Scholarly Research Journal for Interdisciplinary Studies,
Online ISSN 2278-8808, SJIF 2018 = 6.371, www.srjis.com
PEER REVIEWED JOURNAL, JULY-AUG, 2018, VOL- 6/46

AN OVERVIEW OF BLOCKCHAIN AND SMART CONTRACTS AND ENHANCING IT WITH ARTIFICIAL INTELLIGENCE

Prathamesh Patil[1], Nikhil Rathaur[2], Chandra Bhanu Sahoo[3]

Department of Computer Engineering, STESs Sinhgad Academy of Engineering, Pune, Maharashtra, India

Abstract

As online transactions are getting more and more convenient with different media to perform them, their security issues are also rising and are becoming a prime concern for people. This is causing people to get attracted to newer media like the use of cryptocurrency and smart contracts instead of traditional methods. This paper is an overview of these concepts and ex-plains the basic concepts of how these things work, what are the drawbacks or limitations of these things and how these things could be used in the future.

***Keywords**: Blockchain, Smart Contract, Cryptocurrency*

Introduction

About 10 years ago sending money to someone was a time-consuming process, you would have to go to the bank and do a bunch of formalities and procedures and then wait for longer periods of time for the transactions to take place but today the scenario is entirely different. The world has har-nessed the power of the internet and used it to the fullest. Making a transaction like that has become so easy now that it can be done within just a few clicks here and there di-rectly through smartphones. It is human nature to explore and improve from the current state to a better state so nat-urally there will be further progress with these things. How will we progress further? The answer lies in concepts like blockchain and smart contracts. So what is a blockchain or a smart contract? Let's first see what a blockchain is. A blockchain is basically a data structure which is open to everyone who uses it. Basically, it is a chain of records of transactions linked in form of a chain that is one record will be dependant on the previous one and so on. This makes it secure as changing one record will mean that the previous record linked to it needs to be changed accordingly and one before that needs changes too and so on. So, the longer this chain will be the more secure it will become. Huge chains of data already exist in form of Bitcoin and other cryptocur-rency transactions. These data sets are so huge that no one particular person or organisation has the processing power to make changes to the entire chain so it can't be cheated or hacked. This is

the power of blockchain. Details on how the data is entered and accessed by users will be explained in further detail in the literature survey of the paper.

Now let's see what smart contracts are. Smart contracts are contracts which help execute traditional contracts faster by eliminating the need of a middleman to deal between two parties. A smart contract is basically a self-executing con-tract the contents of which can be stored in form of computer code which is stored in a blockchain network. This not only speeds up the process of deals but makes it transparent and more secure as it is running on the blockchain. Consider the example of selling a car. The buyer and the seller can com-municate online and make a deal and have it encoded into the blockchain. Now, a trigger event like receiving a cer-tain amount of cryptocurrency like Bitcoin can release the key to the buyer on a certain date which they agreed upon. With the help of the key, the buyer could go to the given location and access the car by using the key given to him. It's that simple, no middleman dealing with anything. The deal is simple and goes smoothly. This was the basic gist of what blockchain and smart contracts are. To understand the technical concepts that go behind implementing these is explained in further detail.

Overview of Blockchain

In 1991, Stuart Haber and W. Scott Stornetta worked on a system to cryptographically secure the chain of blocks in which document timestamps were made immutable by nature. The blockchain technology was first proposed in 2008 by a person (or group of people) identified by the pseudonym, Satoshi Nakamoto. A blockchain is a decen-tralized, distributed and a public digital ledger that is used to log a list of transactions across many nodes. By design blockchain is resistant to modifications, the record cannot be altered without the alteration of all subsequent blocks and the consensus of the network.

How do blockchains work? Each block in the blockchain contains a cryptographic hash of parent block, a timestamp, and transaction data, a block has only one parent block. The blockchain is managed using a peer-to-peer network and dis-tributed timestamping server. There are three main compo-nents behind the working of a blockchain: 1.Public and Pri-vate key cryptography 2.A distributed network that includes a shared ledger 3.Means to verify transactions and records in the network

A private key is a large randomly generated sequence of alphanumeric characters that gives the user access and con-

trol over their wallets. A private key is used to sign trans-actions that allow the user to transfer their cryptocurrency. Each user has a pair of private key and public key. As op-posed to the public key which is broadcasted out to the net-work, a private key is kept confidential. Blockchain wallet automatically generates a unique private key for each user. When a user transfers some funds from his wallet, the soft-ware signs the transaction with their private key without ac-tually disclosing it. The public key is used with a hash func-tion to generate the public address to which user can send or receive funds. Once the transaction is signed the miners use the sender's public key to ensure the digital signature is authentic, and if the ownership is confirmed they include the transaction in next block, and the money is sent from one wallet to another. Below functions depicts the process

: Sign(Transaction, Private Key) -¿ Digital Signature Ver-ify(Transaction, Public Key, Digital signature) -¿ True/False Security of the system depends on the fact that getting a public key from the private key is a one-way street, which means it is impossible to derive the private key from a pub-lic key likewise it is impossible to derive public key from the address. Only when a majority of nodes comes to a consen-sus that history and signature of a new transaction or an edit to an existing transaction are valid by executing algorithms, the new block of is inserted into the ledger and it is added to the chain. If the majority do not acknowledge the addition or modification of ledger entry, it is denied and not added to the chain of transactions. This allows block chain to run without the need for some central authority.

