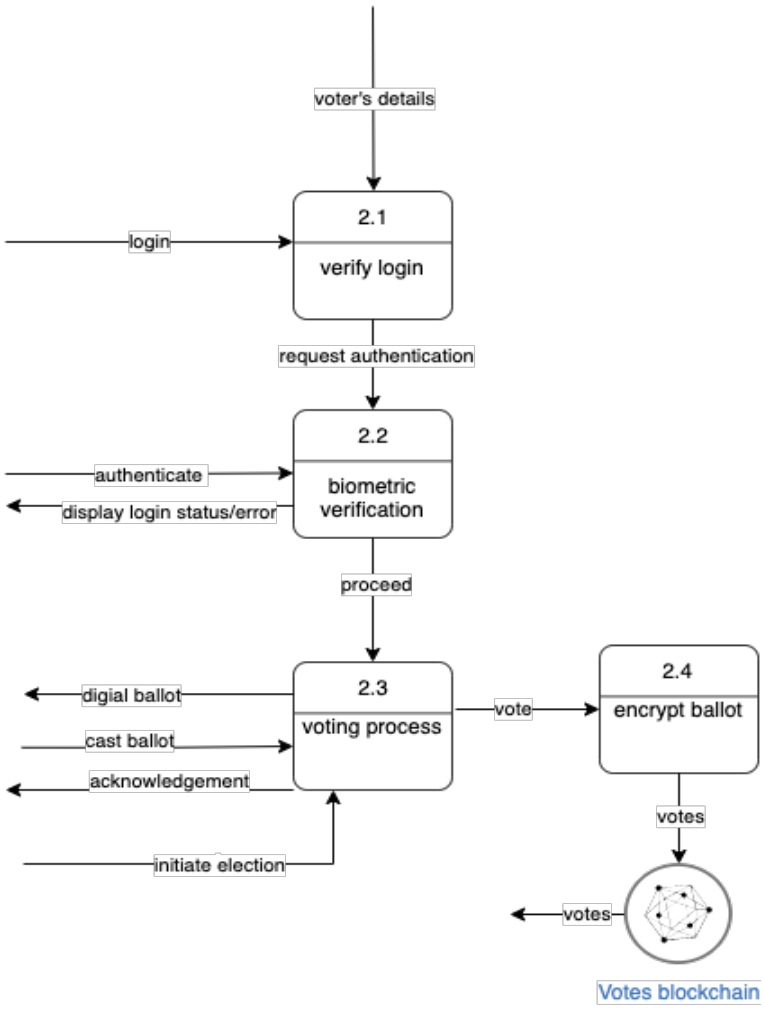
The voting process is as follow:

1. Once the election is opened, the user will open the dApp/web browser from a smartphone or PC with an internet connection or terminals at the polling station.
2. Upon successful authentication, the wallet connects to the dApp and determines if the user has voted or not by checking the votes database.
3. If the user has already voted, then the system would prompt notice to the voter and disconnects the session. If the user has not voted, then the system-generated digital ballot built on a smart contract is prompted to the voter. The digital ballot contains a unique ID, a list of the candidates, and their public keys (depending on the voter's constituent), The smart contract ensures that the voter will get only one digital ballot and can sign only one transaction.
4. Users should select the preferred candidate and the candidate's public key and the voter's public key is filled automatically.
5. The user will then execute the transaction by confirming the action and authenticating the digital ballot with the private key and registered MFA.
6. The successfully signed ballot is then added to the block and a copy is sent to all the nodes in the chain.
7. Once the transaction is complete, the user will be prompted with a system-generated message "You have successfully cast a vote, disconnecting the session.", a wallet will be disconnected from the session.

Once the vote has been confirmed the application will then generate a transaction to remove the user's vote within the voter blockchain. It is important to note that two distinct blockchains are being held; one which contains transactions relating to which users have registered and which users still have a digital ballot, the second containing the contents of the vote (such as what party was voted for.). Using these two distinct blockchains we ensure voter anonymity when selecting their vote.

