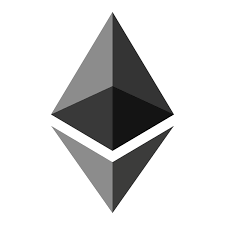
**Token Based System**

****

**Prepared by**

Krutarth Dave(16IT019)

Yashvi Soni(16IT135)

**Under the supervision of**

Dr. Parth Shah

A Report Submitted to

Charotar University of Science and Technology

for Partial Fulfillment of the Requirements for the

Degree of Bachelor of Technology

in Information Technology

IT345 Software Group Project-II (5th sem)

**Submitted at**



**DEPARTMENT OF INFORMATION TECHNOLOGY**

**Chandubhai S. Patel Institute of Technology**

**At: Changa, Dist: Anand – 388421**

**November 2018**



**CERTIFICATE**

This is to certify that the report entitled **“Token Based System”** is a bonafied work carried out by **Mr. Krutarth Dave (16IT019), Ms. Yashvi Soni (16IT135)** under the guidance and supervision of **Dr. Parth Shah** for the subject **Software Group Project-II (IT345)** of **5th** Semester of Bachelor of Technology in **Information Technology** at Faculty of Technology & Engineering – CHARUSAT, Gujarat.

To the best of my knowledge and belief, this work embodies the work of candidate themselves, has duly been completed, and fulfills the requirement of the ordinance relating to the B.Tech. Degree of the University and is up to the standard in respect of content, presentation and language for being referred to the examiner.

|  |
| --- |
| Under supervision of,  Dr. Parth Shah  Head & Associate Professor  Department of Information Technology  CSPIT, Changa, Gujarat. |
|  |

**Chandubhai S Patel Institute of Technology**

At: Changa, Ta. Petlad, Dist. Anand, PIN: 388421. Gujarat

**ABSTRACT**

We live in a world where information is generated and exchanged at a scale that could not have been imagined a few decades ago. A new disruptive force of digital technology is changing the business models and increasingly becoming a crucial factor around the world. A blockchain is a distributed ledger technology that stores information across multiple systems securely to enable peer-to-peer transactions by creating a trustworthy source of ‘truth’ disintermediating the so-called ‘intermediaries of trust’. Also Initial coin offering (‘ICO’, also token launch or token generation) is a term describing a limited period in which a company sells a predefined number of digital tokens (crypto coins) to the public, typically in exchange for major cryptocurrencies. We have combined this two technologies and made our own ICO just for the educational purpose. Our project contains crowdsale environment, where consumers can buy token(s) for a limited period of time.

**ACKNOWLEDGEMENT**

We hereby take this opportunity to thank each and every one who has helped us in creating and formulating this report of subject Seminar. We especially thank our faculties for guiding us through whole period of preparation and presentation. We express our gratitude towards our guide **Mr. Ravi Patel, Mr. Pinal Shah and HOD Sir Dr. Parth Shah**, for giving us moral and academic support. We are also thankful to **Mr. Sagar Patel** for giving suggestion us during project**.**  At last we thank all those who directly or indirectly helped us in preparing the report. We would like to thank all our friends, colleagues and classmates for all the thoughtful and mind stimulating discussions we had, which prompted us to think beyond the obvious. Last but not least we would like to thank our family members who provide us enormous support during this work directly and indirectly.

- Krutarth Dave (16IT019)

- Yashvi Soni (16IT135)

**CONTENTS**

Abstract iii

Acknowledgement iv

Chapter 1 Introduction 1

1.1 Project Overview 1

1.2 Scope 1

1.3 Objective 1

Chapter 2 Theory 1

2.1 Blockchain History 2

2.2 Structure of Blockchain 3

2.3 Types of Blockchain Network 3

2.4 Types of Blockchain 4

2.5 Applications of Blockchain 5

2.6 ERC Tokens 8

2.7 ICO 12

Chapter 3 System Analysis 13

3.1 User Characteristics 13

3.2 Tools & Technology 13

Chapter 4 System Design 14

4.1 Flow of System 14

4.2 Major Functionality 14

4.3 GUI snapshot 15

Chapter 5 Implementation 16

5.1 Implementation Environment 16

5.2 Codding Standards ……………………………………………………….16

5.3 Snapshots of project 16

Chapter 6 Constraints and Future Enhancement 18

Chapter 7 Conclusion 19

Glossary 20

References 21

**LIST OF FIGURES**

Fig 2.1 Merkle Tree……………………………………………………………..2

Fig 2.2 Transaction in bitcoin……………………………….…………………..6

Fig 4.1 Loading Window ……………………………………………….............15

Fig 4.2 Loaded Window………………………………………………....……..15

Fig 5.1 Main Window (with content) …………………………………………..16

Fig 5.2 Metamask conformation………………………………………………..17

Fig 5.3 Information about token after buying…………………………………..17

**Chapter 1: Introduction**

* 1. **Project Overview**

Token Based System is basically a crowdsale website which works as an ICO, where consumers can buy ERC-20 Tokens in exchange of ether(s)(native currency of ethereum) to use the service(s) provided by the website. This is an example of a pre-sale of ICO. A website offers tokens to the users. By this website user can buy the tokens, see how many tokens he have and total number of tokens sold.

* 1. **Scope**

This website can be used in many fields such as health, finance, education, trade etc. Every field which includes the “Trusted Third Party” can be replace with smart contracts. This kind of smart contracts ensures that both party get what they agreed on. And no one can deny that agreement. This smart contracts can be used by businessmen or traders as a trusty agreement.

