ENGINEERING IN ADVANCED RESEARCHSCIENCE AND TECHNOLOGY

ISSN 2352-8648
Vol.01, Issue.03
December-2021
Pages: -622-670

TO DEVELOP A DECENTRALIZED APPLICATION TO DEMONSTRATE THE USAGE OF CRYPTOCURRENCY THROUGH ETHEREUM BLOCKCHAIN

Dr.M. Chaitanya Kishore Reddy.[1], K.Keerthana.[2], P.Padma Soumya[3],K. Vijay Kumar[4]

[1]chkishore.0007@gmail.com,*Professor & HOD-IT, NRI Institute of Technology, A.P, India.*
[2]kommukeerthana2000@gmail.com, *UG Scholar, Dept.of IT, NriInstitute of Technology, A.P, India.*
[3]ppsowmya1815@gmail.com, *UG Scholar, Dept.of IT, NriInstitute of Technology, A.P, India.*
[4]vijaybabu4135@gmail.com, *UG Scholar, Dept.of IT, NriInstitute of Technology, A.P, India.*

----------***----------

Abstract - *Blockchain Technology is a relatively new approach in the field of information technology. As it was begun to shape with one of its first implementations that was bitcoin as a cryptocurrency and has gained a lot of attention and then later it was together with Ethereum in Blockchain implementation with the focus on smart contracts, they represent the very core of modern cryptocurrency development. The importance of Blockchain technology was increased a lot in various fields such as Banking, Health care, Real-estate, payments, Music, etc. In this project, we are going to build our cryptocurrency and build our blockchain using Ethereum and then build a Decentralized application to demonstrate the usage of Blockchain, and then design the smart contracts using the solidity programming language. To establish a web server and Ethereum Blockchain using remix IDE. In this project, we will be developing a web application Where the user will have the chance of transferring funds in the form of digital money (ex: Cryptocurrency) from his account to his colleagues or any other partners. A decentralized application that is utilizing the latest advancing technology called Blockchain which allows us to perform the actions you would do every day like transferring money without a trusted third party in a secure way. Since a Blockchain is a permanent record of transactions that are distributed, every transaction can irrefutably be traced back to exactly know the details of the time it was done and the amount transferred without revealing the owner's identity. In addition, past transactions cannot be changed, while the present can't be manipulated, because every transaction is verified by every single node in the network and any outside or inside attacker must have control of 51% of the nodes to alter the record.*

Key Words: Cryptocurrency, Digital wallets, Transaction Blockchain, Ethereum, DAPP, Soliditylanguage, Remix IDE.

1. INTRODUCTION

Nowadays, the global economy is inevitably moving towards a digital ecosystem. From investment to money transfer, everything is going paperless. The newest and most promising addition to the digital payment sector is cryptocurrency. This cryptocurrency is a medium of exchange like normal currencies such as USD and others but designed to exchange digital information. In general, cryptocurrency is defined as a decentralized (digital or virtual currency) that uses cryptography for security making it difficult to counterfeit and since it is not issued by a central authority, governments can't take it away from you directly. With this cryptocurrency, many organizations and individuals can do secure financial transactions and can control the creation of additional units, and in parallel, they verify the transfer of assets from one to another in a secured manner by applying various encryption techniques. This Blockchain

technology has also enabled companies to change the way they operate digitally and you see over the last couple of years, the digital currency has been rapidly gaining the public eye Some good reasons behind it are. We are preparing our custom-built crypto currency on the Ethereaum Block chain with the smart contracts using solidity language to my organization for our internal use. One thing in general this crypto currency can be transferred between the two entities conducting a financial transaction with minimal or we can say no processing fees and almost instantaneously and this helps side-steps the many hefty fees banking impose for such transactions and the long wait and hold times they impose on us as well instantaneously and this helps side-steps the many hefty fees banking impose for such transactions and the long wait andholdtimes theyimposeonus as well.

1.1 Technical Scope

The scope of our application exceeds that of its predecessors, which initially helped to protect, certify and distribute the data. It is possible to use blockchain-oriented methods without any intermediary clearing houses. Payments, certificates, attestations, copy rights, contracts, patents, registries can theoretically can be administrated without the need to involve banks, notaries, custodians or any state institutions. The increase interest in the blockchain technology is not only evident in the banking sector but also in the real estate, insurance and health industries which can also benefit from blockchain's wide range of use. Analysts also predict its expansion to judicial system, energy industries and public admiration in future.

