A Report

on

E-Voting System using Blockchain

Submitted in partial fulfillment of the

requirement for the award of the degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

Under The Supervision of

Dr. Vishwadeepak Singh Baghela

(Professor)

Submitted By

SHUBHAM KUMAR (18SCSE1010683)/

(18021011906)

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING / DEPARTMENT OF COMPUTERAPPLICATION

GALGOTIAS UNIVERSITY, GREATER NOIDA

INDIA

Dec,2021

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING

GALGOTIAS UNIVERSITY, GREATER NOIDA

CANDIDATE'S DECLARATION

I hereby certify that the work which is being presented in the thesis/project/dissertation, entitled **"E-VOTING SYSTEM USING BLOCKCHAIN"** in partial fulfillment of the requirements for the award of the BACHELOR OF TECHNOLOGY in COMPUTER SCIENCE AND ENGINEERING submitted in the School of Computing Science and Engineering of Galgotias University, Greater Noida, is an original work carried out during the period of month, Year to Month and Year, under the supervision of **Dr. Vishwadeepak Singh Baghela (**Professor**)**, Department of Computer Science and Engineering/Computer Application and Information and Science, of School of Computing Science and Engineering , Galgotias University, Greater Noida

The matter presented in the thesis/project/dissertation has not been submitted by me/us for the award of any other degree of this or any other places.

SHUBHAM KUMAR

(18SCSE1010683)

This is to certify that the above statement made by the candidates is correct to the best of my knowledge.

Supervisor Name

Designation

CERTIFICATE

The Final Thesis/Project/ Dissertation Viva-Voce examination of SHUBHAM KUMAR (18SCSE1010683) has been held on _____ and his/her work is recommended for the award of BACHELOR OF TECHNOLOGY in COMPUTER SCIENCE AND ENGINEERING**.**

Signature of Examiner(s) **Signature of Supervisor(s)**

Signature of Project Coordinator **Signature of Dean**

Date: December, 2021

Place: Greater Noida

Abstract

The main problem is that with the current voting system is less secured. The current system takes much time sometimes it takes months. And also some of the voters are left to vote. A lot of issues can also be encountered in our country, like ILLETRACY, lack of knowledge about the internet and the computer. And one more challenge we will may face is the lack of computer and smart phone devices.

In this paper I tried to implement the E-voting System using the Blockchain technology. The Blockchain technology compromises of the properties such as transparency, decentralization, irreversibility, nonrepudiation, etc.,

Blockchain is not only a basic technology that has great interest in itself, but also has great potential when integrated into many other areas. This paper is based on Blockchain technology, we propose an e-voting law, without the presence of a trusted third party company. In addition, we offer a few extensions and improvements that may meet the requirements for certain voting conditions.

Blockchain technology allows The people to verify that their votes are recorded and counted correctly. Any voter may be able to check the counting without the security being hampered. Also there are security concerns in blockchain-based e-voting too, but it is more secured than the traditional voting systems which uses EVMs. In future the EVMs will be placed in the museums for the next generation.

Electronic voting has many advantages over the traditional way of voting. Some of these advantages are lesser cost, faster tabulation of results, greater accuracy, and lower risk of human and mechanical errors.

Table of Contents

List of Table

List of Figures

Acronyms

B.Tech.	Bachelor of Technology
M.Tech.	Master of Technology
BCA	Bachelor of Computer Applications
MCA	Master of Computer Applications
B.Sc. (CS)	Bachelor of Science in Computer Science
M.Sc. (CS)	Master of Science in Computer Science
SCSE	School of Computing Science and Engineering