Types of blockchain networks: Currently, there are three types of blockchain networks: Private blockchains, Public blockchains, and consortium blockchains. Private Blockchain is operated and controlled by a single organi-zation, thus one cannot join the network unless network ad-ministrators provide the permission. This type of blockchain network is often considered as quasi-decentralized and the organization is also responsible to determine the rules of the chain.

Consortium blockchain is similar to the private blockchain but does not provide power to a single or-ganization, instead, a few selected nodes are predetermined to participate in the verification process. Thus the consor-tium blockchain has the status of being semi-decentralized. It is similar to trusting the power to a council of organi-zations who can decide who has the access to read the ledger.

Public blockchains have absolutely no restrictions to ac-cess the chain, it does this by setting up a peer-to-peer net-work. Anyone can send transactions and each transaction is verified by every node affiliated with the blockchain. Public blockchain can be viewed as a fully decentralized network. Although for public blockchain, costs are higher and speed is slower than the private blockchain, it provides full trans-parency of the ledger.

Copy table of comparison (pub, pri, cons)from an overview of the blockchain

Blockchain Application :

The flexible nature of blockchain technology has lead to numerous applica-tions in the financial domain. There are many other uses for blockchain beyond the financial field. For example, in supply chain management businesses can locate items in real time and also inefficiencies in the supply chain can be detected using blockchain technology. Microsoft is attempting to create decentralized digital ID using its Authenticator App which is used by a lot of people. Another application of blockchain is to share or sell the data and for immutable data backup.

Limitaions of Blockchain:

1. The Volatility of blockchain: The cryptocurrency based on blockchain are very volatile in nature that is the con-stant change in the value of cryptocurrencies like Bitcoin and Etherium. This makes it vulnerable to being accepted by the current market of a nation. If it affects the economy of the nation it may get banned from the market. Countries like China, Russia and Vietnam have banned Bitcoin.

2. Increasing crime: Since transactions on a blockchain network can be done anonymously and there is no way to track down the user, cryptocurrencies have become a very useful method of payment in the black markets around the globe. Criminals are using cryptocurrencies like Bitcoin for their illegal activities.

Technical Limitations of blockchain:

1. **Size of the network:** The network of a blockchain based project must have a huge number of users so as to get the most out of it. The advantage of blockchain is that longer the chain the more secure and useful it will become so if there are not enough users in the network it becomes less useful.
2. **Security Issues**: As the chain grows in size it becomes more vulnerable to security issues like the 51 per cent attack. If more than half of the computers in the network say that a particular transaction is true then it is considered true in the entire network. Similarly, if more

than half computers in the network say if it is a lie then it will be considered as true in the network. This is an unavoidable flaw of the blockchain.

Overview of Smart Contract

The smart contracts are a creation of a cryptographer and legal scholar named Nick Szabo, who in 1995 realized that blockchain's decentralized ledger could be used for creating a digital contract. He thought of converting legal contracts to computer code and putting them in the network of comput-ers that run the blockchain, which gave rise to the currently known blockchain contracts or smart contracts. Smart Con-tract is a code running on a blockchain with a pre-defined set of rules which facilitates, enforces and verifies the ne-gotiation of an agreement or transaction. If the predefined conditions are met, the agreement is automatically enforced.

Working principle of smart contract: Two parties can ex-change money, property, coins, or anything of value in a transparent way by using smart contracts. As smart contracts are already encoded into the blockchain, they are decentral-ized by nature. Smart contracts are defined using high-level programming languages, one such language for Etherium is Solidity. Terms for transactions are established by two par-ties and when conditions for execution of transaction are fulfilled, the contract execution event is triggered. Smart contracts are executed in programming language on the IF-WHEN-THEN basis, for example:

IF/WHEN you send me the item X, THEN the Y funds will be yours

IF/WHEN you transfer the X money, THEN the item Y be yours

IF/WHEN I finish the job X, THEN the Y money will be mine

By creating nested structures, it is possible to implement more real-life transaction scenarios. For example: IF/WHEN you send me the item X and Y by date Z, THEN fund A and item B by date C becomes yours.

Benefits of smart contracts :

Cost-efficiency: By eliminating the middleman, the smart contracts automatically enforces the transaction themselves once certain conditions are fulfilled thus reducing the fees to hire the personnel to monitor.

Processing Speed: Since the smart contract is monitored by the blockchain and runs on automated processes, the re-sults are almost instant.

Trust: Business agreements are made immutable and also the documents are encrypted on a shared ledger and there-fore more trustworthy.

Reliability: Even in case of some data loss at one node, each and every other node of blockchain can be used as a backup.

Accuracy: High accuracy can be achieved through smart contracts by eliminating error caused when filling out heaps of forms manually.