* 1. **Objective**

This application is just for the educational purpose. Using Token Based System, authorized user can buy any number of Tokens from the website when the sale is on, and can use it to view or to use the service(s) provided by the website. Also the transactions are stored on Ethereum blockchain.For this project transactions are stored in ganache local blockchain. This is the base for entering in ICO building skills.

**Chapter 2: Theory**

**2.1 Blockchain History**

The first work on a cryptographically secured chain of blocks was described in 1991 by Stuart Haber and W. Scott Stornetta. They wanted to implement a system where document timestamps could not be tampered with. In 1992, Bayer, Haber and Stornetta incorporated [Merkle trees](https://en.wikipedia.org/wiki/Merkle_tree" \o "Merkle tree) to the design, which improved its efficiency by allowing several document certificates to be collected into one block.

**2.2 Structure of Blockchain**

Initially the structure of blockchain contains merkle tree.

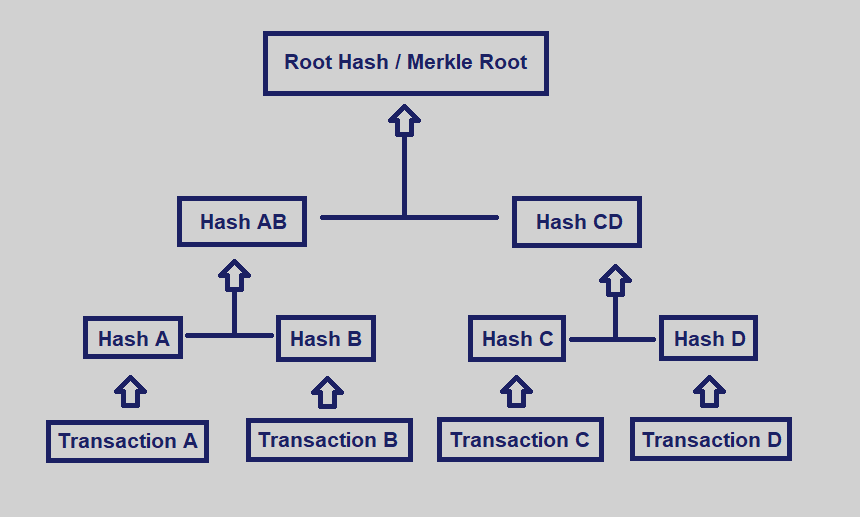
****

Fig 2.1 Merkle Tree

**Merkle Tree:**

In Merkle tree, leaf nodes which holds the documents is labelled with the hash of the data block. And every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes. And this is repeated till the root node. It is such a structure that if someone changes any information in any of the block, the hash of that block will be changed, and so of the root. So that every other node can detect that there is some unauthorized change in the network.

It was the first glance at a blockchain structure. Later on, first blockchain was conceptualized by a person (or group) known as Satoshi Nakamoto in 2008. Nakamoto improved the design in such a way using a hashcash-like method to add blocks to the chain without requiring to be signed by a trusted party.

It is a distributed ledger technology. There are blocks in the ledger. Block holds the batched of valid transactions that are hashed and encoded in merkle tree. Each block includes the cryptographic hash of previous block in the blockchain. Thus linking them as a chain. The linking blocks go all the way to the genesis block.

These hashed block-linking in a merkle tree ensures the security. If someone wants to do change in any block he would have to change all the after blocks in the chain. And that is not feasible for current hardware speed.

**2.3 Types of blockchain network**

There are two types of blockchain network: 1) permission-less 2) permissioned

* **Permission-less:**

This kind of networks work in an open environment and over a large network of participants. The users do not need to know the identity of the peers in the network and hence users do not need to reveal their identity to others. So user can stay anonymous.

Transactions are done by public keys i.e. if A wants to send 50 $ to B, then A should have the public key of B. The longest chain is accepted for the whole network. Examples of these kind of network are bitcoin, litecoin, ethereum.

ICOs are part of these kind of networks. People just need an ethereum account to buy tokens.

* **Permissioned:**

It is also known as Blockchain 2.0. Blockchain can be applied not only to crypto currency, but to secure data too. The underlying concepts of consensus, security, distributed ledgers can be applied to close or permissioned network.

Most enterprise need only tens or hundreds of participants. So this is useful to create and give specific rights and authorities to the participants. It can be used in movement tracking of an asset like in banks and supply chains. Example of this kind of network is IPFS, Hyperledger Fabric. These types of network supports the privacy of the user.

**2.4 Types of blockchain**

* **Public Blockchains:**

A public blockchain has absolutely no access restrictions. Anyone with an [internet](https://en.wikipedia.org/wiki/Internet) connection can send [transactions](https://en.wikipedia.org/wiki/Financial_transaction) to it as well as become a [validator](https://en.wikipedia.org/wiki/Validator) (i.e., participate in the execution of a [consensus protocol](https://en.wikipedia.org/wiki/Consensus_(computer_science))). Usually, such networks offer [economic incentives](https://en.wikipedia.org/wiki/Incentive) for those who secure them and utilize some type of a [Proof of Stake](https://en.wikipedia.org/wiki/Proof-of-stake) or [Proof of Work](https://en.wikipedia.org/wiki/Proof-of-work_system) algorithm. Some of the largest, most known public blockchains are Bitcoin and Ethereum.

