Collaborations with Smart contracts using Blockchain

ANAS BIN YAHIYA QURESHI[*1], SAFI UR RAHMAN PASHA[*2], MOHAMMED SAMEER[*3], Dr. MOHAMMED ABDUL BARI [*4]

[*1] *BE Student, Dept. of Computer Science Engineering, ISL Engineering College*
[*2] *BE Student, Dept. of Computer Science Engineering, ISL Engineering College*
[*3] *BE Student, Dept. of Computer Science Engineering, ISL Engineering College*
[*4] *HOD & Associate Professor, Dept. of Computer Science Engineering, ISL Engineering College*

ABSTRACT: After the 2020 pandemic, everyone realized that the collaborations which were being done offline had to go online. This created a stir among the community as there was no legal bond between the two entities working together. Be it a large company working for another one or an individual working as a contractor. Smart contracts are computer protocols intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts have a broad range of applications, such as financial services, prediction markets, and Internet of Things (IoT), etc. In this paper, we propose how we use blockchain technology and utilize the built-in feature of the blockchain technology called smart contracts to create an agreement between two entities which is then automatically executed/initiated whenever the conditions or the requirements of the contract are met. This makes everything transparent between the contractors which in turn eliminates the need for a third person to testify or the need of depending and trusting the contractor or anyone. This also creates micro-collaborations much easier as it saves time and money spent behind a lawyer to register a company for a trivial collaboration. Smart contracts can be made based on the requirements. This is a decentralized application built using react and solidity.

I. INTRODUCTION

Contracts are used in many ways in today's day and age which is just putting the agreed terms and conditions agreed by both the parties on a document that validates the agreement and works in the legal courtroom. A professional is required who is certified to create the agreement and document it. But in case you're not able to reach out to them, it is not possible to do so. Our venture aims to deal with instances like these. We used the built-in feature of blockchain technology called smart contracts to create an agreement. We developed a payment split smart contract that splits payments among the participants based on the percentage of shares. We also enabled the option to upload an existing contract which is then on the blockchain and is not susceptible to loss or changes unless it involves everyone participating in the contract.

II. PROBLEM STATEMENT

During the pandemic, the majority of the population was confined to their homes to prevent the disease to spread further. This made businesses and individuals suffer as it was hard to get in touch with a lawyer or to trust someone to pay their bills. Trusting just words without any document is hard and not possible. Usage of Ethereum's network to create a dynamic smart contract that enables people to create a payment splitter and for those who want to upload their smart contracts on the blockchain to maintain the integrity of the document and for it to be out there for future legal purposes if the need arises

III. EXISTING SYSTEM

1. Websites exist where user can upload an image to the blockchain network as an NFT or Non-Fungible Tokens.
2. The images are tokens placed on the marketplace to be traded and are auctioned to the highest bidder if it is more than the asking price.
3. Payments are processed through a payment gateway which is based on the blockchain network used.

3.1 Disadvantages

1.Most approaches with the uploading documents are made for auctioning the token which is a security vulnerability in this case as the documents to be uploaded contains confidential information and is widely available for the public to view.
2. The payment gateway does not have any feature for splitting the payment

IV. PROPOSED SYSTEM

A blockchain is essentially a distributed digital ledger of transactions [2] that encompasses the whole network of computers. It is dispersed, which means it does not require a central authority to function. Bitcoin was the first cryptocurrency to leverage blockchain technology. Leveraging this technology, we can implement a system that provides ease of Contract creation between users and also provide Transfer of assets between users. As Blockchain is Immutable, Data present can hold a value which in turn helps companies to maintain a solid track of their history. An End-to-End contract between an Employee and company can be formed which is accepted by both parties and eliminates the interference of any third party for verification purposes as Blockchain is a Public Ledger. Government Can use this data to keep track of Property sale deeds for taxation purposes and Users can also use this

platform for buying and selling Property documents and transferring ownership of land assets in real life. This helps users avoid visiting Registration offices and going through a load of paperwork with the help of blockchain technologies. All transactions are done using Cryptocurrencies which makes transactions substantially secure and faster. We are also implementing a payment splitter method which is essentially a contract that allows splitting Ether payments among a group of accounts. The sender does not need to be aware that the Ether will be split in this way since it is handled transparently by the contract. The split can be in equal parts or any other arbitrary proportion. The way this is specified is by assigning each account to a number of shares. Of all the Ether that this contract receives, each account will then be able to claim an amount proportional to the percentage of total shares they were assigned

