ISSN No:-2456-2165

Making Legal Contract Smart Using Blockchain Technology

Shruti Gatkal, Pornima Borole, Anushka Kawale, Abhijit Mahajan
Computer Engineering at AISSMS College of Engineering,
Pune, Maharashtra, India.

Abstract:- **Blockchain is a peer-to-peer distributed ledger technology that makes the records of any digital asset transparent and immutable and works without involving a third party. Hence, it is independent of a third party and termed as 'decentralized'. Blockchain is an emerging technology and is gaining a lot of popularity, as it is scalable and also has the ability to manage risks. Blockchain is transforming the way value is exchanged, it has expanded technical capabilities to achieve a higher level of innovation and developer products. Blockchain is the most recent technology that can be adopted for data security. This paper aims to make any legal contracts, such as agreements, and property registries, as well as other assets in India using blockchain for solving issues like avoiding third parties, brokerage services, trusty transactions, etc. It makes it safer as well as non-repudiable. We are proposing a Web3 system that is providing a platform for both parties to make legal contracts using smart contracts and deploy it on blockchain to make safer contracts by inheriting blockchain properties. A smart contract is a digital contract that automatically executes the terms of an agreement by itself. In layman's terms, it is a computer code that holds the terms of a contract. It stores in decentralized, distributed public blockchain networks that contracting parties can access from anywhere and at any time. With these designs, this digital type of contract runs on blockchain nodes that cannot be changed. This makes the smart contract legal contracting decentralized, free of brokerage services as well paperless that is digital. This solution demands transparency, participation and cooperation society demands. Hence, would help to obstruct corruption and make government services more efficient.**

Keywords:- *Ethereum Blockchain, Smart Contracts, Machine Readable Legal Agreements.*

I. INTRODUCTION

A contract, simply, is a promise enforceable by law. The "Promise" could be to do something or to refrain from doing something. The creation of a contract requires the mutual assent of a couple of persons, one of them ordinarily making an offer and another accepting. If a person fails to hold up their side of the promise, the other is entitled to legal redress. There is a constant development of these contracts and they not only are a promise but also contain sensitive information about the parties involved in the contract. A secrecy or security should be maintained where sensitive information is involved. A lot of common and civil contracts like birth Certification, Home/Shop Rental Agreements, marriage Certification, etc. require a lot of time and effort, even though the outcome is a single paper or document it takes a lot of time to complete. A person in urgent need has no choice but to wait for the time period required for these traditional contracts to complete. Although this process is time taking, it is necessary as the validation of the information of contract and parties is necessary, if contracts are not monitored properly it can cause a lot of issues between common people and Businesses.

"Blockchain technology is an advanced database mechanism that allows transparent information sharing within a business network". Blockchain is an immutable, shared ledger that facilitates the process of recording transactions and keeping track of assets in a business network. The transactions that happen in a blockchain are duplicated and distributed across the entire network of computer systems on the blockchain. Virtually anything of value/asset, tangible(house, car, land) or intangible(patents, copyrights, branding) can be tracked and traded on a blockchain network which helps in reducing risk and cutting costs for all involved. Payments, accounts, production, etc. can be tracked on a blockchain. And as all members share a single view of the ledger, we can see all the details of a transaction end to end, which gives users greater confidence, as well as new efficiencies and opportunities. Blockchain can hold huge amounts of data which cannot be tampered with nor can it be altered. As it is decentralized and distributed technology, it maintains transparency and builds trust between the users.

A. How Blockchain works -

1. As each transaction occurs, it is recorded as a "Block" of data and these blocks can hold information like the transaction date&time, transaction data, previous block address, nonce, etc. and can hold other information according to the contract.
2. All the blocks are connected to the ones before and after it, this forms a chain formation which is why the name Blockchain. The blocks link securely together to prevent altering between two existing blocks.
3. The chain of blocks is irreversible and each attaching block strengthens the verification of the previous block and hence the entire blockchain. Due to this the possibility of tampering by a malicious actor.