The below diagram shows the decomposition of Process 2.0 "Authentication and Voting process".

Figure 8: Level 2 data flow diagram of voter's login, authentication, and voting process (Author)

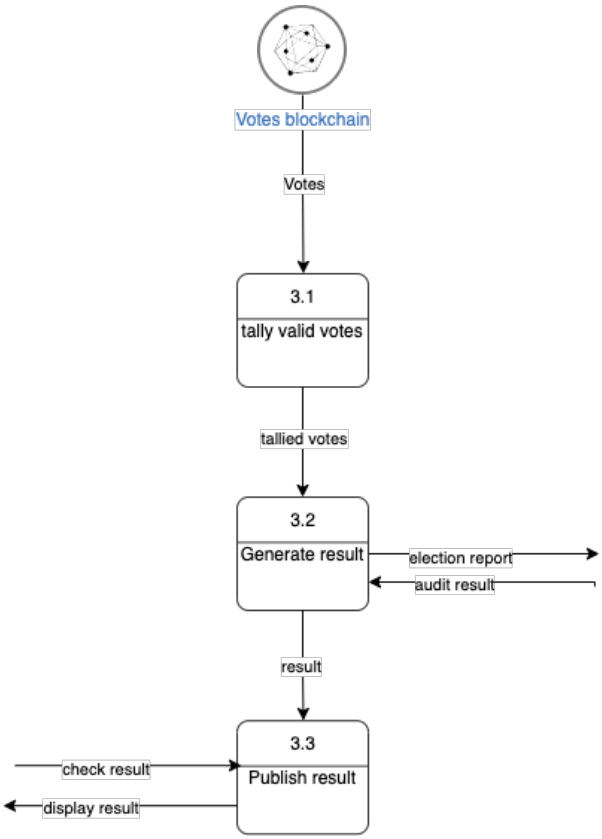


4.2.3 Votes tally and Publish results

After the voting period has ended, the system checks the valid number of the digital ballot and generates a tally from the highest-level blockchain. The report is published on the webpage of the election commission where all the stakeholders can check and analyze the transactions. Furthermore, the ballots are also sent to the jurisdiction/election commissioner for post auditing.

The below diagram shows the decomposition of Process 3.0 "Tally and result process".

Figure 9: Level 2 data flow diagram of vote tally and result
(Author)



4.2.4 CATWOE list for implementation of blockchain-based e-voting in Nepal

CATWOE analysis was formulated by Peter Checkland as part of his soft system methodology. This is an idea of who is involved in an organization or project. The purpose of the analysis is to identify business goals, problem areas, and stakeholders. The analysis consists of six constraints: Clients, Actors, Transformation, Worldwide, Owner, and Environment.

- Clients:

  1. Citizens of Nepal:

     The citizens of Nepal will be using the BEV system to cast votes for their preferred candidate or political party.

- Actors:

  1. Election Commission of Nepal:

     The election commission of Nepal is responsible for implementing the system and initiating pilot projects, training, and awareness.

  2. Registrar:

     The registrar is responsible for the verification of voter eligibility and determining the voter's list.

3. Software engineers:

Software engineers are responsible for the development of the BEV system and maintaining the system throughout its life cycle.

- Transformation:

1. Decentralized electronic voting system:

The system will replace the existing traditional paper ballot voting system with a decentralized electronic voting system.

2. Secure voter registration with biometric data:

To complete the registration of the voter, the voter needs to submit valid documents and provide biometric data for authentication while casting a ballot which discourages misuse of identity fraud especially in cases of remote voting.

3. Paperless ballots:

The traditional paper ballots will be replaced by digital ballots integrated with smart contracts.

4. Tamper proof remote voting system:

The properties of blockchain technology, decentralized application, and the smart contract will prevent the system from data tampering and discourage hacking.

5. Fast, accurate and efficient vote counting:

The BEV system will eliminate the need for manual vote counting which avoids the possible human error while saving a lot of time and money.