Limitations of smart contracts :

1. Immutability : Smart Contracts are not flexible or changeable once they are deployed. Since they can't be changed it makes it very secure but a small flaw or human error can result in loss of time and money as the code will be executed wrong.

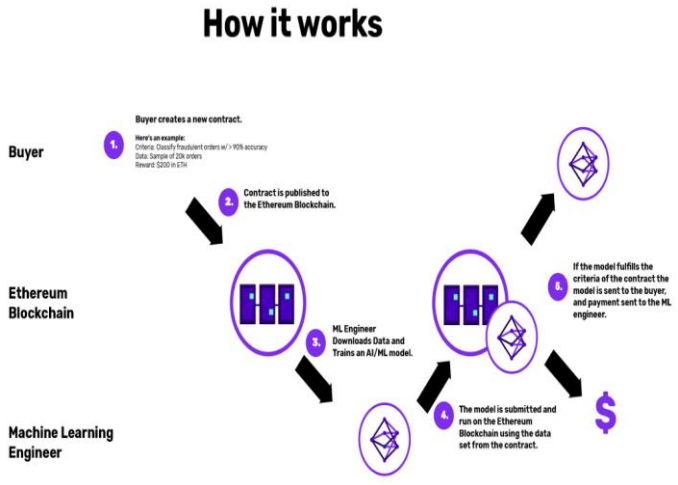
2. Frauds : Smart contracts are not very immune to frauds. Suppose you buy a car and after the transaction, you find out that it has issues with the engine or doesn't have a proper registration, traditionally you could deal with it but with smart contracts, it is near impossible for you get a fair outcome.

3. Not userfriendly: Smart contracts are not so user-friendly as making smart contracts is limited to people who can code. It requires technical skills that need to be learned and basically, it cannot be simply used by a common user.

How Artificial Intelligence can enhance the power of blockchain

The term artificial intelligence was introduced in 1956, but AI became more popular today due to the increase in data, advanced algorithm, and improvements in computer hard-ware and software.

Artificial intelligence made it possible for computer sys-tems to learn from past experience, adjust to new inputs and perform human-like tasks. Most of AI examples that we hear about today from chess-playing computers to self-driving cars are based on deep learning and natural language pro-cessing which are sub-branch of Artificial Intelligence. Us-ing these technologies, computers can be trained to achieve particular tasks by processing huge quantity of data and rec-ognizing patterns in data.



How AI can be used with Smart Contracts? Initially, a buyer creates a new smart-contract. The contract is then published to the Ethereum Blockchain.

A user then submits a dataset, an evaluation function and reward amount to the Ethereum Smart Contract. The evalu-ation function takes a machine learning model and produces a score as output. This output score denotes the quality of the model.

After this, other users download the dataset submitted by the former user and the work with it independently. The users use the dataset and train the machine learning model. When the user now succeeds in training the machine learn-ing model, he/she submits the solution to the blockchain.

Finally, the blockchain (possibly initiated by some user action) will evaluate the models which were some submitted by users, using the evaluation function.

Buyer creates a new contract. The contract is published to Ethereum Blockchain.

ML Engineer downloads data and Trains an AI/ML model.

The model is then submitted and run on the Ethereum Blockchain using the dataset from the contract. If the model fulfils the criteria of the contract, the model is successful and the model is sent to one party(the buyer), and payment sent to the other party(the ML engineer).

Conclusion

In this paper, we have given a brief overview of the con-cepts of blockchain and smart contracts. We have discussed the various advantages and disadvantages of it and also ex-plained how it can be enhanced using artificial intelligence. Combining smart contracts with blockchain and enhancing it with artificial intelligence can take this technology to a new level and will be very beneficial in the future.

References

The Convergence of AI and Blockchain - Corea, Francesco , 2018

Bitcoin: A Peer-to-Peer Electronic Cash System - Satoshi Nakamoto, 2008

An Overview of Blockchain Technology : Architecture, Consensus, and Future Trends - Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, 2017

An Overview of Smart Contract and Use cases in Blockchain Technology - Bhabendu Kumar Mohanta, Soumyashree S Panda, Debasish Jena , 2018

Runtime Verification of Ethereum Smart Contracts - Joshua Ellul, Gordon Pace, 2018

Security Assurance for Smart Contract - Ence Zhou, Song Hua, Bingfeng Pi, Jun Sun, Yashihide Nomura, Kazuhiro Yamashita, Hidetoshi Kurihara, 2018

Smart Contracts Vulnerabilities: A Call for Blockchain Software Engineering? - Giuseppe Destefanis, An-drea Bracciali, Michele Marchesi, Marco Ortu, Roberto Tonelli, Robert Hierons, 2018

Websites

https://blockgeeks.com/guides/smart-contracts/

https://blog.agrello.org/how-to-make-smart-contracts-worthy-of-their-name-using-artificial-intelligence-3a90e4dd3c47

https://blockgeeks.com/guides/blockchain-applications-real-world/

https://www.blockchain-council.org/blockchain/how-does-blockchain-use-public-key-cryptography/

https://www.mycryptopedia.com/public-key-private-key-explained/

https://www.coindesk.com/information/how-does-blockchain-technology-work