International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 07 | July - 2022 Impact Factor: 7.185 ISSN: 2582-3930

DIGITAL ASSETS MANAGEMENT USING BLOCKCHAIN AND SMART CONTRACTS

[1] Mrs.D.Maladhy, [2] K.Bharathkumar, [3]A.H.Abdul nasar, [4] M.Aravind., [5] Mr. R.Vinoth kumar

[1,5]Asst. Professor, faculty of Information Technology, Rajiv Gandhi college of Engineering and Technology, Kirumampakam 607403.

[2,3,4] Department of Information Technology, Rajiv Gandhi college of Engineering and Technology, Kirumampakam 607403.

ABSTRACT :There is an immense need of a Proof of Delivery (PoD) of todays digital media and content, especially those that are subject to payment. Current PoD systems are mostly centralized and heavily dependent on a Trusted Third Party (TTP) especially for payment. Such existing PoD systems often lack security, transparency and visibility, and are not highly credible, as the TTP can be subject to failure, manipulation, corruption, compromise and hacking. Blockchain is used to create a decentralized solution. Utilizing blockchain's immutable and tamper-proof logs, accountability and auditability can be easily achieved. Ethereum which makes blockchain a programmable distributed ledger is used in our implemented solution to create a PoD solution for the digital media. The solution uses a smart contract to allow customers to request the content and be uniquely identified using Cryptographic Hash derived by Sha3 in Ethereum Blockchain. Our solution includes off-chain secure download activity involving the file server and the customers.

KEYWORDS: blockchain, etherum, digital content,smart contract, proof of delivery ,ethereum explorer

INTRODUCTION : A blockchain is a public database that is updated and shared across many computers in a network. Block refers to data and state being stored in consecutive groups known as blocks. If you send ETH to someone else, the transaction data needs to be added to a block to be successful. Chain refers to the fact that each block cryptographically references its parent.

In other words, blocks get chained together. The data in a block cannot change without changing all subsequent blocks, which would require the consensus of the entire network. In the Ethereum universe, there is a single, canonical computer called the Ethereum Virtual Machine, or EVM whose state everyone on the Ethereum network agrees on. Everyone who participates in the Ethereum network (every Ethereum node) keeps a copy of the state of this computer. Additionally, any participant can broadcast a request for this computer to perform arbitrary computation. Whenever such a request is broadcast, other participants on the network verify, validate, and carry out the computation. This execution causes a state change in the EVM, which is committed and propagated throughout the entire network. Requests for computation are called transaction requests; the record of all transactions and the EVM's present state gets stored on the blockchain, which in turn is stored and agreed upon by all nodes. Cryptographic mechanisms ensure that once transactions are verified as valid and added to the blockchain, they can't be tampered with later. The same mechanisms also ensure that all transactions are signed and executed with appropriate permissions.

With the ease and the advancement of communication nowadays, anyone can be a creator. In today's digital ecosystem, any digital content can be copied and distributed without loss of quality. The existing digital rights management system has not substantially reduced copyright infringements.

To track the content uniqueness and ownership we implementing a new decentralized system for registration, licensing and distribution of digital content using a blockchain solution. The execution of the system is taking place without the involvement of intermediaries. The solution utilizes the key features of the blockchain technology, Ethereum smart contracts, as well as the distributed ledger to achieve a decentralized, trusted, traceable, secure delivery of the digital content, with automatic payment and dispute handling.

BLOCKCHAIN: Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Each block in the chain contains several transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant's ledger. The decentralized database managed by multiple participants is known as Distributed Ledger Technology (DLT). Blockchain is a type of DLT in which transactions are recorded with an immutable cryptographic signature called a hash. Blockchain seems complicated, and it definitely can be, but its core concept is quite simple. A blockchain is a type of database. To be able to understand blockchain, it helps to first understand what a database is. A database is a collection of information that is stored electronically on a computer system. In databases, information or data is typically structured in table format to allow for easier searching and filtering for specific information.