1.2 Technical Approach

First, we will be creating a web server using XAMPP and deploying the smart contract on the Ethereum blockchain using Remix IDE. The Textron that will be running in the background will be communicating with the localhost. The address of the smart contracts will be included in the webserver that we are creating and it works according to it. According to the smart contracts, the application gets to know the user's default account whenever the required data is entered, the application works according to the smart contracts and sends tokens to the destined account and then the transaction will be recorded on the blockchain as blocks and can be viewed later.

2. Block Chain:

The blockchain is a growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. Blockchain has been in a lot of buzzes these days and it is the backbone of the very famous cryptocurrency in the world - Bitcoin. Nowadays Many Governments and leading Banks have decided to bring many of their conventional transactions based on the Blockchain concept. The applications and potential of this framework are huge and are considered to be changing the way transactions are made in various domains. A blockchain is a distributed database that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in digital format. Blockchains are best known for their crucial role in cryptocurrency systems, such as Bitcoin, for maintaining a secure and decentralized record of transactions. The innovation of a blockchain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party. One key difference between a typical database and a blockchain is how the data is structured. A blockchain collects information together in groups, known as blocks, that hold sets of information. Blocks have certain storage capacities and, when filled, are closed and linked to the previously filled block, forming a chain of data known as the blockchain. All new information that follows that freshly added block is compiled into a newly formed block that will then also be added to the chain once filled. A database usually structures its data into tables, whereas a blockchain, as its name implies, structures its data into chunks (blocks) that are strung together. This data structure inherently makes an irreversible timeline of data when implemented in a decentralized nature. When a block is filled, it is set in stone and becomes a part of this timeline. Each block in the chain is given an exact timestamp when it is added to the chain. A Blockchain is a type of shared database that differs from a typical database in the way that it stores the information. As new data comes in, it is entered into a fresh block. According to the smart contracts, the application gets to know the user's default account whenever the required data is entered, the application works according to the smart contracts and sends tokens to the destined account and then the transaction will be recorded on the blockchain as blocks and can be viewed later.

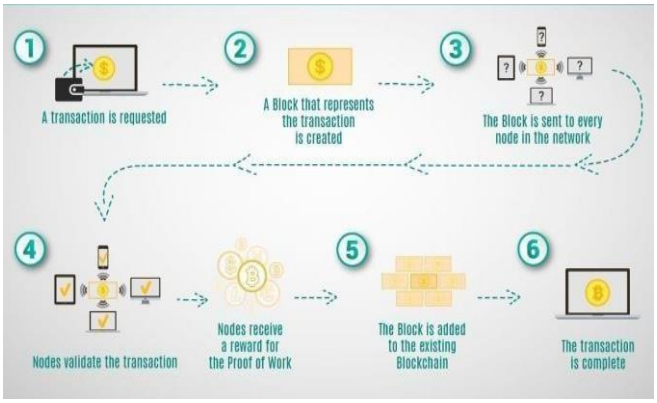


Fig [1]: How Block Chain Works

Once the block is filled with data, it is chained onto the previous block, which makes the data chained together in chronological order. Different types of information can be stored on a blockchain, but the most common use so far has been as a ledger for transactions. In Bitcoin's case, blockchain is used in a decentralized way so that no single person or group has control—rather, all users collectively retain control. Decentralized block chains are immutable, which means that the data entered is irreversible. For Bit coin, means that transactions are permanently recorded and viewable to anyone.

has been asa ledger for transactions.In Bitcoin's case, blockchain is used in a decentralized way so that nosingle person or group has control—rather, all users collectively retain control. Decentralizedblockchains are immutable, which means that the data entered is irreversible. For Bitcoin, means that transactions are permanently recorded and viewable to anyone.