6. Discourage vote manipulation:

Once the vote has been cast, the system will store the transaction data in a block while maintaining the anonymity of the voter making it almost impossible to manipulate.

7. Increase public participation:

The remote voting features of e-voting will encourage physically disabled voters and citizens living abroad to cast a vote without visiting the polling station.

- Worldwide:

1. E-voting exists for the voter to vote remotely and anonymously from the comfort of their house without having to wait long hours in a queue in a polling station.

2. Nepal can be a role model for other developing countries by implementing blockchain in e-voting.

3. Lead the possibility to implement blockchain in other sectors of government.

4. Very essential for handicapped people and people living abroad.

- Owner:
  1. Election Commission, Nepal
  2. Government of Nepal

- Environment:
  1. Lack of IT infrastructure:

     The lack of IT infrastructure plays a vital role in the implementation and operation of the BEV system especially in the rural areas of Nepal which lack good internet connectivity.

  2. Compliance with rules and regulations defined by the Nepalese constitution:

     The development of such systems should follow the rules and regulations defined by the Nepalese constitution to avoid possible conflicts.

  3. Lack of e-readiness

     The lack of e-readiness affects the voting process and may discourage public participation. However, this can be tackled with appropriate training and awareness campaigns.

  4. Low energy price of electricity:

     The low cost of hydroelectricity in Nepal benefits the establishment of the BEV system and makes it cost-efficient.

  5. Bribery and misuse of authority can possess a threat in an election:

     The integrity of people is a key part of any system. The affects the operation and outcome of the whole system.

4.2.5 Use case diagram of the proposed approach

The use case diagram is used to describe the high-level functions and scope of the system.

Figure 10: Use case diagram of blockchain based e-voting system

4.2.6 Cost analysis of the proposed framework

One of the main reasons for implementing a blockchain based e-voting system is to make the electoral system more cost-efficient and transparent than the costly traditional electoral system. In this section, the cost of the system is analyzed based on the cloud-based on-demand services provided by Amazon Web Services compared to the cost of a traditional election. This aims to overcome the issues related to the infrastructure required for implementing the proposed system.

The cost of development of such application and infrastructure depends on the choices of the Election Commission. In-house software developers can be hired//employed to develop the application, and a certain amount of election budget can be invested in computing resources. This approach can be extremely costly depending on various factors like wages/salary of engineers and price of resources for computing. Nevertheless, the polling station should also be provided with multiple terminals and a high-speed internet connection.

Another approach is to use the in-house developers and use cloud-based solutions like Amazon Web Services, Microsoft Azure, or Google cloud services. Below is an overview of the cost of using amazon web services' blockchain cloud service.

Table 5: Instances type for Amazon Managed Blockchain
(Amazon Web Services Inc. 2021)

Instance	vCPUs	Memory (GiB)
bc.c5.4xlarge	16	32.0
bc.c5.2xlarge	8	16.0
bc.t3.small	2.0	2.0

Table 6: Amazon managed blockchain for Hyperledger Fabric pricing
(Amazon Web Services Inc. 2021)

Instance	Peer-node price per hour (approx.)	Peer-node storage rate per GB-month	Data Written price/GB
bc.c5.4xlarge	$1.260	$0.12	$0.11
bc.c5.2xlarge	$0.627	$0.12	$0.11
bc.t3.small	$0.044	$0.12	$0.11

Here, let us assume that we use to create 165 AWS standard membership account including 10 instances of bc.c5.4xlarge peer-node per constituency, and each peer-node storage size contains 500 GB.

