Cryptocurrency using Blockchain Technology

Nupur Bhatt[1], *Aditya Vikram Singh*[2], *Shivani Upadhayay*[3], *Richa Verma*[4]
[1,2,3,4]*Students Department Of Computer Science and Engineering , Raj Kumar Goel* Institute Of Technology

Abstract

This proposed work is aimed at developing a Blockchain-based cryptocurrency that will use a decentralized system[1] that can be used to raise funds for startups who can offer coins to public by proposing their prototype instead of waiting on an investor and moreover it can solve major issues like tampering of confidential information of citizens or even government as it will eradicate the use of a single centralized system which is in today's world responsible for protecting and securing all the data. Features of this system will be distributed ledger to store information which will develop clear transparency among everyone, unlike centralized systems. This will help everyone to know about the recent adaptations taken by everyone in storing data in a decentralized way. This is designed to assist in strategic planning and will help to ensure that an organization is equipped with the right information for the future. Also for those that are always on the go, this technique comes with remote access features, which can allow you to manage your workforce anytime, in the least times. These Systems will ultimately allow you to better manage resources and store your data in an easier form and more protected form.

1) INTRODUCTION

The main objective of this is to make a cryptocurrency or an ICO (Initial Coin Offering) [2] which is the cryptocurrency space's rough equivalent to an IPO (Initial Public Offering) in the mainstream investment world. ICOs act as fundraisers of sorts; a corporation looking to make a replacement coin, app, or service launches an ICO. Next, interested investors buy into the offering, either with online transactions or fiat currency or with pre-existing digital tokens like Ether or Bitcoin. In exchange for his or her support, investors receive a brand new cryptocurrency token specific to the ICO. Investors hope that the token will perform exceptionally well into the future after looking onto the whitepaper of the startup offering the sale and their plans providing them with a stellar return on investment making a win-win situation for both the invertors and the company. The company holding the ICO uses the investor funds as a way of furthering its goals, launching its product, or starting its digital currency. ICOs are employed by startups to bypass the rigorous and regulated capital-raising process required by venture capitalists or banks.

Functionalities:

a. Purchase/Sale the coin.
b. Manages and storage of data in a Decentralized way.
c. Usage of Distributed Ledger [3]
d. Legal documents verified using Smart Contracts
e. Crowdfunding
f. Transactions can be noted in Blockchain System and once noted becomes immutable
g. Distributed Peer to Peer Network
h. Consensus ProtocolSystem [4]
i. Mine for new blocks (or stake ether PoS)

All records are publicly available for anyone to check; although privacy is rumored to be coming within the future, for now, everything is out in the open.