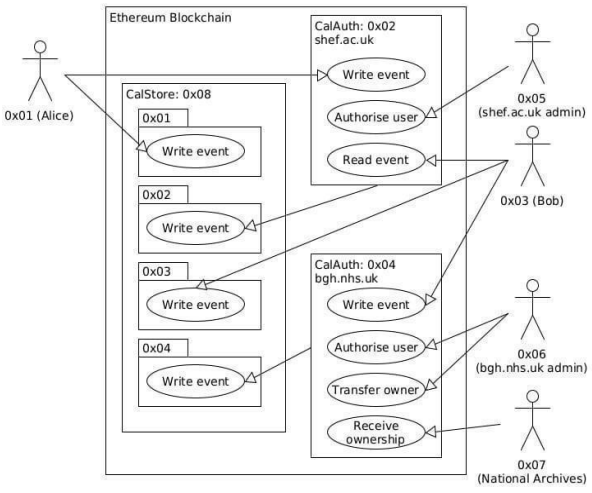
3. Cryptocurrency

A cryptocurrency is a digital or virtual currency designed to work as a medium of exchange. It uses cryptography to secure and verify transactions as well as to control the creation of new units of a particular cryptocurrency. Essentially, cryptocurrencies are limited entries in a database that no one can change unless specific conditions are fulfilled. A cryptocurrency (or "crypto") is a form of payment that can circulate without the need for a central monetary authority such as a government or bank. Instead, cryptocurrencies are created using cryptographic techniques that enable people to buy, sell or trade them securely. Cryptocurrencies can be exchanged for goods and services, though they often are used as investment vehicles. Cryptocurrency is also a key part of the operation of some decentralized financial networks, where digital tokens are an important tool for carrying out transactions. About 16,000 different cryptocurrencies are traded publicly, according to CoinMarketCap.com, a market research website. And cryptocurrencies continue to proliferate. The total value of all cryptocurrencies on Dec. 23, 2021, was about $2.3 trillion, having fallen off an all-time above $ 2.9 trillion weeks later.

4. Existing System

Traditional databases use client-server network architecture. Here, a user (known as a client) can modify data, which is stored on a centralized server. . Control of the database remains with a designated authority, which authenticates a client's credentials before providing access to the database. Since this authority is responsible for the administration of the database, if the security of the authority is compromised, the data can be altered, or even deleted. Blockchain databases consist of several decentralized nodes. Each node participates in administration. all nodes verify new additions to the blockchain and are capable of entering new data into the database. For an addition to be made to the blockchain, the majority of nodes must reach a consensus. This consensus mechanism guarantees the security of the network, making it difficult to tamper with.

5. Proposed System:



A decentralized application that is utilizing the latest advancing technology is called. Blockchain allows us to perform the actions you would do every day like transferring money without a trusted third party in a secure way. Since a Blockchain is a permanent record of transactions that are distributed, every transaction can

irrefutably be traced back to exactly know the details of the time it was done and the amount transferred without revealing the owner's identity. In addition, past transactions cannot be changed, while the present can't be manipulated, because every transaction is verified by every single node in the network and any outside or inside attacker must have control of 51% of the nodes to alter the record.

6. Architecture

The initial The initial excitement about block chain technology was about enabling peer–to–peer transfers of digital currency to anybody in the world, crossing human-created boundaries (such as the borders of countries) without any intermediaries such as banks. This excitement was further heightened by the realization that this peer–to–peer capability could be applied to other, non-crypto currency types of transactions. These The initial excitement about blockchain technology was about enabling peer–to–peer transfers of digital currency to anybody in the world, crossing human-created boundaries (such as the borders of countries) without any intermediaries such as banks. This excitement was further heightened by the realization that this peer–to–peer capability could be applied to other, non-crypto currency types of transactions.

There are three levels of programming:

Protocol-level Programming:

This level involves software that is needed for the deployment and operation of the blockchain itself. This software is similar to your operating system or networking software. If you are a system programmer and administrator, you'll program at this level. This text does not cover protocol-level programming.

Smart contract-level Programming:

One level above is smart contract programming. It is at this level that you design and program the rules for verification and validation, and specify the data and messages that are to be recorded on the underlying blockchain. The smart contract is the engine that drives the blockchain on behalf of the user application.

Application-level Programming:

This level of programming uses web application frameworks and user interface design concepts that are outside the blockchain protocol. Dapps embed a significant code element that of smart contracts. For any given smart contract, an extra copy of the smart contract's code is participant nodes of a blockchain network.