Cost breakdown:

- **Type of instance**: bc.c5.4xlarge
- **Total number of constituencies:** 165
- **Number of members:** 165
- **Total production time:** 1 month (720 hours)
- **Standard membership cost per hour:** $0.63
- **Price of 1 peer node for 1 hour:** $0.627 per hour
- **Required number of peer-nodes**: (165 constituencies) * (10 peer-nodes per constituencies) = 1650
- **Total amount of peer-node storage required:** total number of peer-node required * 500 GB = 825 TB
- **Cost of storage per month** = total storage * price per month = 825,000 * $0.12 = $99,000 per month
- **Cost of data written:** $0.11 per GB

The hourly cost for the network is:
Network member cost: $0.63*165 = $103.95 per hour
Peer node cost: (1650 peer nodes) * ($0.627/hour) = $1,034 per hour
Peer node storage cost: ($99,000 per month) / (730 hours in a month) = $135.12 per hour
Total cost of data written: (165 members) x (1GB per hour) x (0.11 per GB) = $18.15 per hour
Total cost per production hour = $1,291.22
Production cost for 1 month = production cost per hour * 720 = $929,678.4

Table 7: Cost analysis of the proposed system
(Author)

Production cost per month	$1M
Software development cost	$5M
Application support and maintenance cost	$5M
Polling station and setup cost	$10M
Voter registration cost	$10M
Training and awareness campaign cost	$10M
TOTAL	$41M

Compared to the estimated cost of the next election in Nepal, which is expected to be approximately $200M, the cost of the proposed system is approximately $41M. This saves the cost by almost 80% assuming the election system uptime of 1 month.

5 Results and Discussion

5.1 Analysis of the proposed system

The system is designed keeping in mind the laws and regulations related to the use of cryptocurrencies. The proposed recommendation of the development of the system in a Hyperledger Fabric's permissioned blockchain network integrated with smart contracts for casting and recording votes eliminates the need for gas fees required for the transaction.

However, before deploying such crucial application pilot projects should be carried out to perform checks with load balancing and available network capacity. Depending on the result of the pilot project, if the network is unable to handle huge network traffic

Implementation of blockchain based e-voting in Nepal will have a huge positive impact on the quality and accuracy of the election while maintaining the anonymity of voters. This will overcome the issues with voting fraud such as changing of ballots or counting of unregistered voters.

5.1.1 SWOT analysis of the adoption of blockchain-based e-voting of Nepal

The SWOT analysis is used for evaluating the proposed blockchain based e-voting application. Strengths and weaknesses are internal, coming from the application features and characteristics. Whereas opportunities and threats are external referring to factors like market, competitors, legislation, technological developments, and so on.

Table 8: SWOT analysis

Strengths	**Weaknesses**
- Fast and efficient voting - The rapid vote count and tallying - Accurate results - Automation (by using smart contracts) - Increased participation due to remote voting - Transparency - No data tampering - Long-term cost savings	- Still in the early/conceptual stage - Scalability - Infrastructure and environmental requirements - Lack of knowledge - Remote voting in an uncontrolled environment increases the risk of fraud, coercion, family voting, and impersonation, as well as a breach of ballot secrecy.
Opportunities	**Threats**
- Increased convenience for voters - More focused on technology innovation - No transportation cost is required for transferring paper ballots - Building trust between government and public	- Fraud through manipulation by a small group of insiders is a possibility. - Security requirements for keep the credentials safe - Prone to hacking and attacks - Due to reliance on technology, the election committee's level of control is reduced.

5.2 Comparison with related frameworks

In recent times, electronic voting has been applied in several states and governments level elections, although most of them are small-scale. Sharing the same vision for blockchain technology and its application in e-government and other sectors, many organizations are collaborating to create and develop a decentralized voting sector. Several research and literature that has been published portraying different ideas of decentralized electronic voting system are either based on the public blockchain network which is not suitable in the case of Nepal due to restrictions in the use of cryptocurrencies or has scalability and performance issues. Due to these persistent problems of scalability in the current decentralized voting system, it is less suitable to implement at the national level.

The below table shows the availability of the various blockchain-based electronic voting system.