B. Need of Smart Contracts -

1. A smart contract can be thought of as a system that releases digital assets to all or some of the involved parties once arbitrary pre-defined rules have been met. For instance, Alice sends X currency units to Bob, if she receives Y currency units from Carl.
2. Smart contracts unlike traditional paper contracts are automatically executed and the operations in it are carried out as required. The old traditional paper contracts rely on middlemen and third-party intermediaries for execution which is usually a time consuming and tiring procedure.
3. As smart contracts are automated procedures due to which interaction between parties is minimal and reduces administration cost.
4. A smart contract, once deployed, is immutable which means that it stays on the blockchain and can be executed when need be.
5. Compared to traditional contracts, smart contracts enable users to codify their agreements and trust relations by providing automated transactions without the supervision of a central authority.

C. Platforms for Smart Contracts -

Smart Contracts can be developed and deployed on various blockchain platforms like Ethereum, Bitcoin, etc. All these platforms provide distinctive features for developing smart contracts. These platforms provide developers with high level languages to develop these contracts.

1. Ethereum - The ethereum public blockchain is proposed and developed by Vitalik Buterin, it is a platform that can support advanced and customized smart contracts with the help of Turing-complete programming language. Ethereum smart contracts can be written in high-level languages like Solidity, Serpent and LLL which are stack-based bytecode languages and executed in Ethereum Virtual Machine(EVM). Ethereum is currently the most common platform for developing smart contracts.
2. Bitcoin - The bitcoin public blockchain was proposed by a group of individuals called Satoshi Nakamoto and is a platform that can be used to process cryptocurrency transactions but has a very limited compute capability. The bitcoin programming language has limited programming capabilities i.e. writing contracts with complex logic is not possible due to limitations.

We are introducing a new system in which the creation process of common and civil contracts is much faster and reduces the cost of drafting, checking and resolving disputes. The system is a Web Application that allows users or parties to create contract online hassle free and cost effectively. The data of the users will be stored in a database and will be used to create the contract.

II. MOTIVATION

According to our constitution, to make any type of legal contract in India we have to follow some predefined traditional process which is nowadays very hectic and inconvenient because we have to depend on lawyers and Notary offices. On the Other hand most of the conventional contracts are in paper format so there is considerable concern about their security and safety and also they are mutable and require third-party involvement.

To overcome all these issues and make contract-making smart and secure there is a technology called blockchain that can make it very secure and transparent. Smart contracts are fast and efficient and they don't need any third-party involvement so users don't have to rely on lawyers anymore. Also, smart contracts are in virtual formats stored on the decentralized Ethereum blockchain so it ensures integrity and availability.

Compared to conventional contracts, smart contracts are less expensive as they eliminate third-party involvement and the gas fee of one transaction is very less compared to conventional contracts. but the up to date government of India considers conventional contracts as legal as they are made based on Acts and Laws. The future of contracts could rely on making hybrid contracts, which would combine both the smart contract technology and the legality of traditional contracts.

III. RELATED WORK

A. Importance & Need

A contract is a commitment made between two or more parties that is enforceable by law. Once this contract is signed, each party promises to uphold the rights and obligations outlined in it. In essence, every contract is built around a promise. A contract's primary function is to formally establish new ties and lay out the numerous legal obligations that each party has to the other. But nowadays these methods of contracts are not sure about maintaining confidentiality & integrity.

To overcome these threats digital contracts are introduced known as "smart contracts" are triggered automatically when certain criteria are satisfied and are maintained on a blockchain. One significant benefit of implementing smart contracts is the elimination of the need for intermediate services such brokers, agents, etc. to execute a transaction. It does not allow for human involvement in any transactions; the required programme code handles everything. As the data in the decentralized register cannot be lost or attacked online, it assures safety.

To reduce customer dependency on middle objects such lawyers, court dates & availability proposed system is needed to make contacts facility convenient & reliable. Nowadays, the Indian government is looking forward to accepting & embedded blockchain technology all over in the government system so this system has great future scope & contribution to make India digital.