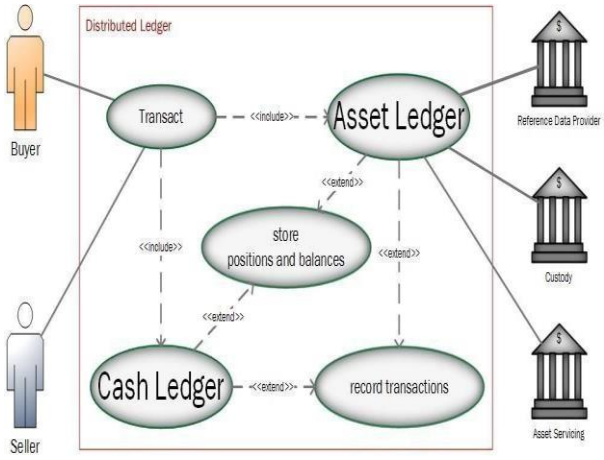


Fig [4]: Distributed Ledger

A SC has a state – permanently stored in Blockchain storage variables. The main characteristic of the SCs is that they run in an isolated environment. The program results must be the same whatever node they run in, so, they cannot access the external world (that changes with time); they can only access and send messages to the Blockchain itself (that is immutable). On the contrary, computer programs continuously interact with the external world. Moreover, once a SC is deployed on the Blockchain, it is there forever – it cannot be undone or erased. In Ethereum, SCs are created by special transactions; they can use other SCs, or inherit from other SCs. Creating a SC and changing its state costs GAS, which must be paid in Ether (the cryptocurrency associated to Ethereum Blockchain). A SC is endowed of public functions, that can be called after its creation (call of the constructor), or using a transaction (message call). A SC can be endowed of Ethers and can send Ethers to other SC, or to Ethereum addresses. A SC, upon a call of one of its functions, can change its state, can create and send a transaction to an address or to another SC, can call one or more of its functions, and can return a value without changing its state or sending a transaction – in this case, there is no cost for sending the message. A SC cannot initiate an action autonomously (for instance at given times), or access the external world. When developing BOS, we develop a complete system that is used by its customers, who typically do not care whether the system is based on a Blockchain or not. A BOS system is typically composed of two parts:

- A traditional software system, running on servers and/or on mobile devices, communicating with users and external

devices;

- The SCs running on the Blockchain.

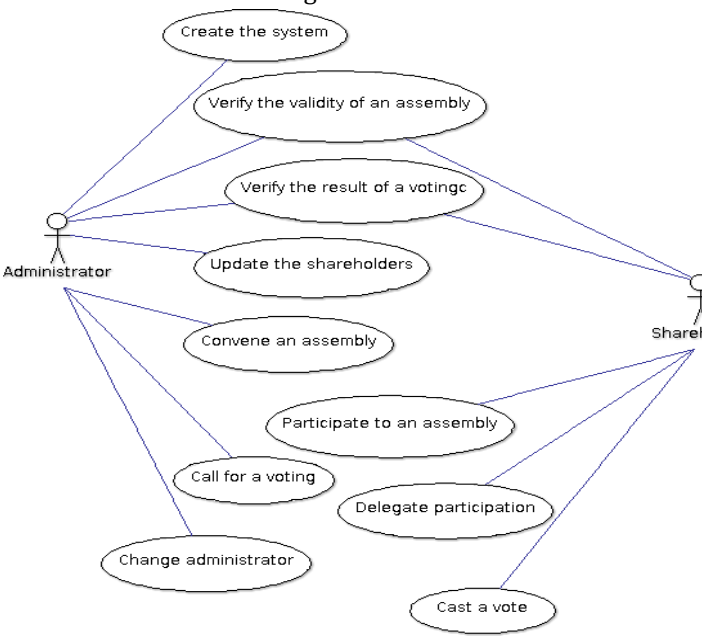


Fig [5]: The User Stories of the System Specifications

Here we have no room to show the USs in detail. Instead, we show the UML class diagram derived by an analysis of the given USs. Again, this diagram is not bound to a specific implementation of the voting system, but just shows the entities, the data structures and the operations emerging from the USs of Fig [5].