Table 9: Availability of current blockchain-based electoral systems

(Jafar, Aziz, Shukur 2021)

Online voting platforms	Framework	Language	Cryptographic Algorithm	Consensus Protocol
Follow My Vote	Bitcoin	C++/Phython	ECC	PoW
Voatz	Hyperledger Fabric	Go/Javascript	AES/GCM	PBFT
Polyas	Private/Local Blockchain	NP	ECC	PET
Luxoft	Hyperledger Fabric	Go/JavaScript	EC/ElGamal	PBFT
Polys	Ethereum	Solidity	Shamir's Secret Sharing	PoW
Agora	Bitcoin	Phython	ElGamal	BFT-r

5.2.1 Follow My Vote

Follow My Vote has developed the world's first verifiable end-to-end online voting platform for use in government-sponsored elections around the world based on Bitcoin's proof-of-work consensus mechanism. The end-to-end online voting platform allows voters to track their votes in the ballot box and ensure that the votes were taken as intended and counted as votes. It also provides transparency to voters throughout the ballot box and ensures that the reported election results are truly correct. Elliptic Curve Cryptography technology keeps the voting process secure while protecting the rights of all voters to the privacy of the system. Their goal is to open the black box where elections are taking place today by allowing each voter to count votes to ensure the legitimacy of the election and to ensure that the votes were counted correctly (Follow My Vote 2021).

5.2.2 Voatz

Voatz is a smartphone-based voting platform built on the Hyperledger Fabric framework utilizing the practical Byzantine Fault Tolerance (pBFT) consensus protocol. The application requires voters to complete the verification process by pairing the voter identity to the voter's smartphone or biometrics or PIN. After successfully casting the mobile ballot, the voter will receive an anonymized receipt to verify their selections. The respective jurisdiction will use the exact receipt for a post-election audit (Voatz 2020).

5.2.3 Polyas

Founded in Finland in 1996. The company uses blockchain technology to provide electronic voting systems for the public and private sectors. In 2016, Polyas was certified as secure enough by the Federal Office for Information Security for electronic voting applications. Many major companies across Germany use Polyas to operate their electronic voting systems.

5.2.4 Agora

Agora is the group that launched the blockchain digital voting platform. Founded in 2015, it was partially held in the March 2018 presidential election in Sierra Leone. Agora's architecture is built on several innovations, including custom blockchain, unique participatory security, and Byzantine fault consensus mechanisms. It encourages citizens and elected groups working as electoral writers around the world to work to ensure that the election process is safe and transparent. Voice is a universal token of the Agora ecosystem (Agora 2018).

Table 10: Scalability analysis of top blockchain platforms
(Jafar, Aziz, Shukur 2021)

Framework	Generation Time	Hash Rate	Transactions Per Sec	Cryptographic Algorithm	Mining Difficulty	Power Consumption	Reward	Scalability
Bitcoin	9.7 min	899.624 Th/s	4.6 max 7	ECDSA	High	Very High	25 BTC	Very Low
Ethereum	10 to 19s	168.59 TH/s	15	ECDSA	High	High	5 Ether	Low
Hyperledger Fabric	10 ms	N.A.	3500	ECC	No mining required	Very Low	N.A.	Very Good
Litecoin	2.5 min	1.307 Th/s	56	Scrypt	Low	Moderate	25 LTC	Average
Ripple	3.5 s	NA	1500	RPCA	No mining required	Very low	Base fee	Good
Dogecoin	1 min	1.4 TH/s	33	Scrypt	Low	Low	10,000 Doge	Low
Peercoin	10 min	1.4 TH/s	8	Hybrid	Moderate	Low	67.12 PPC	Low

Based on the comparison of various frameworks, Hyperledger Fabric’s frameworks are the most feasible compared to the rest of the frameworks. The Hyperledger Fabric can process up to 3500 transactions per second with a block generation time of 10ms. Hyperledger fabric operates in a permissioned mode and fine-grained access control which results in solving scalability, performance, and privacy-related issues. Moreover, it is very energy and cost-efficient since it does not require mining to validate a block. Hence, also eliminating the need for gas fees required for performing transactions.