* **Private Blockchains:**

A private blockchain is permissioned. One cannot join it unless invited by the network administrators. Participant and validator access is restricted. This type of blockchains can be considered a middle-ground for companies that are interested in the blockchain technology in general but are not comfortable with a level of control offered by public networks. Typically, they seek to [incorporate](https://en.wikipedia.org/wiki/Incorporation_(business)) blockchain into their accounting and record-keeping procedures without sacrificing autonomy and running the risk of exposing sensitive data to the public internet.

* **Consortium Blockchains:**

A consortium blockchain is often said to be semi-decentralized. It, too, is permissioned but instead of a single [organization](https://en.wikipedia.org/wiki/Organization) controlling it, a number of companies might each operate a [node](https://en.wikipedia.org/wiki/Node_(networking)) on such a network. The administrators of a consortium chain restrict users' reading rights as they see fit and only allow a limited set of trusted nodes to execute a consensus protocol.

**2.5 Applications of Blockchain**

* **Cryptocurrencies:**

The primary use of the blockchains today is a distributed ledger for cryptocurrency. In crypto currency a block is generated when a computationally difficult hashed function is solved and the block is added to the current chain. This computing takes a lot of electricity. This solving hash and generating block is called mining of the coins. There are many methods for mining process too. With each block added to the chain, certain amount of coin or cryptocurrency is generated.

There are many challenges for this kind of network. Security is less of a issue because of the blockchain structure. Main concern is consensus. Every node has a copy of the existing chain. And after certain time a new block is added. So every node in the world should get the latest updated chain at almost same time.

There are many cryptocurrencies like bitcoin, litecoin, ether etc. We will take an example of bitcoin to understand this.

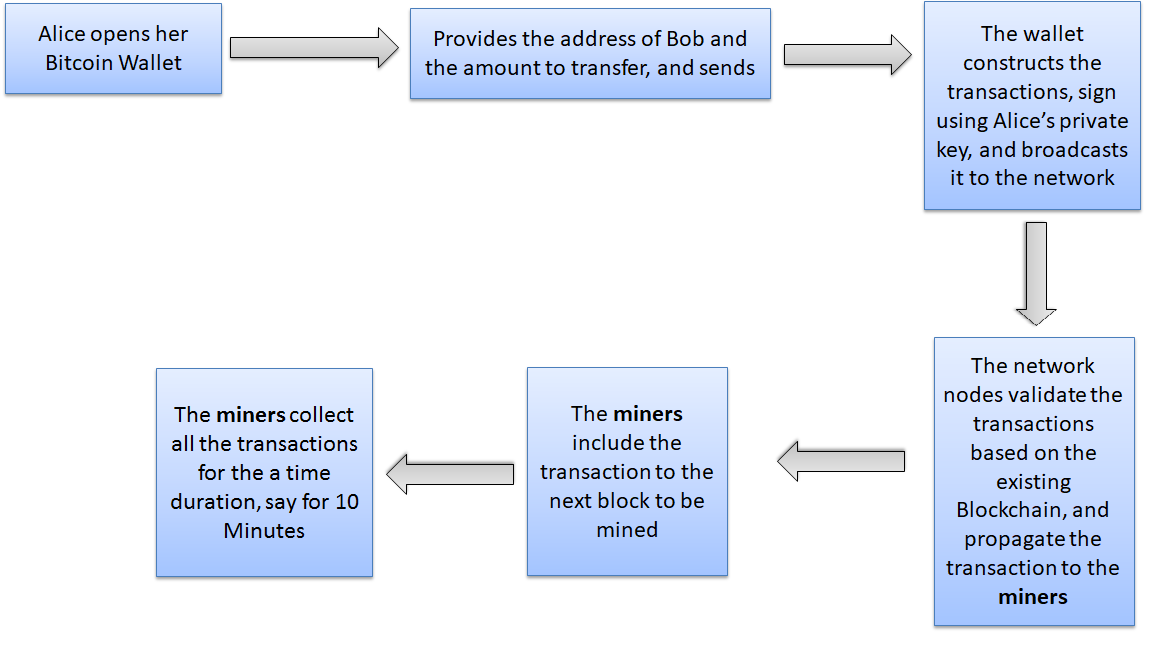
Bitcoin is a completely decentralized, peer-to-peer, permission-less cryptocurrency put forth in 2009.

* Decentralized: No central party to ordering or controlling or recording anything.
* Peer to peer: Software that runs on the machines of all the stakeholders to form a system
* Permission-less: no-identity. No need to sign up anywhere to use.

It is a currency on which no government or central party has any control.

Then the other well-known application of this is smart contracts. The current bitcoin price is $6398.21 (as of 23rd October,2018 at 1:20pm).

Let’s take an example of one transaction. Say, Alice wants to send some bitcoin to Bob. So this happens:



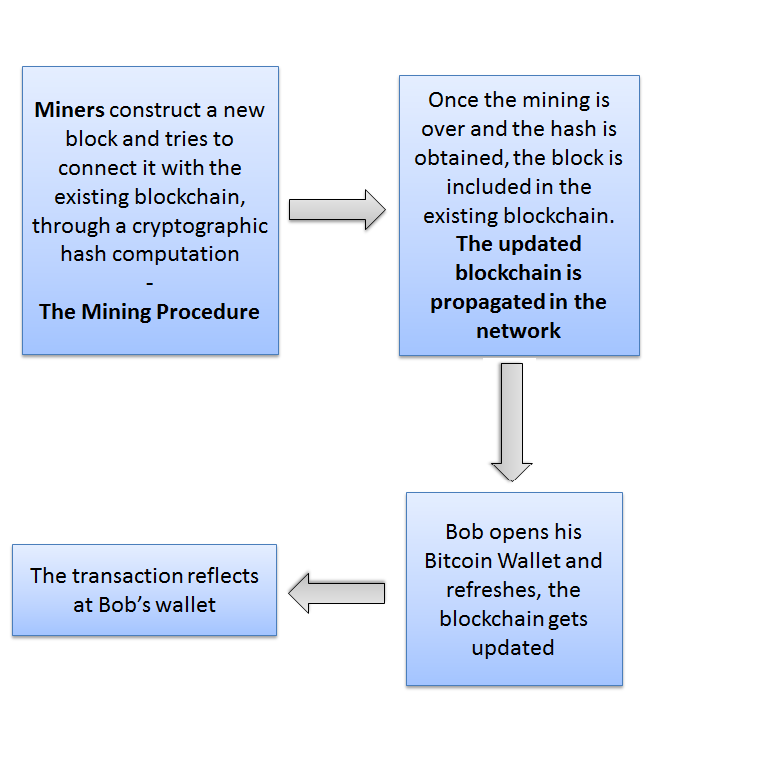


Fig 2.2 Transaction in Bitcoin

* **Smart Contracts:**

The term was coined by Nick Szabo, a computer scientist and cryptographer, in 1996. An automated computerized protocol used for digitally facilitating, verifying or enforcing the negotiation or performance of a legal contract by avoiding intermediates and directly validating the contract over a decentralized platform – faster, cheaper and more secure. Szabo claimed that smart contracts can be realized with the help of a public ledger. Blockchain can be a pioneering technology to realize smart contracts.

Advantages of these smart contracts are:

* **Immutable**: No party will be able to change the contract once it is fixed and written to the public ledger (the Blockchain)
* **Distributed:** All the steps of the contract can be validated by every participating party – no one can claim later that the contract was not validated

Some of the platforms of Smart Contracts are:

* Ethereum
* Rootstock Software
* Hyperledger
* Ripple

ICOs are offering the tokens with smart contracts written on them. These tokens usually follow the ERC-20 standards.

**2.6 ERC Tokens**

There are basically two types of Tokens:

* Fungible Tokens
* Non-Fungible Tokens

|  |  |
| --- | --- |
| **Fungible Token** | **Non- Fungible Token** |
| **Interchangeable** A token can be exchanged for any other token with the same value. A EUR coin can be used for another EUR coin, with no difference to the user. | **Non-interchangeable** NFTs cannot be replaced with other tokens of the same type. If you lend the token to someone, you would expect them to return the same token, just as a museum that lends a Picasso painting to another museum for an exhibition. The other museum cannot simply return another Picasso painting. |
| **Uniform** Tokens of the same type are identical in specification, each token is identical to another token of the same type. | **Unique** Non-fungible assets have unique information or attributes that make them irreplaceable or impossible to swap. Each token is unique and differs from other tokens of the same class. While plane tickets from and to the same destination look the same, each one has different passenger names, departure times and seat numbers, and therefore not easily transferable. |
| **Divisible** FTs are divisible into smaller amounts. It does not matter which unit you get as long as it has the same value. Changing bills for coins is a good example. Fungible tokens are divisible meaning you can send a fraction of token to someone else. | **Non-divisible** Cannot be divided, the elementary unit is the token. You cannot trade your university certificate with a university certificate of that same university but of another person, and you cannot divide it into different parts. |

The blockchain based token economy today is currently predominantly built on fungible tokens like Bitcoin, Zchash, Ether or any ERC-20 token. So let’s understand the tokens in detail by taking examples.

* **ERC-721 (NFT)**

ERC-721 is a free, open standard that describes how to build non-fungible or unique tokens on the Ethereum blockchain. Non-fungible tokens on the blockchain are unique in nature, everyone knows how many there are, they can be distinguished from each other and have varying properties. They can offer unique characteristics which make them different and thus digitally scarce. While attempts to offer and manage digital scarce assets, like avatars in video games, have existed before blockchain, this type of scarcity was costly to manage and relied on the validation and security of the game creators. In this context, distributed ledgers are significant because they enable a decentralized way to maintain distinct, digitally scarce items. NFTs on the blockchain allow for digital scarcity to be verified without the need for a centralizing organization to confirm authenticity at very low operational costs. This creates publicly verifiable digital scarcity and makes it desirable for its uniqueness, instead of being a placeholder or representation.

The successful Application of ERC-721 Token is :

* **Cryptokitties**

One early pioneer of non-fungible tokens was [CryptoKitties](https://cointelegraph.com/tags/cryptokitties), a blockchain-driven game where players have the chance to collect and breed digital cats, with each cat’s digital genetic material being stored on the blockchain. They can be bought and sold using ETH, some cats are rarer than others. In 2017 sales of Cryptokitties hit $12 million, with the most expensive CryptoKitty reportedly going for $120,000. Other blockchain games followed quickly (see list below). Major League Baseball in the US is planning to launch a game where baseball cards can be exchanged on the Ethereum blockchain. Crypto-collectibles like [CryptoPunks](http://thecryptopunks.com/), [CryptoAlpacas](https://www.cryptoalpaca.pet/), and [CryptoKitties](https://www.cryptokitties.co/), are basically digitizing the very essence of the sports cards hobby – the joy of owning something unique and the thrill of comparing it to others.