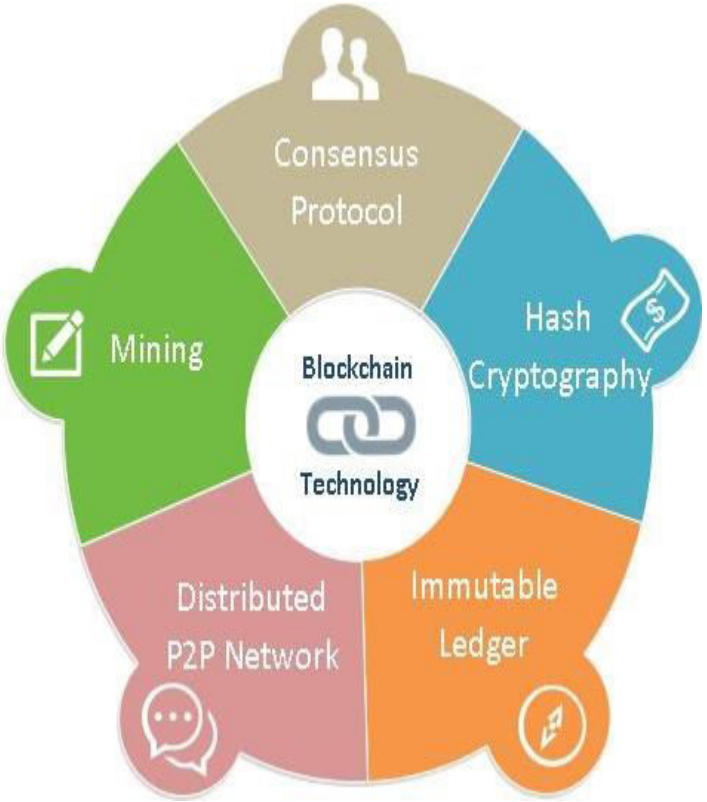

Figure 1. Key forces of Blockchain technology

2) LITERATURE SURVEY

Satoshi Nakamoto implemented the bitcoin software as open-source code and released it in January 2009 [5][6][7]andon 3 January 2009, the bitcoin network was created when Nakamoto mined the first block of the chain, known as the genesis block.[8][9]The receiver of the first bitcoin transaction was Cypherpunk Hal Finney, who had created the first reusable proof-of-work system (RPoW) in 2004. [10]

According to a survey,blockchain technology offers a massive change to capital markets and a more efficient way for performing operations like:

a. Securities and derivatives transaction (Van de Velde et al., 2016, Wu and Liang, 2017)
b. Digital payments (Papadopoulos et al., 2015, Beck et al., 2016, Min et al., 2016, Yamada et al., 2017, English and Nezhadian, 2017, Lundqvist et al., 2017, Gao et al., 2018)
c. Loan management schemes (Gazali et al., 2017)
d. General banking services (Cocco et al., 2017)
e. Financial auditing (Dai and Vasarhelyi,2017)
f. Cryptocurrency payment and exchange (i.e., e-wallets) (Cawrey, 2014, Rizzo, 2014)

Notably, a set of the world's biggest banks, including Barclays and Goldman Sachs have joined forces with R3 to establish an operating blockchain-based framework for the financial market.
Anothe bank cooperation is the Global Payments Steering Group (GPSG) , whose members include Santander, Bank of America and UniCredit, among others. The cryptocurrency behind GPSG is XRP, created by Ripple (Britto et al., 2012) which implements an interoperable and scalable open-source infrastructure enabling global payments and currency exchanges.

3) SOFTWARE REQUIREMENT SPECIFICATION

The Software Requirement Specification is produced at the culmination of the analysis of the task. The Function and performance allocated to the software as a part of system engineering and refined by establishing an

entire information description, an in depth functional and behavioral description, a sign of performance requirements and design constraints, validation criteria and other data requirements.

The proposed system has following requirements:

a. System need to store information about the new entry(Block).
b. System need to maintain the quantity record.
c. System need to help the transaction done on [11]Ethereum Network.
d. System need to setup MyEtherWallet.
e. System need to be decentralized.
f. System need to be secure.
g. System needs to have its unique address using Hash.

3.1 Identification of need:

The old system was facing a series of drawbacks and it was not desentralized. And to develop a coin on Ethereum based platform we need the setup of EVM . Before the arrival of Ethereum, cryptocurrencies were designed with a narrow range of function (sometimes this was completely singular). Bitcoin, for instance , could only operate as digital currency.Developers had hit a roadblock; they'd either got to expand the functionality of Bitcoin onto the prevailing blockchain (very time consuming and technically challenging) or start from scratch with a whole new platform. Recognizing this impasse, Buterin stepped into the void, pioneering the EVM. All the Ethereum nodes execute contracts using their EVMs and this invention is large because it allows people to create things during a more efficient way than ever before. Now every application can be built in one place; there is no need for an original blockchain for every new project.. Ethereum provides a base for these contracts because it is "software that can host other software". This offers A level of functionality that a lot of other cryptocurrencies simply don't have. Ethereum is projected to have the ability to deal with things like identity systems, insurance payments, and management of permissions (to name a few)generation. One more problem was it was very difficult in finding errors while entering the data. Once it was entered it was very difficult to update as well.

The reason behind it was thee was lot of information to be maintained and have to be kept in mind while

running the organization. For this reason, we've provided features present system which is partially automated, actually existing system is sort of laborious together has got to enter an equivalent information at three different places.