7. Future Scope:

Thesystemwillprovidebetterandefficientsolutionto current financialtransaction. Thiswillprovide safe and secure mode of transferring one's money to others without any hiccups. Despite the huge effort presently ongoing in developing DApps, software engineering practicesare still poorly applied in software development of BOS. The field is in fact still in its infancy,andtoolsortechniques formodelingand managingthepeculiaritiesasoftwaredevelopermustfacewh endealingwithBlockchainOrientedsoftwaresystemsarestill matterforresearchers. Tools andtechniques of traditionalsoftware engineeringhave notyetbeen adaptedandmodified to adhere to this new software paradigm. A sound software engineering approachmightgreatly helpin overcomingmany of theissuesplaguingBlockchaindevelopment providing developers with instruments similar to those typically used in traditional softwareengineering to afford architectural design, security issues, testing planes and strategies and toimprove software quality and maintenance. Researchers in soft- ware engineering have a bigopportunity to start studying a field that is very important and brand-new exploiting concepts,tools, instruments and ideas already consolidated in software engineering and changing andadaptingthemtothisnewsoftwaretechnology.

8. Conclusion:

The system can be equipped with additional features like:

- Addingblockchaintothepresentscenario.
- Makingtheapplicationmorefeasible.
- Changingthesmartcontractandmakingmore efficient.
- Willbedeployingitonthecloudusing SASS.

9. References:

[1] 21.CO.Bitnodes. https://bitnodes.21.co/. Accessed June 2017

[2] Apostolaki, M., Zohar, A., Vanbever, L.: Hijacking bitcoin: routing attacks on cryptocurrencies. arXiv preprint arXiv:1605.07524 (2016)

[3] Benben Team. Benben. http://benben.com.gh/. Accessed Oct 2016

[4] Biryukov, A., Khovratovich, D., Pustogarov, I.: Deanonymisation of clients in Bitcoin P2P network. In: Proceedings of the ACM Conference on Computer and Communications Security (CCS), pp. 15–29 (2014)

[5] BitcoinCommunity. Bitcoin source. https://github.com/bitcoin/bitcoin. Accessed June 2017

[6] Bitcoin Community. Protocol rules. https://en.bitcoin.it/wiki/Protocol_rules. Accessed June 2017

[7] Bitcoin Community. Protocol specification. https://en.bitcoin.it/wiki/Protocol_specification. Accessed June 2017

[8] Blockchain Info Team. Blockchain Info. https://blockchain.info/. Accessed May 2017

[9] BlockTrail Team. Blocktrail API. https://www.blocktrail.com/api/docs#api_data. Accessed Apr 2017

[10] Buterin, V.: Critical update re: DAO vulnerability. https://blog.ethereum.org/2016/0

6/17/critical-update-re-dao-vulnerability/. Accessed Apr 2017

BIOGRAPHIES

[1]Dr.Chaitanya Kishore Reddy. M is currently Working as a professor in the Department of Information Technology Pothavarappadu, Agiripally, Krishna(dist), India. He received Ph.D. in Computer Science and Engineering and M.Tech in Computer science and Engineering at Jawarlal Nehru Technology university, Kakinada. He published 40 research papers in various National and International Journals and International Conferences. He is a member in ISTE, CSI, and IAENG. His research areas are in Mobile Ad-hoc Networks, IoT, and Cloud Computing.

[2]Kommu Keerthana currently studying B.Tech with specification of Information Technology in NRI Institute of Technology. She is a member of IAENG. She completed her internshipat NRI Institute of Technology on Google forms, Web development. She participated in fest at JNTUK.She also published a paper on "Sentiment Analysis on Tweets" in journal of "InterdisciplinaryCycle Research" with an impact factor 6.2.

[3]P.Padma Soumya currently studying B.Tech with specification of Information Technology in NRI Institute of Technology. She is a member of IAENG. She completed her internship at NRI Institute of Technology on Google forms, Web development. She also published a paper on "Sentiment Analysis on Tweets" on journal of "interdisciplinary Cycle Research" with an impact factor 6.2.

[4]K Vijay Kumar currently studying B.Tech with specification of Information Technology in NRI Institute of Technology. She is a member of IAENG. He completed his internship at NRI Institute of Technology on Google forms, Web development. He also published a paper on "Sentiment Analysis on Tweets" on journal of "interdisciplinary Cycle Research" with an impact factor 6.2.