* **ERC-20 (FT)**

ERC-20 stands for Ethereum Request For Comment and 20 is the number that is assigned to this request. ERC-20 is a technical standard used for [smart contracts](https://en.wikipedia.org/wiki/Smart_contract) on the [Ethereum](https://en.wikipedia.org/wiki/Ethereum" \o "Ethereum) [blockchain](https://en.wikipedia.org/wiki/Blockchain" \o "Blockchain) for implementing tokens. The clear majority of tokens issued on the Ethereum blockchain are ERC-20 compliant. As of 2018-07-26, a total of 103621 of ERC-20 compatible tokens are found on Ethereum main network, according to Etherscan.io.ERC-20 defines a common list of rules for Ethereum tokens to follow within the larger Ethereum ecosystem, allowing developers to accurately predict interaction between tokens. These rules include how the tokens are transferred between addresses and how data within each token is accessed.

These are some functions that a ERC-20 token must have:

1. **totalSupply()** public view returns (uint256 totalSupply)

* Get the total token supply

1. **balanceOf(address \_owner)** public view returns (uint256 balance)

* Get the account balance of another account with address \_owner

1. **transfer(address \_to, uint256\_value)** public returns (bool success)

* Send \_value amount of tokens to address \_to

1. **transferFrom(address \_from, address \_to, uint256 \_value)** public returns (bool success)

* Send \_value amount of tokens from address \_fromto address \_to

1. **approve(address \_spender, uint256 \_value)** public returns (bool success)

* Allow \_spender to withdraw from your account, multiple times, up to the \_value amount. If this function is called again it overwrites the current allowance with \_value

1. **allowance(address \_owner, address \_spender)** public view returns (uint256 remaining)

* Returns the amount which \_spender is still allowed to withdraw from \_owner

These are some events that an ERC-20 token should handle:

1. **Transfer(address indexed \_from, address indexed \_to, uint256 \_value)**

* Triggered when tokens are transferred

1. **Approval(address indexed \_owner, address indexed \_spender, uint256 \_value)**

* Triggered whenever approve(address \_spender, uint256 \_value) is called

Applications of ERC-20 Tokens are :

* As of July 26 2018, there were more than 103,621 ERC-20 token contracts.
* Among the most successful ERC20 token sales are [EOS](https://en.wikipedia.org/wiki/EOS.IO), [Filecoin](https://en.wikipedia.org/wiki/Filecoin" \o "Filecoin), Bancor, Qash, and Bankex, raising over $70 million each.



**2.7 ICO**

* **History**

The first token sale (also known as an ICO) was held by Mastercoin in July 2013. [Ethereum](https://en.wikipedia.org/wiki/Ethereum" \o "Ethereum) raised money with a token sale in 2014, raising 3,700 BTC in its first 12 hours, equal to approximately $2.3 million at the time. ICOs and token sales became popular in 2017. There were at least 18 websites tracking ICOs before mid-year. In May, the ICO for a new web browser called [Brave](https://en.wikipedia.org/wiki/Brave_(web_browser)) generated about $35 million in under 30 seconds. Messaging app developer [Kik](https://en.wikipedia.org/wiki/Kik_Messenger" \o "Kik Messenger)'s September 2017 ICO raised nearly $100 million. At the start of October 2017, ICO coin sales worth $2.3 billion had been conducted during the year, more than ten times as much as in all of 2016. As of November 2017, there were around 50 offerings a month, with the highest-grossing ICO as of January 2018, being Filecoin raising $257 million (and $200 million of that within the first hour of their token sale). By the end of 2017, ICOs had raised almost 40 times as much capital as they had raised in 2016, although still amounting to less than two percent of the capital raised by [IPOs](https://en.wikipedia.org/wiki/Initial_public_offering). According to industry newsletter Cointelegraph, companies raised around $6 billion via ICOs in 2017; 37% of that amount was made by only 20 ICOs. Already by February, 2018, an estimated 46% of the 2017 ICOs had failed. ICOs are sometimes called "[token sales](https://en.wikipedia.org/wiki/Token_sale)". Ethereum is (as of February 2018) the leading [blockchain](https://en.wikipedia.org/wiki/Blockchain" \o "Blockchain) platform for ICOs with more than 80% market share. Tokens are generally based on the Ethereum [ERC-20](https://en.wikipedia.org/wiki/ERC-20) standard.

* **Introduction**

An initial coin offering (ICO) or initial currency offering is a type of funding using [cryptocurrencies](https://en.wikipedia.org/wiki/Cryptocurrency" \o "Cryptocurrency). Mostly the process is done by [crowdfunding](https://en.wikipedia.org/wiki/Crowdfunding" \o "Crowdfunding) but private ICO's are becoming more common. In an ICO, a quantity of cryptocurrency is sold in the form of "tokens" ("coins") to [speculators](https://en.wikipedia.org/wiki/Speculator) or [investors](https://en.wikipedia.org/wiki/Investor), in exchange for [legal tender](https://en.wikipedia.org/wiki/Legal_tender) or other cryptocurrencies such as [Bitcoin](https://en.wikipedia.org/wiki/Bitcoin" \o "Bitcoin) or [Ethereum](https://en.wikipedia.org/wiki/Ethereum" \o "Ethereum). The tokens sold are promoted as future functional units of currency if or when the ICO's funding goal is met and the project launches. In some cases like Ethereum the tokens are required to use the system for its purposes. An ICO can be a source of [capital](https://en.wikipedia.org/wiki/Financial_capital) for [startup companies](https://en.wikipedia.org/wiki/Startup_company).[[1]](https://en.wikipedia.org/wiki/Initial_coin_offering#cite_note-1) ICOs can allow startups to avoid regulatory compliance and intermediaries such as venture capitalists, banks and stock exchanges.