4.1 Advantages

1. Confedentiality
2. Easy payments

V. SYSTEM ARCHITECTURE

A. Blockchain

Bitcoin uses the "proof of work" [4] technique to reach a consensus on transaction data in a distributed system, as explained by Nakamoto. Blockchain is a distributed, attached-only database that keeps track of a list of data items connected and safeguarded via cryptographic methods [5]. Blockchain technology solves the long-standing Byzantine problem, which was formerly solved by a huge network of dishonest people. Because any changes to the recorded data invalidate all subsequent data, the blockchain's shared data becomes immutable once it has been authenticated by the majority of nodes. Ethereum is the most commonly used blockchain platform in NFT schemes because it provides a secure environment for smart contract execution.

B. Ethereum

Ethereum is a community-run technology software platform that allows for the creation and deployment of hundreds of decentralized apps. Blockchain technology underpins Ethereum. It's a blockchain with a Turing-complete programming language built right in. It has an abstract layer that allows users to design their ownership, transaction formats, and state transition techniques. Smart contracts, which are a collection of cryptographic rules that are only executed if specified terms are met, are used to do this [6]. Furthermore, a platform like this serves as the foundation for a virtual currency called Ether, which is a financial asset used on the Ethereum blockchain. In some ways, Ether serves as the fuel for Ethereum's distributed applications. This currency can be used to pay money to other accounts or machines that do specific tasks. As a result, Ether may be used to run decentralized apps, construct smart contracts, produce tokens, and conduct regular peer-to-peer payments. Ethereum is hence referred to as "programmable currency" [7]. EOA and Contract are the two components of Ethereum. A private key controls the EOA, whereas contract accounts are controlled by contract code. Nonce, ether balance, contract code hash, and storage root are the four components of an account.

C. Smart contracts

Szabo first proposed smart contracts as a way of speeding up, validating, and executing digital agreements. Ethereum is a Blockchain platform that uses powerful smart contracts. Smart contracts on the blockchain make use of To ensure ultimate consistency, Turing-complete scripting languages and stringent state transition replication through consensus methods are used to conduct complex tasks. Smart contracts allow unidentified parties and dispersed participants to perform fair transactions without the use of a trusted third party, and they also provide a consistent framework for developing applications in a variety of industries. State-transition methods help apps that run on top of smart contracts. All users have access to the states holding the instructions and parameters, ensuring that the instructions are followed to the letter. Furthermore, state assignments between distant nodes must remain consistent, which is critical for consistency. To support order-sensitive executions, the majority of NFT systems use smart contract-based blockchain platforms.

D. ERC-721 Standard

The ERC-721 sets a standard for NFT, which means that this type of Token is unique and might have a different value than another Token from the same Smart Contract, for example, due to its age, rarity, or even its visual appearance. The ERC-721 (Ethereum Request for Comments 721) is a Non-Fungible Token Standard that implements an API for tokens within Smart Contracts, as suggested by William Entriken, Dieter Shirley, Jacob Evans, and Nastassia Sachs in January 2018. It has features like transferring tokens from one account to another, getting an account's current token balance, finding the owner of a certain token, and seeing the entire supply of a token on the network. It also has some other features, such as approving the transfer of a certain quantity of tokens from one account to a third-party account. An ERC-721 Non-Fungible Token Contract is a Smart Contract that implements the following methods and events and is responsible for keeping track of the produced tokens on Ethereum once deployed.