Block explorers enable you to search for information on a particular blockchain. Block explorers are one of the most important tools in a crypto enthusiast's arsenal. They provide an online interface for searching a blockchain, and enable you to retrieve data about transactions, addresses, blocks, fees, and more. Each block explorer provides data about a particular blockchain, and the type of information included will vary depending on the architecture of the blockchain it serves.

ETHEREUM: Ethereum is a blockchain platform with its cryptocurrency, called Ether (ETH) or Ethereum, and its programming language, called Solidity. As a blockchain network, Ethereum is a decentralized public ledger for verifying and recording transactions. The network's users can create, publish, monetize, and use applications on the platform, and use its Ether cryptocurrency as payment. Insiders call the decentralized applications on the network "dapps." Ethereum is an open-source blockchain-based platform used to create and share business, financial services, and entertainment applications. Ethereum users pay fees to use dapps. The fees are called "gas" because they vary depending on the amount of computational power required. Ethereum has its associated cryptocurrency, Ether or ETH.

Ethereum is a permissionless, non-hierarchical network of computers (nodes) that build and come to a consensus on an ever-growing series of "blocks", or batches of transactions, known as the blockchain. Each block contains an identifier of the block that it must immediately follow in the chain if it is to be considered valid. Whenever a node adds a block to its chain, it executes the transactions therein in their order, thereby altering the ETH balances and other storage values of Ethereum accounts. These balances and values, collectively known as the state, are maintained on the node's computer separately from the blockchain, in a Merkle tree.Each node communicates with a relatively small subset of the network, known as its peers. Whenever a node wishes to include a new transaction in the blockchain, it sends the transaction to its peers, who then send it to their peers, and so on. In this way, it propagates throughout the network. Certain nodes, called miners, maintain a list of all of these new transactions and use them to create new blocks, which they then send to the rest of the network.Whenever a node receives a block, it checks the validity of the block and all of the transactions therein and, if valid, adds it to its blockchain and executes all of the said transactions. As the network is non-hierarchical, a node may receive competing blocks, which may form competing chains. The network comes to a consensus on the blockchain by following the "longest-chain rule", which states that the chain with the most blocks at any given time is the canonical chain.

This rule achieves consensus because miners do not want to expend their computational work trying to add blocks to a chain that will be abandoned by the network.

ETHER :Ether (ETH) is the cryptocurrency generated by the Ethereum protocol as a reward to miners in a proof-of-work system for adding blocks to the blockchain. It is the only currency accepted in the payment of transaction fees, which also go to miners. The block reward together with the transaction fees provides the incentive to miners to keep the blockchain growing (i.e. to keep processing new transactions). Therefore, ETH is fundamental to the operation of the network. Each Ethereum account has an ETH balance and may send ETH to any other account. The smallest subunit of ETH is known as a Wei and is equal to 10−18 ETH. Ether is often erroneously referred to as "Ethereum".Ether is listed on exchanges under the ticker symbol ETH.

SMARTCONTRACT: Self-executing,automate applications containing terms and conditions that execute on a blockchain Traditionally, when two parties enter into a contract, they utilize the services of a trusted third party to execute the agreement Smart Contracts are simple programs, running on a blockchain under predefined conditions without any third party A smart contract is a computer program or a transaction protocol that is intended to automatically execute, control, or document legally relevant events and actions according to the terms of a contract or an agreement. The objectives of smart contracts are the reduction of need in trusted intermediates, arbitrations, and enforcement costs, fraud losses, as well as the reduction of malicious and accidental exceptions. Vending machines are mentioned as the oldest piece of technology equivalent to smart contract implementation. 2014's white paper about the cryptocurrency Ethereum describes the Bitcoin protocol as a weak version of the smart contract concept as defined by computer scientist, lawyer, and cryptographer Nick Szabo. Since Ethereum, various cryptocurrencies support scripting languages which allow for more advanced smart contracts between untrusted parties. Smart contracts should be distinguished from smart legal contracts.

The latter refers to a traditional natural language legally-binding agreement which has certain terms expressed and implemented in machine-readable code Smart contracts were first proposed in the early 1990s by Nick Szabo, who coined the term, using it to refer to "a set of promises, specified in digital form, including protocols within which the parties perform on these promises". In 1998, the term was used to describe objects in the rights management service layer of the system *The Stanford Infobus*, which was a part of the Stanford Digital Library Project.