**Chapter 3: System Requirements Study**

**3.1 User Characteristics**

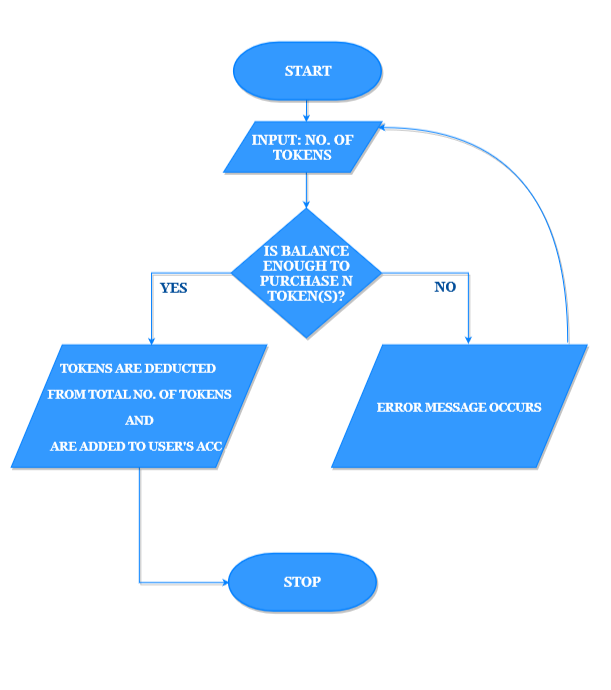
We designed our Token Based System in such a way that anyone can easily access it. Just he/she should have an ethereum account.

**3.2 Tools & Technology Used**

We have made our project with truffle framework and code written in backend is in Solidity. We have used Ganache, a local Blockchain Test Network. For front end we have used HTML, CSS, bootstrap and java script. To connect our website to a network we have used a Google Chrome extension termed Meta Mask, which allows us to interact with the blockchain accounts. And to handle node.js we have used NPM.

**Chapter 4: System Design**

**4.1 Project Flow**



**4.2 Major Functionality:**

* Easily accessible from anywhere and anytime.
* Can be bought using Ether.
* Can see how many tokens are there in one’s account.