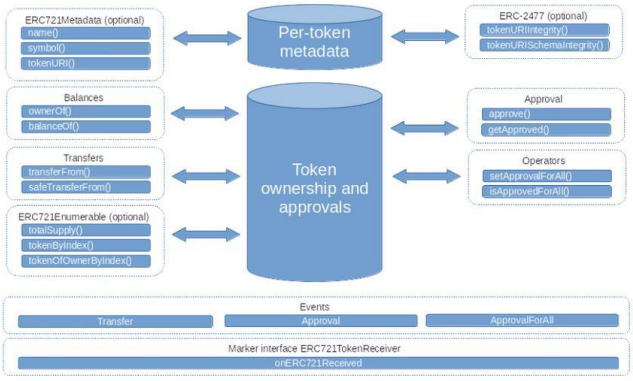

Fig: ERC 721 working.

E. Addresses & Transactions

In cryptocurrencies, blockchain addresses and transactions are fundamental notions. A blockchain address is a unique identifier that allows a user to send and receive assets, similar to how a bank account works when using cash. It's made up of a string of alphanumeric characters that are generated by a pair of public and private keys. To send NFTs to another address(es), the owner must show that he or she has the right private key and use a valid digital signature. This simple activity is known as submitting a transaction to use the ERC-777 [8] smart contract standard and is commonly accomplished using a bitcoin wallet.

F. Encoding

The process of converting data from one type to another is known as encoding. Many files are frequently encoded in either efficient, compressed formats for memory conservation or uncompressed formats for high quality/resolution. Hex values are used to encode transaction components such as function names, arguments, and return values in popular blockchain systems such as Bitcoin [9] and Ethereum. This means that the actual NFT data must adhere to these guidelines. When someone asserts ownership of NFT-based intellectual property rights, they are essentially asserting ownership of the creator's original hex value chunk. Others are free to copy the raw data, but they cannot claim ownership. As a result, there may be an increase in NFT-related actions.

VI. CONCLUSION

In this paper, we planned and built a system wherein users can create smart contracts without any knowledge of solidity. Enabled the users to upload their contracts on the blockchain as an NFT and built a smart contract that splits their payment.

VII. REFERENCES

[1] C. Usman W, "Non-Fungible Tokens: Blockchains, Scarcity, and Value," Critical Blockchain Research Initiative (CBRI) Working
Papers, p. 14, 2021.
[2] S. a. G. G. Adhami, "Initial coin offerings: Tokens as innovative financial assets," in Contributions to Economics, Germany, Springer,2019, pp. 61-81.
[3] L. a. D. D. Baele, "Could cryptocurrencies contribute to a well-diversified portfolio for European investors?.," 2017.
[4] A. e. a. Gervais, "On the security and performance of proof of work blockchains.," in ACM SIGSAC conference on computer and
communications security, 2016.
[5] J. K. A. L. N. Garay, "The bitcoin backbone protocol with chains," in Lecture Notes in Computer Science, Springer, Cham, 2017, pp. 291-323.
[6] G. Wood, Ethereum: A secure decentralised generalised transaction ledger, 2014, pp. 1-32.
[7] N. Szabo, "Smart contracts: building blocks for digital markets," Journal of Transhumanist Thought,, 1996.
[8] D. J. B. T. S. Jacques, "Erc-777 token standard," 20 11 2017. [Online]. Available:https://eips.ethereum.org/EIPS/eip-777.
[9] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Manubot, 2019.
[10] C. T. Z. M. G. S. R. G. P. Ba, "The Effect of Cryptocurrency Price on a Blockchain-Based Social Network," in Studies in Computational Intelligence, 2020, pp. 581-592.
[11] V. V. B. Fabian, "Erc-20 token standard," 19 11 2015. [Online]. Available:https://eips.ethereum.org/EIPS/eip-20.
[12] R. e. a. Witek, "EIP-1155: Multi Token Standard," 17 06 2018. [Online]. Available: https://eips.ethereum.org/EIPS/eip-1155.
[13] V. e. a. Buterin, "A next-generation smart contract and decentralized application," 2014.
[14] E. D. S. J. E. N. S. William, "EIP-721: Non-Fungible Token Standard," 24 1 2018. [Online]. Available: https://eips.ethereum.org/EIPS/eip-721.
[15] W. e. a. Cai, "Decentralized Applications: The Blockchain-Empowered Software System," in IEEE, 2018.