5.3 Limitation for implementation

Blockchain technology will eliminate several problems related to electronic voting whilst making it cost-efficient, convenient, and secure than other networks. However, several research has identified certain challenges such as:

1. Scalability

Scalability is one of the major drawbacks of blockchain when implemented in a large-scale election, the pilot projects should test the capacity of the system and allocate resources accordingly. This is where the on-demand cloud service of AWS comes in handy.

2. Voter Verification

The identification verification of voters plays a vital role in the operation of the whole system. Hence, the offices delegated for the voter registration should perform identity verification with full integrity.

3. Transactional Privacy

One of the features of the blockchain is that the transactions are transparent. The user's identity can be determined by examining and analyzing the transactions. The features of permissioned blockchain can eliminate such issues if the roles of the members and nodes are configured properly.

4. Acceptableness

People should be aware and ready to accept the decentralized electoral system as people's confidence and integrity can only maintain the integrity of the system itself. Although blockchain is not a commonly understood technology and neither is the idea of online voting for many people, those without knowledge of technology may take a step back for accepting such a system. The government should primarily focus on public awareness and increase the e-literacy rate before implementing the decentralized electoral system.

5. Political Leader's Resistance

Political leaders who have been benefitted from the existing election system are more likely the denial the technology. They will discourage the system and promote negligence among their followers.

6 Conclusion

The main objective of the thesis was to examine a possible application of a blockchain based electronic voting system in Nepal. The current state of e-government and blockchain in Nepal was analyzed based on the review of existing literature related to the field. Additionally, several examples of successful implementation of blockchain in various countries were reviewed to illustrate the core concept of blockchain and its application in e-government and create a proposal for the implementation of a decentralized e-voting system in Nepal.

In the practical part, a feasible approach to implement a blockchain-based electoral system in Nepal was proposed. A system of proceeding with permissioned blockchain was proposed and described. Processes involved in the proposed system has been defined using data flow diagrams and use case diagram. Moreover, a cost analysis was also performed based on the available pricing of on-demand cloud services and other factors.

Nevertheless, due to limitations such as the low literacy rate, e-readiness, and lack of infrastructure, the government should focus on improving IT infrastructure, uplift e-government services by initiating public awareness programs in rural areas of Nepal. Alongside, pilot projects should be performed to check the capacity handling of the system and public participation. Depending on the result, a specific date and time could be set for each constituency. It can also be suggested to deploy this system for Nepalese migrants as a part of the pilot project.

By implementing the principles of blockchain technology in the electoral system it can transform the traditional election system into a digital system and make it very cost-efficient. This kind of system inspires transparency in government, discourage bribery and fraud, and privacy of citizens, secure transactions, and run robust and cost-efficient digital administration facilitating the citizen of the nation. In the case of Nepal, where almost 10% of people live abroad for study and foreign employment purposes, this system encourages the participation of Nepalese migrants.

Furthermore, in future work, a practical application will be developed and various tests including transaction time, system load capacity, scalability, efficiency, etc. will be performed.

References

(HEDGETRADE), Mary Thibodeau, 2019. No Title. [online]. 2019. Available from: https://hedgetrade.com/3-types-of-blockchain-explained/

AGORA, 2018. Bringing voting systems into the digital age. [online]. 2018. Available from: https://www.agora.vote

ALISON MCGUIRE, 2018. GLOBAL BLOCKCHAIN ADOPTION: WHICH COUNTRIES ARE LEADING THE CHARGE? [online]. 2018. Available from: https://irishtechnews.ie/global-blockchain-adoption-which-countries-are-leading-the-charge/

AMAZON WEB SERVICES INC., 2021. Amazon Managed Blockchain pricing. . 2021.