CHAPTER-1

Introduction

1.1 Introduction

Blockchain has revolutionized the exchange of information and media after the Internet. Blockchain technology is pertained to as a path-breaking innovation and the forerunner of a fresh economic period. Many sectors, like finance, medicine, manufacturing, and education, use blockchain applications to profit from the unique bundle of characteristics of this technology. Blockchain technology (BT) promises benefits in tractability, collaboration, organization, identification, credibility, and transparency. When talking about BT, the distributed ledger technology needs to get mentioned since it is an umbrella term that includes blockchains as one type. A distributed ledger uses independent systems (nodes) to record, share, and synchronize transactions in a decentralized network. A blockchain network works without a centralized server. Transactions made in such a network are verified by the decentralized nodes and stored in so-called blocks with a timestamp. The size limit of blocks can differ between varying blockchains. The blocks are getting linked in chronological order because every one of them (except the first ―genesis‖ block) contains the cryptographic hash of the previous one, so they form a chain. The block hash considers not only structural data of a specific block but also its content like, for example, transactions. It depends on the blockchain whether users can store complete files on-chain or they need to use offchain solutions like a cloud or an Inter Planetary File System (IPFS) due to file sizes. Verification: Once the owner of the coin has broadcasted their transaction into the peer-to-peer network, it must undergo a verification process called ―mining‖ before it can become a part of the public ledger. For efficiency, these transactions are grouped into blocks for verification - hence the name blockchain. Verification is then performed by miners who devote computing power to solving a puzzle. This is the ―proof of work‖ mechanism. Double Spend and Decentralization: Attempts by the owner of a Bitcoin to double spend a coin by issuing two transactions for the same coin are thwarted via the verification process. If a node completes a proof of work puzzle on a block that contains a coin that has already been spent, it will be rejected by the rest of the nodes in the network, and subsequently will not be added to the blockchain. Scalability: Much discussion currently

surrounds Bitcoin's block size limit, which restricts blocks to 1Mb of transaction and header data. As blocks are mined every 10 minutes this limits the number of transactions per second (TPS) to a theoretical limit of 7 TPS [7]. As Blockchain became more popular and more nodes joined the network, the number of transactions increased and this limit became a significant problem. If the transaction creation rate increases too much it could surpass the rate at which transactions are added to the blockchain, creating a backlog of transactions.

1.2 Formulation of Problem

Elections, became the subject of a survey that took place in the last few years in cryptography. Compared to Traditional voting or Paper based voting, E-Voting is very Environmental friendly, there is no COUNTING MISTAKES. Taking about the Time and voting efforts, there is very less effort and will be no wastage of time, some of the peoples are also out of station so they are unable to vote for the welfare of the country so, VOTE RESULTS may be increase with the introduction of the E-Voting system. In another way, E-VOTING is used only in few countries, example, ESTONIA, CANADA, AUSTRALIA. On the other hand, the E-voting is abandoned in some country like GERMANY, due to the security issues and the vulnerability.

Security is the biggest challenge will be faced when we are implementing this E-voting system.

1.2.1 Tool and Technology Used

The main Technology used is Blockchain, python, SQL, bootstrap, HTML,CSS

Literature Survey:

Blockchain has revolutionized the exchange of information and media after the Internet. Blockchain technology is pertained to as a path-breaking innovation and the forerunner of a fresh economic period. Many sectors, like finance, medicine, manufacturing, and education, use blockchain applications to profit from the unique bundle of characteristics of this technology. Blockchain technology (BT) promises benefits in treatability, collaboration, organization, identification, credibility, and transparency.

When talking about BT, the distributed ledger technology needs to get mentioned since it is an umbrella term that includes blockchains as one type . A distributed ledger uses independent systems (nodes) to record, share, and synchronize transactions in a decentralized network.

A blockchain network works without a centralized server. Transactions made in such a network are verified by the decentralized nodes and stored in so-called blocks with a

timestamp . The size limit of blocks can differ between varying blockchains. The blocks are getting linked in chronological order because every one of them (except the first “genesis” block) contains the

cryptographic hash of the previous one, so they form a chain . The block hash considers not only structural data of a specific block but also its content like, for example, transactions.

It depends on the blockchain whether users can store complete files on-chain or they need to use off-chain solutions like a cloud or an Inter Planetary File System (IPFS) due to file sizes.

Voting system

There are many practices which are introduced with various variations which should be done in the existing system to make it more reliable and usable. Some of them guarantee privacy as well security in the system to some extent, but still the voting information and process must be in control as well. And also be managed with advanced programs that will also ensures the safety and confidentiality of voters as well.

The systems that are developed to caste the vote are Programs designed to vote with digital methods using online portals and power devices, uses various encryption strategies to ensure secure data transaction.