EXISTING SYSTEM: In the Existing Asset Management system search user request the content access to the data owner. The user will get the digital content once the data owner approves the access. A centralized system that lacks transparency and no automation profit distribution for the content download. The Existing system did not check for the content uniques for content creators while uploading.

ISSUES IN EXISTING SYSTEM : No Micropayment based pricing model . Lack of sales transparency with the current service providers.Piracy and copy rights infringements Issues. Profit distribution with the intermediaries

PROPOSED SYSTEM : This project platform allows the user (content creator) to add the content which in turn verifies the ownership of the content and adds it to the blockchain. The content ownership verification is automatically takes place whenever the user adds the content ledger using Smart Contract.This project uses the benefits of blockchain which allows any registered user can check the details of the content such as owner, data created, price, etc. When the user requests access to the content by paying the required amount, the smart contract fetches the data from the blockchain and is shared with the user. The owner gets paid for every download of its content.

BENEFITS OF PROPOSED SYSTEM :

- Micropayments for content
- Transparency
- High security
- Royalty distribution
- Elimination of Middleman

SYSTEM REQUIREMENTS

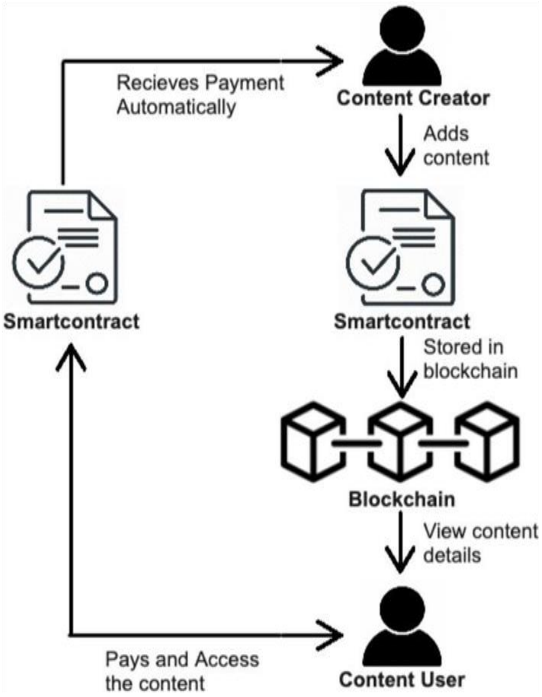
HARDWARE REQUIREMENTS :

- Processor Type : Pentium IV
- Speed : 2.4 GHZ
- RAM : 256 MB
- Hard disk : 20 GB

SOFTWARE REQUIREMENTS :

BLOCKCHAIN :	ETHEREUM
LANGUAGE :	SOLIDITY
FRONT END :	BOOTSTRAP
BACKEND :	JAVA

SYSTEM DESIGN :



MODULE DESCRIPTION

USER MODULE : The user module allows users to register, log in, and log out. Users benefit from being able to sign on because this associates content they create with their account and allows various permissions to be set for their roles. The user module supports user roles, which can be set up with fine-grained permissions allowing each role to do only what the administrator permits. Each user is assigned one or more roles. By default there are three roles: anonymous (a user who has not logged in) and authenticated (a user who is registered), and administrator (a signed-in user who will be assigned site administrator permissions).

Users can use their own name or handle and can fine-tune some personal configuration settings through their individual account page. Registered users need to authenticate by supplying their username and password, or alternately an OpenID login.

A visitor accessing your website is assigned a unique ID, the so-called session ID stored in a cookie. For security's sake, the cookie does not contain personal information but acts as a key to retrieving the information stored on your server.

FILE MODULE : File module is used to deal with the files, directories, and symlinks. You can create or get the file details form Blockchain Ledger through file module. The File module enables you to upload and attach files to content and to manage these uploads if you have the appropriate permissions.

This module is responsible for validating file content and managing uploaded files. It also provides options for displaying file content.As a site administrator, you will be able to control what type of files can be uploaded and their maximum size. The File module provides its functionality by defining a File field type for the field module.