ASTE, Tomaso, TASCA, Paolo and MATTEO, T Di, 2017. Blockchain Technologies : foreseeable impact on industry and society Draft NOT for distribution , to be published on IEEE 2017. *Computer* [online]. 2017. Vol. 50, no. 9, p. 18–28. Available from: http://discovery.ucl.ac.uk/10043048/1/Aste_BlockchainIEEE_600W_v3.3_A.doccceptedVersion.x.pdf

BAARS, Henning and KEMPER, Hans-Georg, 2015. Integration von Big Data-Komponenten in die Business Intelligence. *Controlling* [online]. 2015. Vol. 27, no. 4–5, p. 222–228. DOI 10.15358/0935-0381-2015-4-5-222. Available from: http://elibrary.vahlen.de/index.php?doi=10.15358/0935-0381-2015-4-5-222

BANK, World, 2013. E-government. [online]. 2013. Available from: https://www.worldbank.org/en/webarchives/archive?url=httpzzxxweb.worldbank.org/archive/website01358/WEB/0__MENUP.HTM&mdk=23350751

BENBYA, Hind and MCKELVEY, Bill, 2006. Using Coevolutionary and Complexity Theories to Improve IS Alignment: A multi–Level Approach. *Journal of Information Technology* [online]. 1 December 2006. Vol. 21, no. 4, p. 284–298. DOI 10.1057/palgrave.jit.2000080. Available from: https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf

BITFURY, 2017. *Public vs Private blockchain* [online]. Available from: https://bitfury.com/content/downloads/public-vs-private-pt1-1.pdf

CAI, Wei, WANG, Zehua, ERNST, Jason B., HONG, Zhen, FENG, Chen and LEUNG, Victor C. M., 2018. Decentralized Applications: The Blockchain-Empowered Software System. *IEEE Access* [online]. 2018. Vol. 6, p. 53019–53033. DOI 10.1109/ACCESS.2018.2870644. Available from: https://ieeexplore.ieee.org/document/8466786/

CARDANO, 2020. Proof-Of-Stake And Proof-Of-Work. [online]. 2020. Available from: https://cardano.org/ouroboros/

DIALLO, Nour, SHI, Weidong, XU, Lei, GAO, Zhimin, CHEN, Lin, LU, Yang, SHAH, Nolan, CARRANCO, Larry, LE, Ton Chanh, SUREZ, Abraham Bez and TURNER, Glenn,

2018. EGov-DAO: A Better Government using Blockchain based Decentralized Autonomous Organization. *2018 5th International Conference on eDemocracy and eGovernment, ICEDEG 2018*. 2018. No. October, p. 166–171. DOI 10.1109/ICEDEG.2018.8372356.

ELECTION COMMISSION OF NEPAL, 2017. *General election report 2017* [online]. Available from: https://result.election.gov.np

ETHEREUM, 2021. Introduction to Dapps. [online]. 2021. Available from: https://ethereum.org/en/developers/docs/dapps/

FOLLOW MY VOTE, Inc., 2021. Online Voting Platform. [online]. 2021. Available from: https://followmyvote.com/online-voting-platform-benefits/

GARDINER HARRIS, 2013. Vote Fraud Is Claimed by Maoists in Nepal. [online]. 2013. Available from: https://www.nytimes.com/2013/11/22/world/asia/nepals-maoists-losing-vote-charge-election-fraud.html

GOVERNMENT, Seoul Metropolitan, 2009. Kathmandu Metropolitan City Feasibility Study Final Report. . 2009.

HILL, MARGOT, WALLNER, ASTRID and FURTADO, JOSE, 2010. Reducing vulnerability to climate change in the Swiss Alps: a study of adaptive planning. *Climate Policy* [online]. January 2010. Vol. 10, no. 1, p. 70–86. DOI 10.3763/cpol.2008.0536. Available from: http://www.tandfonline.com/doi/abs/10.3763/cpol.2008.0536

HOWARD, Mark, 2001. e-Government Across the Globe: How Will" e" Change Government? *Government finance review* [online]. 2001. P. 6–9. Available from: https://www.gfoa.org/downloads/eGovGFRAug01.pdf

JAFAR, Uzma, AZIZ, Mohd Juzaiddin Ab and SHUKUR, Zarina, 2021. Blockchain for electronic voting system—review and open research challenges. *Sensors*. 2021. Vol. 21, no. 17. DOI 10.3390/s21175874.

