VOLUME-8, ISSUE-5, MAY-2019 • PRINT ISSN No. 2277 - 8160

Original Research Paper

Computer Science

APPLICATION OF MACHINE LEARNING RANKING IN BLOCKCHAIN BASED LOAN APP

Ritwik Tiwari Department of Computer Science and Engineering, Jaypee University of Information Technology

Deepesh Yadav* Department of Computer Science and Engineering, Jaypee University of Information Technology *Corresponding Author

ABSTRACT The online loan application is a venture created to give a simple method to apply for credit using cryptocurrency. Information can be acquired by the users about applying for a loan and apply for the same. Before the ascent of banks, loans and reimbursements occurred peer-to-peer. After some time, the trust started to diminish, and mediators and outsiders were added to the situation. These mediators gave a layer of security, yet in doing as such charge high expenses while including additional layers of multifaceted security and control the process. Being based on a distributed record, the very idea of its structure is trustless and decentralized. This makes it conceivable to exchange responsibility for resources starting with one individual then onto the next, without the requirement for a middle person, a quality which could help resuscitate peer-to-peer model. Blockchain loaning basically expands on the immortal peer-to-peer model, making the whole procedure progressively consistent and decreasing the measure of time the procedure takes. The agent (a bank) is thrown away, and singular borrowers are associated straightforwardly to willing loan. The incredible estimation of such decentralized loaning is that with a solitary demand, a borrower can get to extremely focused financing, as geography is no imperative on a blockchain stage, lenders from everywhere throughout the world can bid to give the loan. And the most suitable bid, that is, with minimum interest can be selected. Whilst, the borrower has to maintain a minimum account balance. Imperatively, there is no compelling reason to depend on an outsider for individual verifications. Since all exchanges are open and auditable, each location can be relegated a credit rating, inconsequentially.

KEYWORDS : Learn To Rank Algorithm, Blockchain, Ethereum, Smart Contracts, Decentralized Ledger Technology, Hash Rate, Cryptocurrency.

I. INTRODUCTION

The online loan application has had various forms of procurement. Be it via private companies or P2P system being developed. In a traditional online loan application and confirmation framework, the client to applies for credit by enrollment, transferring of records, endorsement or dismissal status of advance are done on online by administrator i.e. bank representative with the assistance of CIBIL score. The PAN number of clients is utilized for getting CIBIL report where it gives subtleties of one's obligation accounts and their installments in different banks. The client gets an advance endorsement or rejects status when he logins, whenever affirmed transferring of reports to the administrator and after that rest, procedure is done physically. Internationally, various online commercial center moneylenders have made this a reality and are putting forth online stages that coordinate borrowers straightforwardly with financial specialists. This purported distributed (P2P) or commercial center loaning display is developing in prominence with borrowers due to its apparent low-financing costs, disentangled application procedure, and speedy loaning choices. This show is quickly extending to new item classifications, counting contracts and other verified advances. Specifically, P2P stages appear to have discovered a specialty by offering borrowers an improved loaning experience—and they are rapidly picking up energy. Further, related work is discussed in section 2. Methodology and application of the algorithm are mentioned in section 3 followed by the future work and conclusion in the section 4. Section 5 has the references.

II. RELATED WORK

In this section, a review on total of 4 manuscripts and 2 patents has been carried out.

According to [1] Adebayo et. al a credit is a measure of cash given to an individual or organization depending on the prerequisite that it will be paid back over a guaranteed period with enthusiasm, with fills in an installment for the utilization of cash there are different kinds of advances, for example, credits, funds, and mortgages. The manual procedure of acquiring and conceding advances is stressful, badly designed and time squandering for loan specialists and borrowers also. There is a need to computerize the credit preparing system however much as could reasonably be expected. The objective of this venture is, in this manner, to plan and make credit robotization application programming that can catch the required advance information components just once, keep such data secure all through the credit procedure, convert the past hand to hand arrangement of getting and allowing advances into a modernized less stressful structure, monitor people all the while, screen and track advances offered out to permit better stream and upgrade consistence to conditions, guarantee security of data decrease loaning life cycle times, apply suitable enthusiasm to advances and advise the concerned individual on the advancement of their credit [1].

Subbareddy et. al discusses, for the most part, contains the credits the board framework was grown explicitly a large number of the banks give advances for physically by this paper I presenting the new idea for online credits administrations. Presently coming to paper, we make the security given by who are having as of now account in that specific bank. The client needs to take the one-time secret key then the client takes the online advance in anyplace specifically locales. This thought is very to utilize full for all informed clients, presently we as a whole utilize the ATM. Why we can give the Security? For the motivation behind interloper does not permit this framework. Since the interloper does not know the right secret word and right client name. In this security gives to every single financial administration. The client gets the username and secret key by email or SMS. The client gets the credit cash by ATM [2].