**4.3 GUI snapshots**

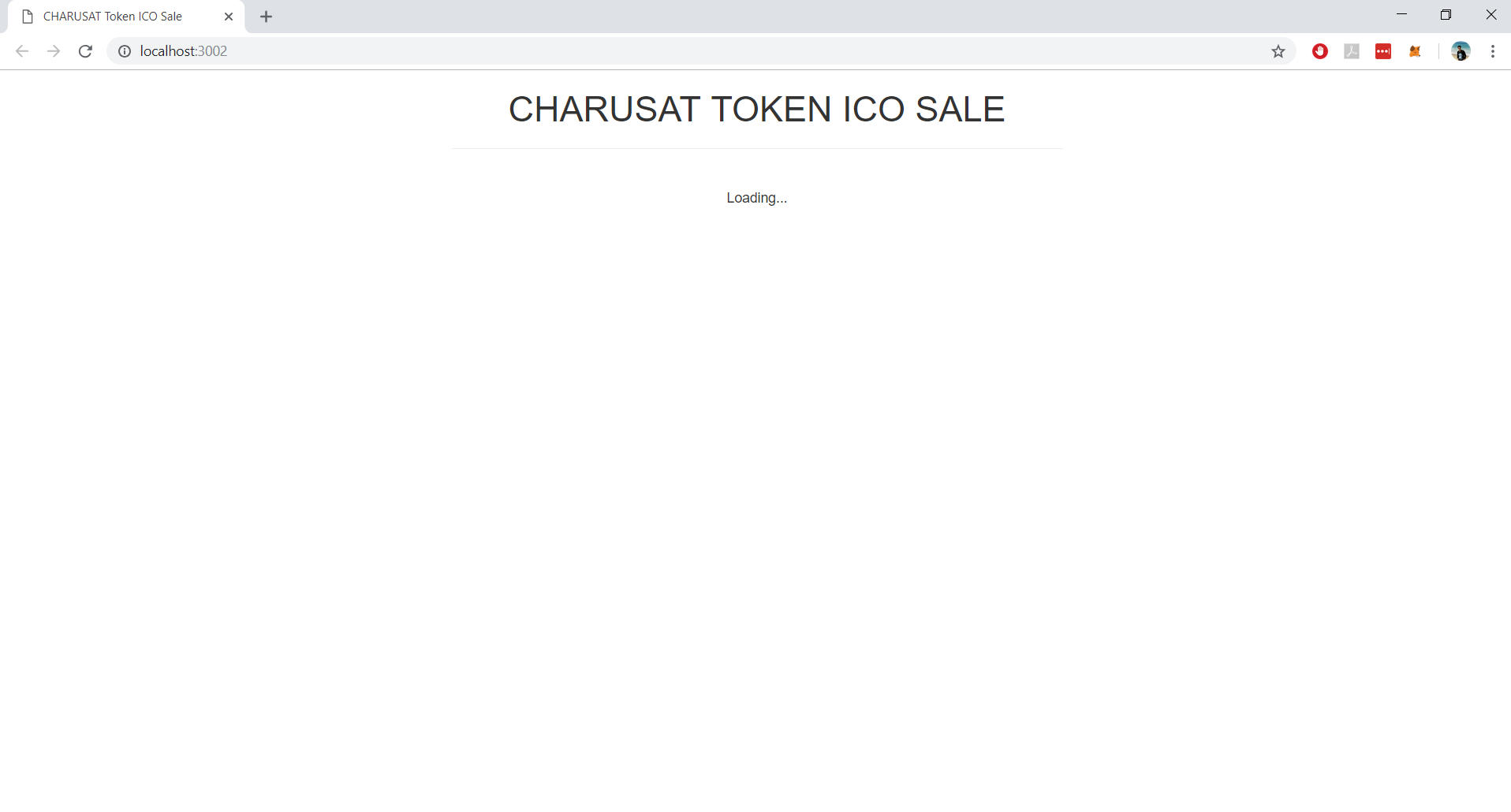


Fig 4.1 loading Window

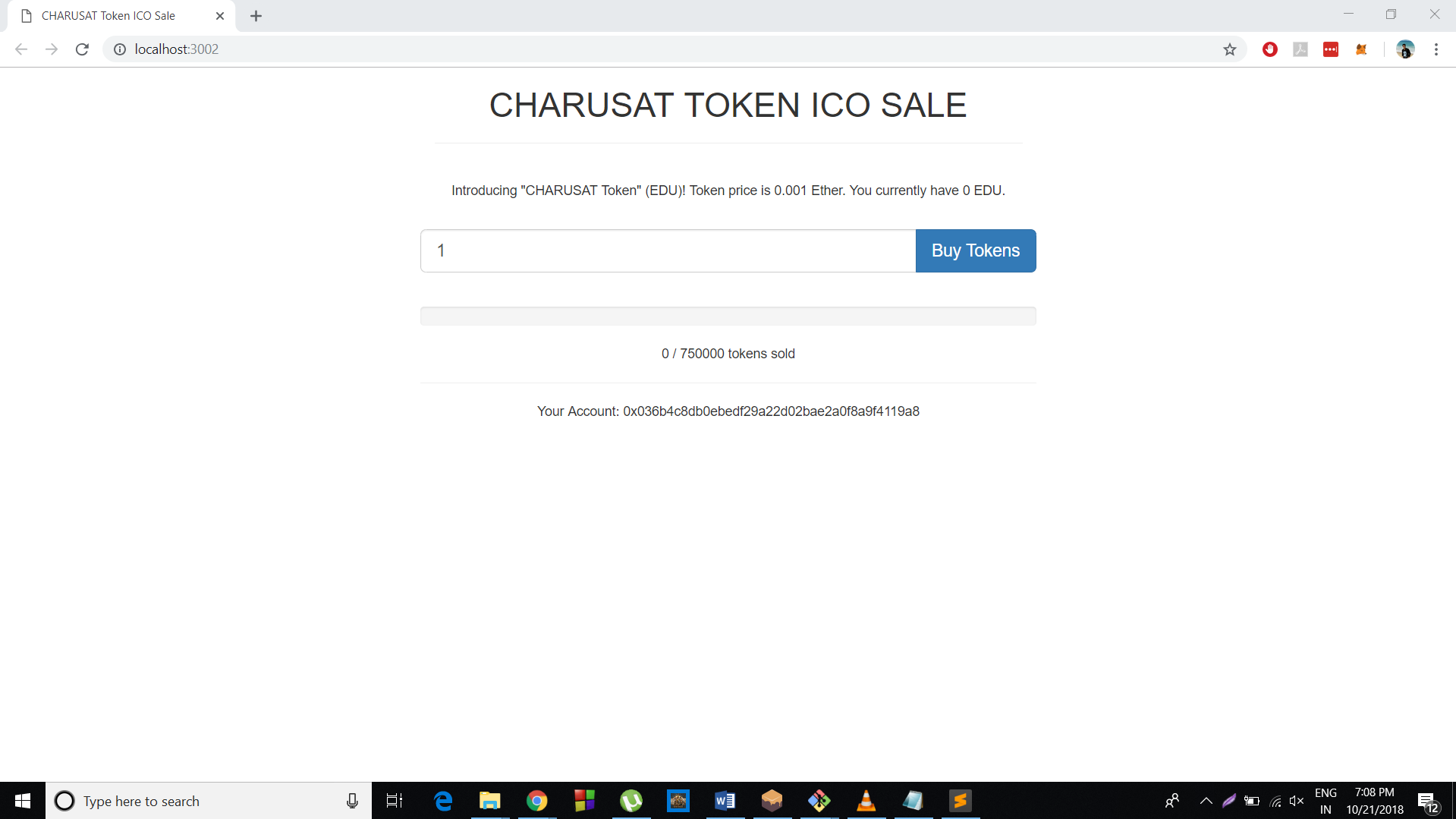


Fig 4.2 loaded screen

**Chapter 5: Implementation Planning**

**5.1 Implementation Environment**

We implemented this project in Windows 10 using sublime text editor. For tests we have used Truffle Framework and local Blockchain Ganache.

**5.2 Coding Standards**

We used ERC-20 standards for creating our tokens and determined how they behave.