KSHETRI, Nir and VOAS, Jeffrey, 2018. Blockchain-Enabled E-voting By: Nir Kshetri and Jeffrey Voas Kshetri, Nir and Voas, J. (2018)." Blockchain-Enabled E-voting ", IEEE. *Cryptology ePrint Archive* [online]. 2018. Vol. 35, no. i, p. 95–99. Available from: https://eprint.iacr.org/2018/642.pdf%0Ahttps://doi.org/10.1016/j.procs.2018.03.063%0Ahttp://dx.doi.org/10.1016/B978-0-12-802117-0.00022-9

METACO, 2020. Can permissioned and permissionless blockchains co-exist? . 2020.

NDOU, Valentina Dardha, 2004. E - Government for Developing Countries: Opportunities and Challenges. *The Electronic Journal of Information Systems in Developing Countries*. 2004. Vol. 18, no. 1, p. 1–24. DOI 10.1002/j.1681-4835.2004.tb00117.x.

NEPAL, Government of, 2020. No Title. . 2020.

NEW AMERICA, 2020. Georgia land titling system. *New America Blog* [online]. 2020. Available from: https://www.newamerica.org/digital-impact-governance-initiative/digital-impact-and-governance-initiative-projects/digi-blogs/project-capsule-georgia-land-titling-

system/

SHANG, Qiuyun and PRICE, Allison, 2019. A Blockchain-Based Land Titling Project in the Republic of Georgia: Rebuilding Public Trust and Lessons for Future Pilot Projects. *Innovations: Technology, Governance, Globalization* [online]. January 2019. Vol. 12, no. 3–4, p. 72–78. DOI 10.1162/inov_a_00276. Available from: https://direct.mit.edu/itgg/article/12/3-4/72-78/9852

SHARMA, Gajendra, 2020. Digital Governance in Nepal. *Journal of Management Research*. 2020. Vol. 12, no. 3, p. 41. DOI 10.5296/jmr.v12i3.17061.

SPIELMAN, Avi and SUPERVISOR, Thesis, 2016. Blockchain: Digitally Rebuilding the Real Estate Industry. . 2016. P. 1–78.

TARASOV, Pavel and TEWARI, Hitesh, 2017. THE FUTURE OF E-VOTING. . 2017. Vol. 12, no. 2, p. 148–165.

TERZI, Sofia, VOTIS, Konstantinos, TZOVARAS, Dimitrios, STAMELOS, Ioannis and COOPER, Kelly, 2019. Blockchain 3.0 Smart Contracts in E-Government 3.0 Applications. [online]. 11 October 2019. Available from: http://arxiv.org/abs/1910.06092

THE ANNAPURNA EXPRESS, 2021. Rs 100 billion: The cost of Nepal's next parliamentary election. . 2021.

UNITED NATIONS, 2020. *E-government Development Index* [online]. Available from: https://publicadministration.un.org/egovkb/Data-Center

VOATZ, Inc, 2020. How does Voatz work? [online]. 2020. Available from: https://voatz.com/how-it-works/

ZHENG, Zibin, XIE, Shaoan, DAI, Hong-Ning, CHEN, Xiangping and WANG, Huaimin, 2017. Blockchain Challenges and Opportunities : A Survey Shaoan Xie Hong-Ning Dai Huaimin Wang. *International Journal of Web and Grid Services* [online]. 2017. Vol. 14, no. 4, p. 1–24. DOI 10125/41338. Available from: http://inpluslab.sysu.edu.cn/files/blockchain/blockchain.pdf

КАМЕРНИЦКИЙ, АВ and ЛЕВИНА, ИС, 2005. Прегна-D'-Пентараны-Прогестины И Антипрогестины I. Разделение Биологических Функций Стероидных Гормонов. *Биоорганическая Химия* [online]. 2005. Vol. 31, no. 2, p. 115–129. Available from: http://elibrary.ru/item.asp?id=9174603