Homomorphic Encryption Technique:

Homomorphic encryption has some known powerful strategies with many useful applications. Recently, it is used in an online voting system. The voting system is based on this encryption uses the exponential ElGamal cryptosystem.

Before shipping, the content of each vote is coded using ElGamal encryption for interpreter. In Addition, the homomorphism property of this crypto system does it is possible to combine votes cast directly outside to delete codes.

Centralized architecture

However, strategic numbers are available convert data in encoded format to block it cheating while transferring to a network. One drawback can be discussed here that after the correct one the data is stored in a database trust as well as security is required on a large scale. Placed in one place storage is disrupted when data is honored because Unauthorized access and attacks by hackers will not a system challenge about fidelity.

Verification--

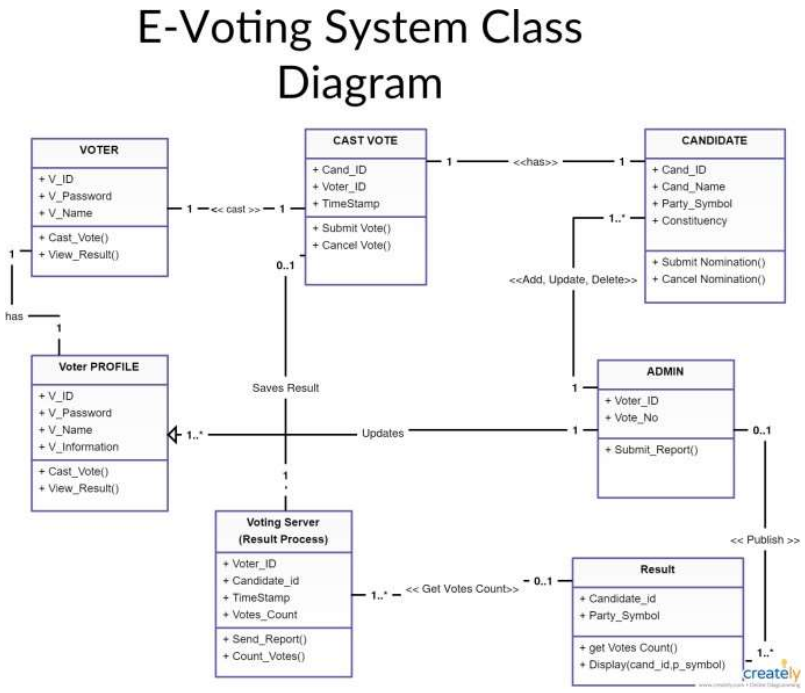
Once the owner of the coin has broadcasted their transaction into the peer-to-peer network, it must undergo a verification process called “mining” before it can become a part of the public ledger. For efficiency, these transactions are grouped into blocks for verification - hence the name blockchain. Verification is then performed by miners who devote computing power to solving a puzzle. This is the “proof of work” mechanism.

Double Spend and Decentralization--

Attempts by the owner of a Bitcoin to double spend a coin by issuing two transactions for the same coin are thwarted via the verification process. If a node completes a proof of work puzzle on a block that contains a coin that has already been spent, it will be rejected by the rest of the nodes in the network, and subsequently will not be added to the blockchain.

Scalability--

Much discussion currently surrounds Bitcoin's block size limit, which restricts blocks to 1Mb of transaction and header data. As blocks are mined every 10 minutes this limits the number of transactions per second (TPS) to a theoretical limit of 7 TPS [7]. As Blockchain became more popular and more nodes joined the network, the number of transactions increased and this limit became a significant problem. If the transaction creation rate increases too much it could surpass the rate at which transactions are added to the blockchain, creating a backlog of transactions.



1. Sample voter's data

S.No.	Name	Address	Mob. No.	Age
1.	Shubham kumar	Koilwar,Bihar	12345	21
2.	Ram	Patna	43222	35
3.	Priya kumari	Ara, Bihar	87687	28
4.	Jeet singh	Ara, Bihar	89644	60

2. Voting location table

S.No.	Voting location	pin code
1.	Old colony, Patna 1, Bihar	543432
2.	Rajeev nagar, ara, Bihar	345678
3.	Char nagar, Koilwar, Bihar	897645

CHAPTER 3

Functionality/ Working of Project

Traditional elections satisfy neither citizens nor political authorities in recent years. They are not fully secure since it is easy to attack votes. It threatens also privacy and transparency of voters. Additionally, it takes too much time to count the votes. This paper proposes a solution using Blockchain to eliminate all disadvantages of conventional elections. Security and data integrity of votes is absolutely provided theoretically. Voter privacy is another requirement that is ensured in the system. Lastly, waiting time for results decreased significantly in proposed Blockchain voting system.