B. Existing System & their Impact

There are multiple platforms to write smart contracts such as Ethereum, Steller, Cardano, etc. But to use these platforms users need to know the technical background of it. So, these platforms are not convenient for people from non-technical backgrounds. Our proposed system is intended to provide a platform for all users to make their contracts quickly & accordingly Indian constitution Act & law.

One existing system named "AccordProject" took one step forward in smart contracts building. They provide facilities to generate structured templates for any agreement using the smart contract concept & also provide the facility to write your own contracts, but as earlier mentioned this platform also needs users from a technical background. and this platform does not provide any Indian constitutional law authorization.

Therefore, till today there is not any existing platform that provides the facility to make legal contracts smart without which is designed according to Indian constitution Act & law and also easily accessible to non-technical people.

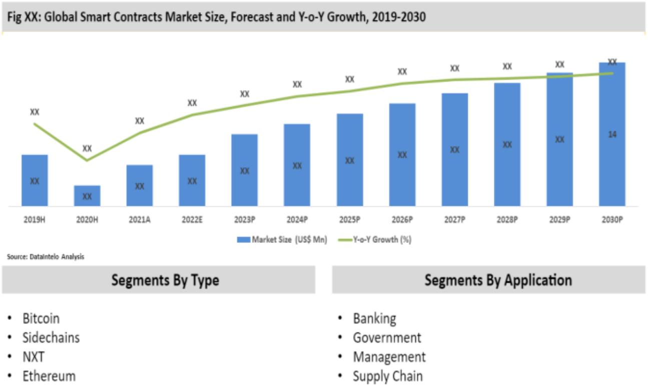

Fig.1. Smart Contract Evolution in Market

IV. IMPLEMENTATION

A. Basic system architecture -

The proposed system is a Web Application which will allow users to register and login to the system. All necessary information of the user will be requested during the registration, and to identify a user uniquely their aadhar number will be used which is unique to all and will be encrypted while storing into the system. Once the user has entered all their information and logged in they will be redirected to their respective Home page in the application.

The home page will contain navigation buttons to user profile and different types of contracts. If the user wishes to view or change any of their information they will be able to do so in the profile page of the application.

Different contracts that can be created on the system will be displayed on the home page and if a user wishes to create a contract they have to click on the particular contract and they will be redirected to the respective contracts page.

Once a user is on the contracts page they will have to fill in the necessary information and mention the people that will be involved in the contract. The people involved in the contract will receive a notification regarding the contract creation before it is deployed. Once all the participants accept the contract the creator of the contract can deploy it to the Blockchain. A final validation of the same contract will be done before deployment as once a Contract is deployed it can't be altered. If the user approves of the contract it will be deployed.

The user will be able to view all the contracts they have created or are a part of in the application. If the user wishes to get the contract in a virtual document form that option will also be provided in this section.

Traditionally every contract has a legal fee that has to be paid before we get the form, the user will have to pay a fee to create a contract which they will pay before contract creation.

All the success or failure messages regarding the system or contract creation process will be displayed to the user for a friendly and seamless process.

The frontend of the system will be built using Reactjs and the user data will be stored in the document database MongoDB. The Truffle suit will be used with Ganache to provide and interact with the Ethereum Blockchain. An alternative to truffle is Thirdweb which also can be used for interaction with the Ethereum Blockchain. Metamask will work as an intermediate between the Dapp and the Ethereum Blockchain for validating transactions. All the data required for the contracts will be fetched from MongoDB initially and then into the smart contract which will be deployed on the Ethereum blockchain. Solidity programming language will be used to write the smart contracts. The Application will be tested using the dummy ether accounts provided by ganache or using Thirdweb.