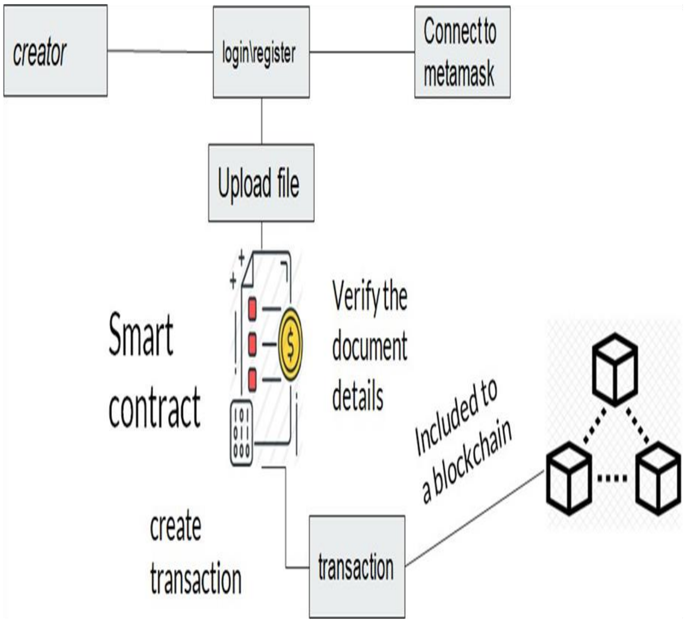
CUSTOMER EXPLORER : The public ledger stores data such as Ethereum transactions, Ethereum wallet addresses and balances. By using a Ethereum block explorer, you can search through this data and find the relevant information you might need. There are multiple ways in which the Ethereum block explorer is vital during your cryptocurrency adventure.

●Transaction details

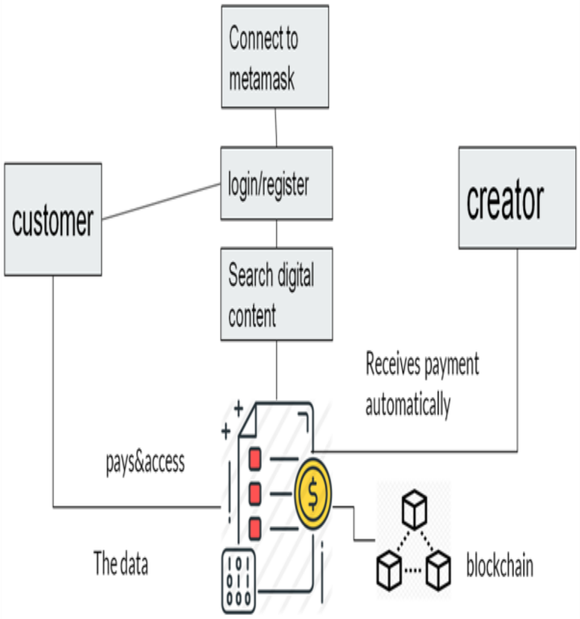
●Event websocket for smart contract

IMPLEMENTATION

CONTENT CREATOR : The content creator is used to register and login process and Connect to the metamask and the content creator upload the assets to the smart contract and the smart contract verify the document details and Create transaction and gives the payment details and the document included to a blockchain.

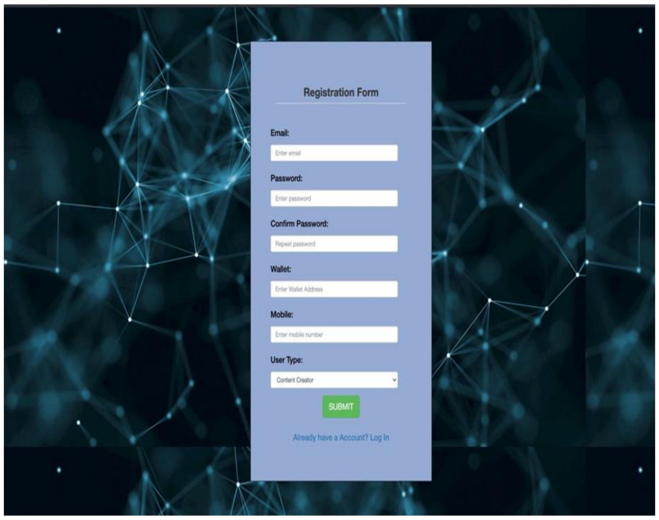


CONTENT CUSTOMER : The content customer used to register and login process and Connect to the metamask and the content customer search for the content they need and they download the smart contract verify the document details and Create transaction and gives the payment details and smart contract retrieve document from the blockchain.