Following points should be considered:

a. Documents and reports must be provided by the new system, there can also be a few reports , which can help in management and decision making and cost controlling.
b. Details of the information needed for each document and report.
c. The required frequency and distribution of each project.
d. Probable sources and information for report and document.
e. With the implementation of computerized system, the problem of keeping records will be solved.
f. The greatest of all is the retrieval of information, which will be at the click of the mouse.
g. So the proposed system helps in saving time in different operations and making information flow easy giving valuable reports.

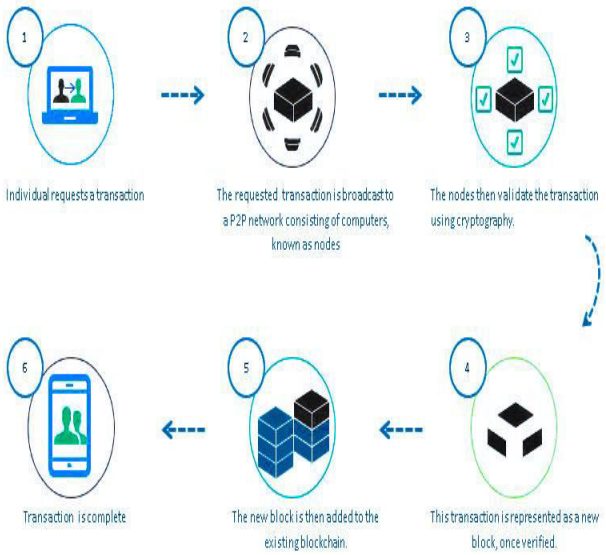

Figure 2. Transaction Validation through Blockchain

3.2System design of the cryptocurrency:

In this phase, the logical system is built considering all the requirements and fulfills all the requirements. Design phase of software development deals with transforming the clients requirements into logically working system.Normally design is done in following two steps:

3.2.1Primary Design Phase:

In this phase, the system is designed in block level.The blocks are created on the basis of analysis done in the problem identification phase. Different blocks are created for various functions emphasis is placed on minimising the knowledge flow between blocks.Thus all the activites which require more Interaction are kept in one block.

3.2.2Secondary Design Phase:

In this phase, the deatailed design is done.
The general tasks involved within the design process are the following:

a. Design Various blocks for overall system process.
b. Design Smaller, compact and workable modules in each block.
c. Design various database structures.
d. Specify details of programme to achieve desired functionality.
e. Design the form of inputs and outputs of the system
f. Perform documentation of the design.
g. System reviews.

3.3Modules Introduced:

Modules introduced are: -

3.3.1 Blockchain Application:

a. **Index:** It will show the index number for a particular Block.
b. **Previous Hash:** It will show & store the Hash code for the Previous Block.
c. **Message:** This will help you to know how many blocks you have mined & to see the chain.
d. **Proof:** It defines the proof of work for the transaction.
e. **Timestamp:** The timestamp is used primarily for establishing the difficulty. Without a timestamp, new nodes wouldn't be ready

to determine the right difficulty to be used for every block period as they would not skills long it took to mine those blocks.

f. **Mine Block:** It will Evertime help you to mine a new Block.
g. **Get chain:** It will help to get the full chain of blocks.

3.3.2 Cryptocurrency:

a. **Sender:** It will store the details of sender who is sending the cryptocurrency.
b. **Receiver:** It will store the details of the receiver who is receiving the cryptocurrency.
c. **Amount:** It will help you to know the number of the cryptocurrency you want to Send/Receive.
d. **View Transactions:** It will store all the transactions by creation of new Block.

3.4User-Interface Design:

It is concerned with the everything ranging from logging into the system to the eventually presentation of desired inputs and outputs. The flow of screens and messages is called as dialogue.

The Following steps are for proper UID:

a. The system user should be ensure with what to try and do next.
b. The screen should be formatted so various varieties of information, instructions and message always appears within the same general display area.
c. Message should be displayed long enough to permit the system user to read them.
d. Use display attributes sparingly.
e. Default values for fields and answers to be entered by the user should be specified.
f. user mustn't be allowed to proceed without correcting a slipup or a mistake.
g. The system mustn't get an OS error or fatal error.