Considering today's technology, blockchain may create one of the most prominent alternative to traditional voting in terms of security, consistency and speed. While designing a chain for voting in a crowded country, the system should be secure. Many aspects should be considered in order to construct a secure blockchain-based election system. First factor is human for such a system. In the solution, human interference is absolutely prohibited. The proposed system will be consisting of nodes (computers in design) that is closed to human interference. Any input that cannot be considered as vote will be ignored in this system. For such a system, stealing votes or changing votes are totally blocked. Second issue is saving system from hackers. In order to manipulate votes, hackers need to enter the system as a citizen at proposed solution. Also, it is guaranteed that a citizen can only vote for one time. When citizen cast a ballot, e-government system will be informed without revealing any information about vote. Then, e-government system marks that person as voted. In a blockchain system, every transaction is related to the previous one. So, changing an accepted transaction is impossible for such a system. Due to the consistency of the blockchain, data will always be consistent and voting will be reliable.

The E-voting system must have the following Characteristics:

• Eligibility and Authentication: The voters who are authorized or verified by the government authorities are only able to vote.

• Uniqueness: One voter is allowed to vote for only one time.

• Accuracy: Every vote should be considered.

• Integrity: No Modification or loss of data should happen that may lead to the failure of the system.

•Reliability: System must be designed in such a way that it can be stable even after failures and loss of internet and can be run no low internet also.

• Convenience: The system should be convenient that will be handled easily with less amount of skillset.

Electronic Ballot

Electronic voting systems should use electronic ballot to store votes in computer memory. The use of electronic ballots will lead to no risk of exhausting the supply of ballots. Additionally, these electronic ballots will remove the need for printing of paper ballots, and also decrease the cost so that it will be more effective.

Cryptographic verification

The concept of electoral validation through cryptographic solutions has emerged in educational manuals to introduce transparency and confidence in electronic voting systems. Allows voters and election observers to ensure that votes are recorded, counted and declared correctly, independently of the hardware and software that runs the election.

Proposed System

Speaking about the feasibility of this system, we mean a cost-effective, scalable, secure, easy to use, and easy-to-deploy system. The blockchain-based solution should be cheaper enough. The traditional elections are the long-term procedure compared to the blockchain based E-voting system, say in a 3-years period with at least 1 election per year.

The blockchain based voting should not be more expensive than non-blockchain solutions. This system should support millions of people, depending on the population of the country, business size or target group population. The security level of the system should be higher than non-blockchain solutions.

Blockchain solutions are suitable, when these characteristics are present in the legacy subject systems:

*Shared data: The information should be structured when shared between the entities.

*Multiple parties: Where there is a need for more than one entity which reads or writes the data.

*Low trust: When there is no full trust between the members of the system.

*No trusted third party: If it is not available or not preferred due to difficulties or costs.

*Auditability: The records should be immutable, not to be changed or deleted after recording.

CHAPTER-4

Result and Discussion

Feasibility Analysis:

By speaking of feasibility, we mean a cost-effective, scalable, secure, and easy-to-deploy system (or subsystem). Any blockchain-based solution should be (noticeably) cheaper than the traditional elections in the long term, say in a 3-years period with at least 1 election per year.

It should not be more expensive than non-blockchain solutions either. The system should support millions of people, depending on the country, business size or target group population. The security level should not be lower than non-blockchain solutions.

Blockchain solutions are suitable, when the following characteristics are present in the legacy subject systems:

Shared data: When there is structured information which should be shared between entities.

Multiple parties: When there is a need for more than one entity which reads or writes the data.

Low trust: When there is no presumed full trust between the members of the system.

No trusted third party: If it is not available or not preferred due to implementation difficulties or costs.

Auditability: If we want the records to be immutable (not to be changed or deleted after recording.