SCREENSHOTS

REGISTRATION FORM :



Registration Form

Email: Enter email

Password: Enter password

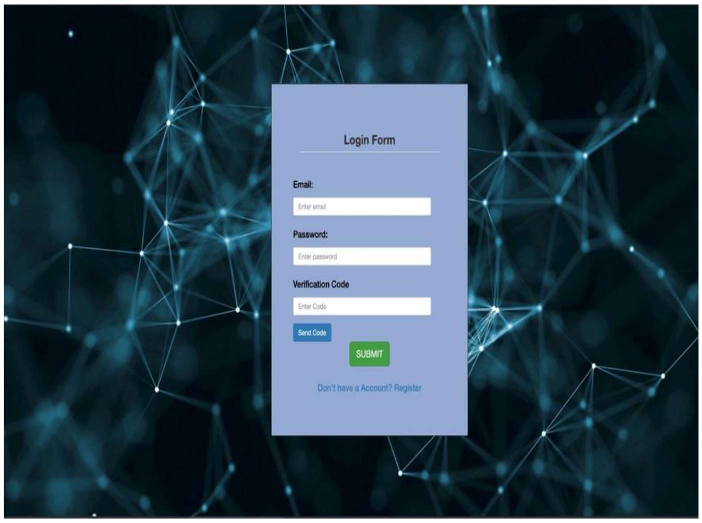
Confirm Password: Repeat password

Wallet: Enter Wallet Address

Mobile: Enter mobile number

User Type: Content Creator

LOGIN FORM :