3.5Preliminary Product Description:

The first step within the preliminary development cycle is that the investigation to work out the feasibility of the system.The purpose of the preliminary investigation is to guage the project requests.It is not a design study nor does it include the gathering of details to elucidate the business system altogether respect .Rather, it's collecting the data which helps in commiting members to guage the merits of the project request and make an informed judgement about the feasibility of the proposed work.

3.6 Qualitative & Quantitative analysis:

a. A Crypto used be utilized by small startups to extend funds and will also help the individuals who will invest in it.
b. It helps us create a decentralized system which'll be able to store transactions inside a block.
c. It'll help to make the sharing economy.
d. Blockchain take this to another degree ,potentially creating crowd-sourced capital funds.
e. By making the results fully transparent and publicly accessible, distributed database technology could bring full transparency to elections or poll taking. Ethereum-based smart contracts help to automate the tactic.
f. Decentralizing file storage online brings clear benefits. Distributing data throughout the network protects files from getting hacked or lost.
g. Liberty to make transactions happen within seconds.
h. Active involvement of Users.
i. Untraceable in nature
j. Fewer risks for merchants.

4) Technologies used:

4.1 Python is an interpreted, high level,general-purpose computer language .It provides constructs that enable clear programming on both minute and massive scales. The Back-end section of this proposed work is done on Python.

4.2 Flask, a micro web framework written in Python. It's classified as a micro framework because it doesn't require particular tools or libraries.There is no database abstraction layer, form validation, or components wherepre-existing third-party libraries provide common functions.

4.3Postman, a Google Chrome app for interacting with HTTP APIs. It presents you with a friendly GUI for constructing requests and reading responses.

4.4Solidity, a contract-oriented Etherum language for writing smart contracts. It's used for implementing smart contracts on various blockchain platforms.

4.5Ganache, a personal blockchain for Ethereum development that is used to deploy contracts, develop applications, and run tests, available as both a desktop application and a command-line tool.

4.6 MyEtherWallet, an open-source, client-side interface. It allows you to interact directly with the blockchain while remaining in total control of your keys & your funds.

Figure 2. Technologies involved

Name of the component	Specification
Language	Python,Solidity,Remix
Operating System	Windows/Mac (Any)
Framework	Flask
Connecting Service	Postman (HTTP Post/Get)
Ethereum based Wallet	MyEtherWallet(Erc-20)
IDE	Remix
Wallet Type	Web
Supported CryptoCurrencies	ETH, ETC, EOS & ERC20 tokens

Table 1. Requirement analysis

5) CONCLUSION:

Our Work is just merely humble venture to satisfy the necessities to manage the work. Several User friendly coding have also adopted. The technology of this package shall convince to be a package in satisfying all the wants in several sectors like finance, medical, government etc. The main focus of software planning is to provide a framework that allows the manager to make reasonable estimates made within a limited time-frame at the beginning of the software project and must be updated regularly .

At the highest it's concluded that efforts are made on following points:

a. An outline of the background and context of this paper and its reference to work already concluded in that area.
b. Made statement of the aim of the proposed work.
c. Defined the impact of this work on real world and the wayit can revolutionize the present technology.
d. Described the requiredspecifications of the system and therefore the actions which will be done on this stuff and have included features and operations through demographics.
e. System is implemented and tested consistent with the test cases.

REFERENCE:

[1] https://medium.com/distributed-economy/what-is-the-difference-between-decentralized-and-distributed-systems-f4190a5c6462
[2] https://www.binance.vision/economics/what-is-an-ico
[3] https://www.investopedia.com/terms/d/distributed-ledgers.asp
[4] https://www.geeksforgeeks.org/consensus-algorithms-in-blockchain/
[5] https://www.ijltemas.in/DigitalLibrary/Vol.7Issue3/241-242.pdf
[6] https://sourceforge.net/p/bitcoin/code/HEAD/tree/
[7] https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency
[8] https://www.wired.com/2011/11/mf-bitcoin/
[9] https://blockexplorer.com/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
[10] https://www.sfgate.com/technology/businessinsider/article/Here-s-The-Problem-With-The-New-Theory-That-A-4529573.php
[11] https://www.blockgeeks.com/guides/ethereum/