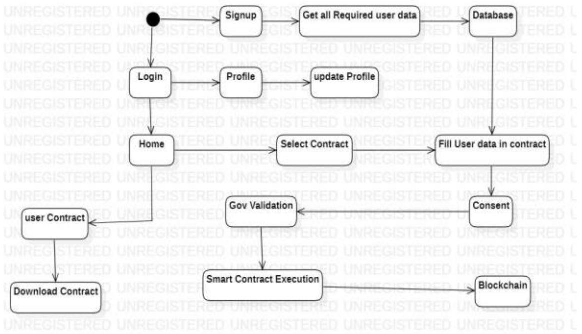

Fig.2. System Design

B. Technology and Tools -

1. Ethereum Blockchain - Ethereum is a decentralized public Blockchain which provides smart contract functionality to the developers. Ethereum runs it's smart contract on EVM(Ethereum Virtual machine). Ether is the currency used in the Ethereum Blockchain, Wei being the smallest unit of ether is used for paying gas fees and the transaction fees. As Ethereum is a public open source Blockchain it is ideal for our system.
2. Solidity - Solidity is a high level programming language used to write smart contracts in the Ethereum Blockchain. Solidity supports inheritance and complex data types which is necessary for developing complex systems. Solidity is designed to target the Ethereum Virtual machine. As Solidity is a bracket-pair language it has a syntax very similar to popular object oriented languages like Java and c++ which makes it easy to use and development friendly.
3. Truffle - Truffle is a development & testing environment for Blockchains using the Ethereum Virtual machine. It also allows the pipelining of assets using the EVM. Truffle has inbuilt smart contract compilation, linking, deployment and binary management. The truffle suit CLI makes it very easy to contact the smart contracts in our system. Truffle supports network management for deploying to any number of public and private Blockchain.
4. Ganache - Ganache is a personal/local Blockchain that runs on our system and provides rapid Ethereum and corda Blockchain development. Ganache has a GUI & CLI version which provides developers with a lot of options. Ganache provides free test ether accounts for development and testing. Truffle and ganache together give developers a Hassle free development experience which is ideal for creating complete and complex systems.
5. Metamask - Metamask is a browser extension that allows us to securely store our digital assets like crypto currency and make secure transactions. The metamask extension injects the web3 api into the browsers javascript context which allows Dapps to read from Blockchain. This allows the Dapps to receive and retrieve information from Blockchain and the transaction is validated and paid for through Metamask.
6. React.js - React is an open source frontend development library developed by facebook. Reactjs provides robustness and requires less code for development when compared to vanilla javascript. React provides components that can be reused in different parts of the system. Using react we can create interactive and single page web applications, which is why we will be using reactjs as a frontend for our application.
7. Mongodb - Mongodb is an open-source document database which provides easy storage and retrieval of information.

C. Algorithms and Concepts -

1. Cryptography - Cryptography is the practice of techniques for secure communication to safeguard from adversarial behavior. Cryptography helps us in having secure communication and prevent third parties from reading sensitive information. Cryptography usually works by scrambling plaintext(ordinary text) into ciphertext(encrypted text) then back again. For instance, if A sends a text to B the text initially will be plain text then it will be encrypted and sent to B, B will decrypt this text and will be able to see the original plain text.

There are two types of cryptography -

a. Symmetric-key - These encryption algorithms create a fixed size of bits called blocks. A secret key is also created and this key is used by the sender/creator to encrypt the data and the receiver uses it to decrypt the data. Ex - AES, DES.
b. Asymmetric-key - Asymmetric-key encryption also called public key encryption uses 2 keys for the process of encryption. A public key associated with the creator/sender for encryption and a private key that only the originator knows for decryption. The Ethereum blockchain uses the Asymmetric type of cryptography algorithm called the Keccak-256.

2. Keccak-256 - It is a Cryptographic function, a part of the SHA-3 family which computes an input to a fixed-length output, the output is a singular 32-byte hash regardless of the input size. This function is a part of Solidity and is a one direction function. Keccak-256 is used in the consensus engine called Ethash of the Ethereum blockchain. Compared to other cryptographic algorithms Keccak-256 produces small-sized cryptographic signatures, it is much stronger and faster compared to other algorithms.

V. FUTURE SCOPE & WORK

We have identified that blockchain technology provides many promising opportunities as well as applications for the future domain. Future work includes expanding our framework to support each type of statement and input. These upgrades would allow our framework to represent more such agreements. The future of digital transactions, business deals, communications, and modern life will likely carry the footmark of smart contracts. This blockchain-based technology is unwrapped opportunities not only for legal professionals but for graduates of blockchain degree programs as well. with consensus mechanisms, smart contracts, and modern cryptographic techniques has made it feasible for entities to communicate without the help of any central authority or mediator.