**5.3 Snapshots of project**

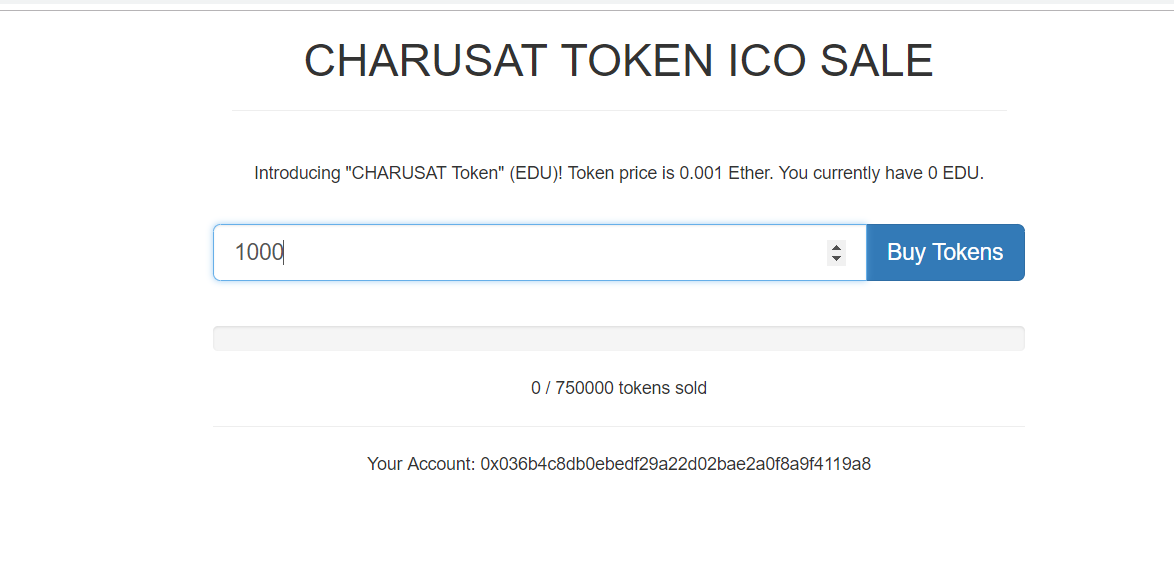


Fig 5.1 Main Window (with content)

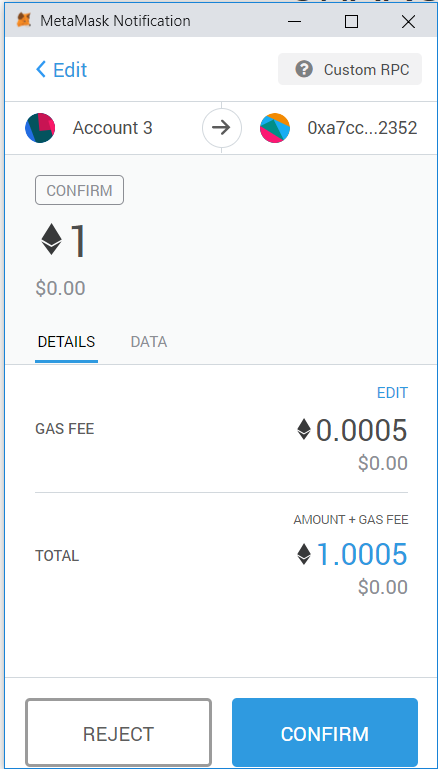


Fig 5.2 Metamask Conformation

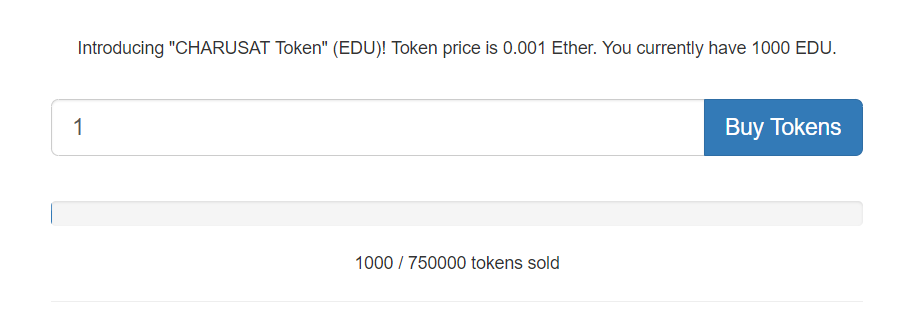


Fig 5.3 information about token after buying

**Chapter 6: Constraints and Future Enhancement**

* **Limitations:**
* The limitations are not yet in sight.
* **Future Enhancement:**
* To provide the service(s) to the user for the purchased tokens.

.

**Chapter 7: Conclusion**

Token Based System is not completed yet. We will complete this in near future.

After completion of our project we learnt how to work with Blockchain Technology and how to create an ICO. We learnt much about smart contracts too. Also, we learnt how to make a project in group. Also we came to know which kind of difficulties arises during group project and how to solve it.

**Glossary**

|  |  |
| --- | --- |
| ICO | Initial Coin Offering |
|  |  |
| ERC | Ethereum Request For Comment |
|  |  |
| NFT | Non-Fungible Token |
|  |  |
| FT | Fungible Token |
| NPM | Node Packet Manager |

**References**

1. <www.dappuniversity.com/articles/code-your-own-cryptocurrency-on-ethereum>
2. [in-strategy-innovation-blockchain-technology-india-opportunities-challenges-noexp.pdf](2.%09in-strategy-innovation-blockchain-technology-india-opportunities-challenges-noexp.pdf)
3. <https://youtu.be/XdKv5uwEk5A?list=PLS5SEs8ZftgWFuKg2wbm_0GLV0Tiy1R-n>

4. [Arup%20%20Blockchain%20Technology%20Report.pdf](file:///C:\Users\sairam\Downloads\Arup%20%20Blockchain%20Technology%20Report.pdf)

5. <https://cryptovalley.swiss/wp-content/uploads/20180628_PwC-S-CVA-ICO-Report_EN.pdf>