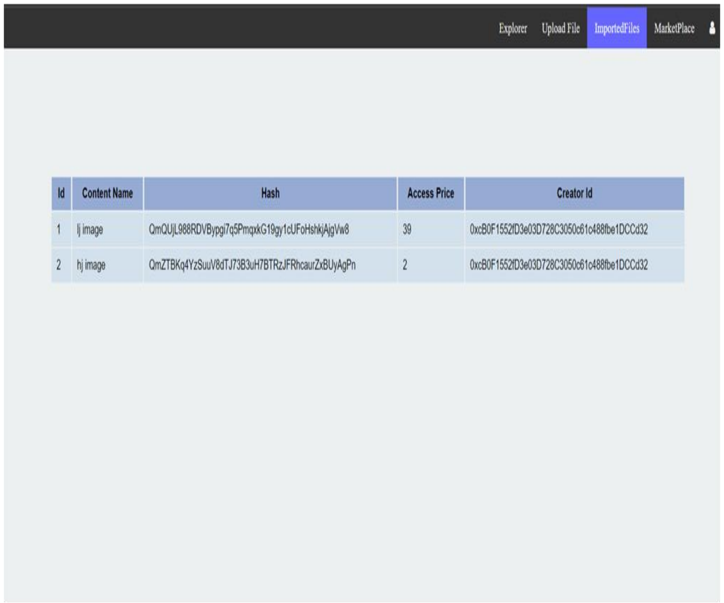
Login Form

Email:
Enter email

Password:
Enter password

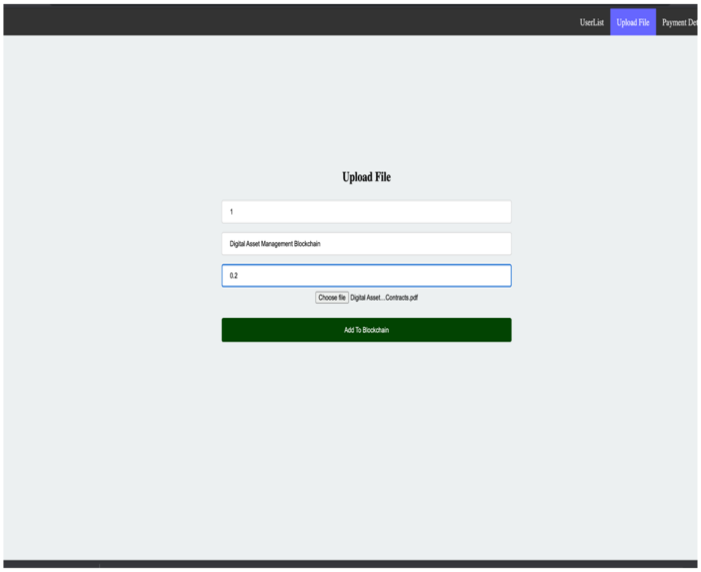
Verification Code
Enter Code

IMPORTED FILES :



Id	Content Name	Hash	Access Price	Creator Id
1	lj image	QmQUjL988RDVBypgi7q5PmqxkG19gy1cUFoHshkjAjgVw8	39	0xcB0F1552fD3e03D728C3050c61c488fbe1DCCd32
2	hj image	QmZTBKq4YzSuuV8dTJ73B3uH7BTRzJFRhcaurZxBUyAgPn	2	0xcB0F1552fD3e03D728C3050c61c488fbe1DCCd32

UPLOAD FILE :



Upload File

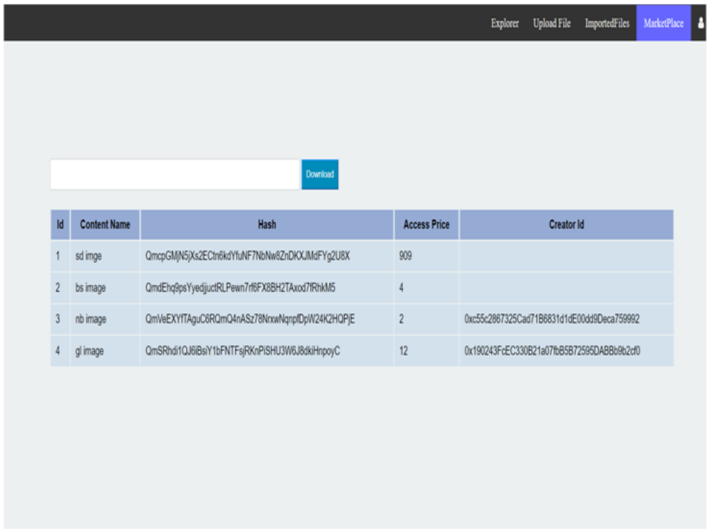
1

Digital Asset Management Blockchain

0.2

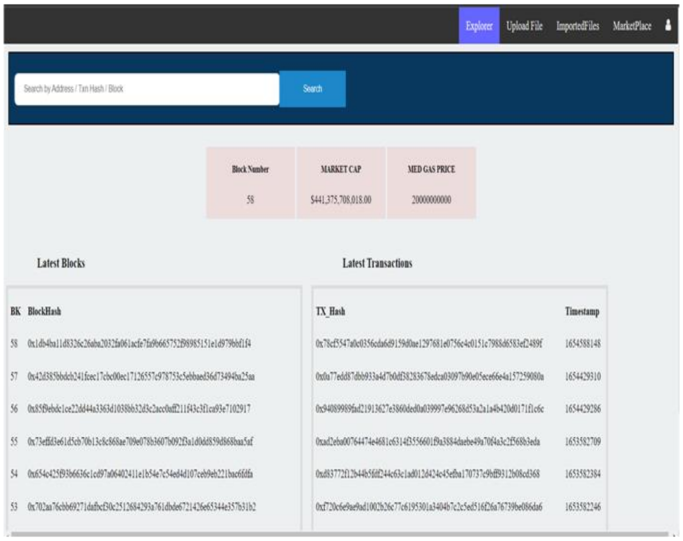
Choose file Digital Asset...Contracts.pdf

MARKET PLACE :