VI. CONCLUSION

Blockchain is an emerging area of research that has attracted rapidly growing attention. Decentralization, auto-enforcing and verifiability are the main characteristics of smart contracts that can be encoded in peer-to-peer networks, where every node has a special authority without the involvement of a centralized server or a third party. One of the major applications of smart contracts is to facilitate the executable codes, execute and then enforce the agreement between two parties. Currently, Ethereum is one of the most common blockchain platforms for developing smart contracts. We systematically searched for papers from different online databases in order to reach the desired solution. We extracted 20 papers. Based on the wide survey of decentralized applications, we have presented a way to implement smart contracts. In this research paper, we have presented a survey of blockchain-enabled smart contract solutions, the included research papers we categorized and discussed the existing smart contract-based studies. We have also included the implementation of the smart contract. Finally, the future scope and work of smart contracts were discussed.

ACKNOWLEDGMENT

This is a proposed system which has not been implemented yet. But this system wouldn't have been done without the support & availability of Smart contracts tools & Ethereum blockchain technology.

To make this system authorized in India, the system should follow the Indian constitution act & law, this wouldn't be possible without the Government's authorization & acceptance.

REFERENCES

[1]. F. S. Hardwick, R. N. Akram and K. Markantonakis, "Fair and Transparent Blockchain Based Tendering Framework - A Step Towards Open Governance," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018, pp. 1342-1347, doi: 10.1109/TrustCom/BigDataSE.2018.00185.https://ieeexplore.ieee.org/document/8456054

[2]. Rouhani S, Deters R (2019) Security, performance, and applications of smart contracts: A systematic survey. (IEEE Access7:50759–50779)

[3]. R. K. Kaushal, N. Kumar, S. N. Panda and V. Kukreja, "Immutable Smart Contracts on Blockchain Technology: Its Benefits and Barriers," 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2021, pp. 1-5, doi: 10.1109/ICRITO51393.2021.9596538.

[4]. X. Huang, C. Xu, P. Wang, and H. Liu, "LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem," *IEEE Access*, vol. 6, pp. 13 565–13 574, 2018.

[5]. V. Buterin, "A next-generation smart contract and decentralized application platform.," Available online at:https://github.com/ethereum/wiki/wiki/White-Paper/ [Accessed 19/02/2017].

[6]. V. Buterin, "On public and private blockchains," Available online at:https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ [Accessed 01/03/2017].

[7]. G. Wood, "Ethereum: A secure decentralized generalized transaction ledger," Ethereum ProjectYellow Paper, 2014.

[8]. H. Desai, K. Liu, M. Kantarcioglu, and L. Kagal, "Adjudicating violations in data sharing agreements using smart contracts," in 2018.IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), July 2018, pp. 1553–1560.[Online].Available:https://ieeexplore.ieee.org/document/8726492

[9]. Web3. Ethereum Foundation. [Online]. https://github.com/ethereum/web3.js

[10]. [1]Vishal G. Kartiki S. Rajendra J. " Smart Contract for Educational Digital Certificate using Blockchain"(IJSRD/Vol. 8/Issue 1/2020/253)

[11]. "Smart Contracts" : http://searchcompliance.techtarget.com/definition/smart-contract, 2017, [Online; accessed 4-Dec- 2017]

[12]. M. Raskin. The Law of Smart Contracts. https://ssrn.com/abstract=2842258, 22 September 2016 (last rev. 13 December 2016).

[13]. State of the DApps, 2020. [Online]. Available:http://stateofthedapps.com

[14]. Klaytn Mainnet: Cypress, The First Blockchain for Everyday Life,2020. [Online]. Available: https://www.klaytn.com/

[15]. V. Aleksieva, H. Valchanov and A. Huliyan, Application of smart contracts based on Ethereum Blockchain for the purpose of insurance services//Informatics and Innovative Technologies, pp.7-14, No1(1), 2019.