➔Financial Aspects

Undoubtedly, using automated electronic systems, including web portals and mobile applications, will lower the administrative costs in the long term, despite their higher initial investment costs. A previous study showing a rough comparison regarding infrastructure and maintenance costs of traditional and electronic elections was recently made. Per to the study, the advantages of switching to an online elections system may provide savings up to several times per year.

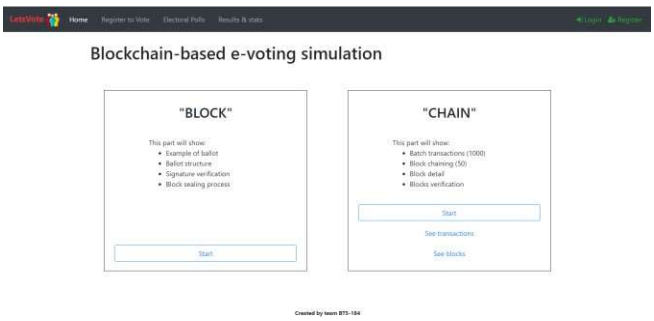
➔ Security and Reliability

The security services that the blockchain provides is compared with other database solutions. The blockchain provides transparency with anonymity. The privacy is not aimed but can be implemented. In blockchain Each block keeps the hash of the previous block and this eventually provides a chain of blocks that are linked to each thus any change in any block leads to the change of the hash of that block and there is a change in whole blockchain. Merkle tree is used in order to keep the integrity of the records.

A. Login Module:

User Login is the first form users connected when the voting page is loaded from the internet. It will have a connection to the database to validate the user credentials. User types are either voters or Administrators. It is assumed that users have used another interface or form to register for voting. In the same login page there will be Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) validation with random numbers. Six digit random numbers will be created each time the page is loaded to be able to stop any kind of computer attacks to the voting site.

1. This is home page

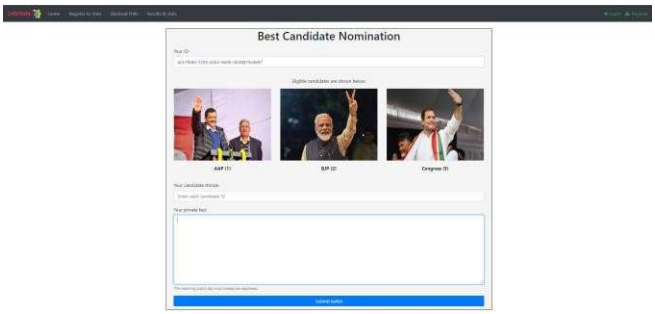


B. Election:

This is automated phase. During the stipulated date and time election is started. Voter can cast their vote within this time period. If anyone wants to cast vote before then he/she will be directed to page that displays correct date and time for the elections to be conducted.

C. Register User:

In this module the user can register to the government's database by entering the details and uploading the documents like (government ids to verify the identity of the user). The application's data base will be accessed by a separate URL.