Id	Content Name	Hash	Access Price	Creator Id
1	sd imge	QmcpGMjN5jXs2ECtn6kdYfuNF7NbNw8ZnDKXJMdFYg2U8X	909	
2	bs image	QmdEhq9psYyedjjuctRLPewn7rf6FX8BH2TAxod7fRhkM5	4	
3	nb image	QmVeEXYfTAguC6RQmQ4nASz78NrxwNqnpfDpW24K2HQPjE	2	0xc55c2867325Cad71B6831d1dE00dd9Deca759992
4	gl image	QmSRhdi1QJ6iBsiY1bFNTFsjRKnPiSHU3W6J8dkiHnpoyC	12	0x190243FcEC330B21a07fbB5B72595DABBb9b2cf0

EXPLORER :



Block Number	MARKET CAP	MED GAS PRICE
58	$441,375,708,018.00	2000000000

Latest Blocks

BK	BlockHash
58	0x1db4ba11d8326c26aba2032fa061acfe7fa9b665752f98985151e1d979bbf1f4
57	0x42d385bbdcb241fcec17cbc00ec17126557c978753c5ebbaed36d73494ba25aa
56	0x85f9ebdc1ce22dd44a3363d1038bb32d3c2acc0aff211f43c3f1ca93e7102917
55	0x73effd3e61d5cb70b13c8c868ae709e078b3607b092f3a1d0dd859d868baa5af
54	0x654c425f93b6636c1cd97a06402411e1b54e7c54ed4d107ceb9eb221bac6fdfa
53	0x702aa76cbb69271dafbcf30c2512684293a761dbde6721426e65344e357b31b2

Latest Transactions

TX_Hash	Timestamp
0x78cf5547a0c0356eda6d9159d0ae1297681e0756c4c0151c7988d6583ef2489f	1654588148
0x0a77edd87dbb933a4d7b0df38283678edca03097b90e05ece66e4a157259080a	1654429310
0x94089989fad21913627e3860ded0a039997e96268d53a2a1a4b420d0171f1c6c	1654429286
0xad2eba00764474e4681c6314f3556601f9a3884daebe49a70f4a3c2f568b3eda	1653582709
0xd83772f12b44b5fdf244c63c1ad012d424c45efba170737c9bff9312b08cd368	1653582384
0xf720c6e9ae9ad1002b26c77c6195301a3404b7c2c5ed516f26a76739be086da6	1653582246

CONCLUSION : In this thesis, we proposed a new framework, named Digital Asset Management Using Blockchain, that can give the license pattern for digital content creators. And it makes the system decentralized which allows any user to preview the content. Fully automated functionality using smart contracts which eliminate middleman operation and eliminates human error.

The decentralization, auto-enforcing ability, and verifiability characteristics of smart contracts enable their encoded business rules to be executed in a peer-to-peer network, where each node is "equal" and none has any special authority without the involvement of a trusted authority or a central server. Thus, smart contracts are expected to revolutionize many traditional industries, such as financial, healthcare, energy, etc. Next version of this project will be developed in the future to improve the Digital Asset Management system.

REFERENCE :

[1] Alharby M, Aldweesh A, van Moorsel A (2018) Blockchain-based smart contracts: A systematic mapping study of academic research (2018). In: 2018 International Conference on Cloud Computing, Big Data and Blockchain (ICCBB), IEEE, pp 1–6

[2] Atzei N, Bartoletti M, Cimoli T (2017) A survey of attacks on ethereum smart contracts (sok). In: International Conference on Principles of Security and Trust,Springer, pp 164–186

[3] Bogner A, Chanson M, Meeuw A (2016) A decentralised sharing app running a smart contract on the ethereum blockchain. In: Proceedings of the 6th International Conference on the Internet of Things. Association for Computing Machinery, New York, pp 177–178

[4] H. Hasan and K. Salah, "Blockchain-based Solution for Proof of Delivery of Physical Assets," International Conference on Blockchain (ICBC), Seattle, USA.

[5] P. Treleaven, R. G. Brown, and D. Yang, "Blockchain technology in finance,"Computer, no. 9, pp. 14–17.