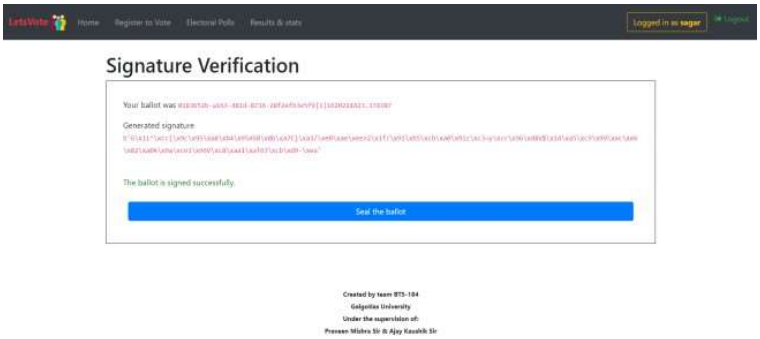


Complete work plan layout

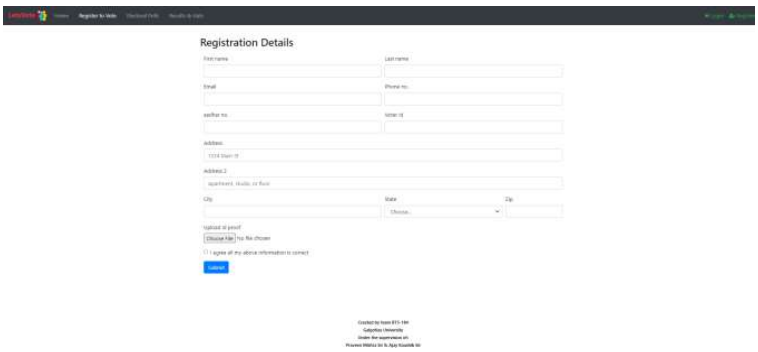
In this Minor Project first we are going to research on Blockchain technology, some ways to secure data with the help of Python Language like what modules and libraries will help in blockchain. We are going through research papers, documentations, and several other stuff.

After the Successful research, In the second phase we will implement e-voting system using this technology. We will implement this technology in a web app that will be creating using Django (a python supported framework for web). The project is result of equal contribution of all the three candidates and aimed to outline our proposal to solve the issues of digital voting by using blockchain.

3. Signature verification



4. Voter registration page



Some more Discussions

Elections, became the subject of a survey that took place in the last few years in cryptography. Compared to Traditional voting or Paper based voting, E-Voting is very Environmental friendly, there is no COUNTING MISTAKES. Taking about the Time and voting efforts, there is very less effort and will be no wastage of time, some of the peoples are also out of station so they are unable to vote for the welfare of the country so, VOTE RESULTS may be increase with the introduction of the E-Voting system. In another way, E-VOTING is used only in few countries, example, ESTONIA, CANADA, AUSTRALIA. On the other hand, the E-voting is abandoned in some country like GERMANY, due to the security issues and the vulnerability.

A lot of issues can also be encountered in our country, like ILLETRACY, lack of knowledge about the internet and the computer. And one more challenge we will may face is the lack of computer and smart phone devices.

Security is the biggest challenge will be faced when we are implementing this E-voting system.

CHAPTER- 5

Conclusion and Future Scope

Conclusions

Electronic voting has many advantages over the traditional way of voting. Some of these advantages are lesser cost, faster tabulation of results, greater accuracy, and lower risk of human and mechanical errors.

In this paper we have seen various techniques and frameworks which gives short review on the various methodologies which is used in the online voting system. This paper will help to develop a more secured and convenient system which will deal with the current and upcoming challenges and remove the drawbacks of the current system.

Future Scope

Blockchain technology allows The people to verify that their votes are recorded and counted correctly. Any voter may be able to check the counting without the security being hampered. Also there are security concerns in blockchain-based e-voting too, but it is more secured than the traditional voting systems which uses EVMs. In future the EVMs will be placed in the museums for the next generation.

There are many practices which are introduced with various variations which should be done in the existing system to make it more reliable and usable. Some of them guarantee privacy as well security in the system to some extent, but still the voting information and process must be in control as well. And also be managed with advanced programs that will also ensures the safety and confidentiality of voters as well.

From the recent studies it has been revealed that the Election commission of India is working on a project with IIT Madras. And it is expected that by 2024 you will see some fundamental differences in the voting system as the former Chief Election Commissioner Sunil Arora said recently.

Earlier, the Senior Deputy Election Commissioner Sandeep Saxena said that, to cast a vote, electors would still have to physically present at a designated venue and the concept is a "two-way electronic voting system, in a controlled environment, by listed IP devices given by the Election commission on dedicated internet lines, enabled with biometric scanners and a web camera". It is very clear that the voting will be not from home, or anytime-anywhere on any device.

Reference

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

2. International Research Journal of Engineering and Technology (IRJET). Available at: https://www.irjet.net/archives/V6/i6/IRJET-V6I6119.pdf.

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

4. The Indian Express journal. Available at: https://www.newindianexpress.com/opinions/2021/apr/26/from-evms-to-blockchain-based-e-voting-2294834.html

5. Ethdocs.org. (2018). What is Ethereum? — Ethereum Homestead 0.1 documentation. Available at: http://ethdocs.org/en/latest/introduction/what-is-ethereum.html

Publication/ Screen Shots