Hu et. al patented a system and accommodation customer/server framework transmit pertinent credit data from a borrower to at least one bank PC framework through pre-characterized document layouts, which are used amid advance start. A programmed information stream process from the start screen populates the applicable fields in some other related advance structures and word handling records. Diverse structures are upheld for various kinds of credits. The advance originator PC framework incorporates an advance beginning programming program coordinated with an internet browser-based interface framework. The interface framework couples the credit start programming project to at least one accomplice PCs. The accomplices involve credit financiers, loan specialists, and settlement administration merchants. The interface

framework gives dynamic arranging and information transmission for various associations relying upon the exchange type and target accomplice. In online usage, the interface framework populates information legitimately from the advance beginning programming system to the proper website pages of the objective accomplices [3].

Jenusha et. al proposes a credit beginning framework interface module for preparing advance applications from a client through a loan specialist site is portrayed. The advance originator gets to a bank site to perform advance handling methods. The module is incorporated on the loan specialist's website page through a standard article reference in HTML particular. The module contains data one of a kind to that bank, and the loan specialist's recognizable proof number just as wanted information position. When the advance originator chooses to exchange a credit application or supplemental information to the moneylender, the module looks at the advance start programming pipeline and presents a choice of advanced items to the client. When the client makes a choice, the module separates credit data put away in the advance beginning programming by directing a look for each required information field, relates that information to the particular field in the merchant application configuration, and bundles the information in an organization adequate to the loan specialist. The module at that point finds the suitable course to convey the advance information to the moneylender, either straightforwardly through a standard Internet secure correspondence convention, or in a roundabout way through a different server PC. Credit preparing happens on the moneylender's site, and the collaboration of the site and advance start programming is taken care of by the module [4].
Heiston et. al has patented a mechanized framework for gathering and scattering advance data over a system association incorporates a server that gets advance information, including every day advance information, from banks and stores the credit information in a database. A web server gives to clients (e.g., representatives, reporters, or retail credit clients) intelligent web content including advance data and a rundown of advance criteria which would influence the cited focuses, rate, top, or edge related with a specific advance. The web server gets a client's material advance criteria chose from the rundown of conceivable advance criteria. What's more, it utilizes that appropriate credit criteria and the advance information from the moneylender to make a rundown of acclimations to the focuses, rate, top or edge. A cited loan fee and the rundown of material adjustments are transmitted by the web server to the client [5].

Benefits of using Blockchain Technology are:

Fraud Prevention: As this application is based on the idea of sharing data crosswise over gatherings and amongst parties amid transactions; it saves money on compromise cost among banks and avoids misfortunes in view of documentary fakes.

Versatility through repetition: Being disseminated engineering by structure, this application empowers the system to be worked by all permissioned hubs in the biological community. All the imperative individuals from the installment biological community – banks, money related organizations will viably turn into taking interest hubs. On account of an untoward occasion influencing the biological system (like war, floods, seismic tremors, digital assaults), regardless of whether a few hubs of the system are inaccessible, the accord calculations worked as a piece of the Blockchain technology arrange guarantee an exchange can be endorsed by the rest of the hubs in the system.

Immutable Transactions: Maintaining a permanent record of exchange occasions in a sequential request being a primary mainstay of its engineering, BCT ensures much wanted ascribes to banking and money related exchanges, for example, immutability and finality.

Control and Security: Users are responsible for their exchanges, without previous security while conquering data fraud. Because of the way that blockchain exchanges can't be turned around, don't convey with them individual data, and are secure, traders are shielded from potential misfortunes that may happen from misrepresentation.

Transparency: All concluded exchanges are accessible for the viewing pleasure of anyone passing by consequently permitting quick confirmation of exchanges. Conventions being open source experience wide examination, consequently empowering trust in the fundamental stage and ensuring that they can't be controlled by any single individual, association, or government. It is conceivable to send also, get cash anyplace on the planet at any given time, without a focal specialist.

III. METHODOLOGY

Blockchains are an advanced innovation that consolidates cryptographic, information the board, organizing, and motivating force systems to help the checking, execution, what's more, recording of exchanges between gatherings. A blockchain ledger is a rundown ('chain') of gatherings ('blocks') of exchanges. Gatherings proposing an exchange may add it to a pool of exchanges proposed to be recorded on the record. Handling hubs inside that blockchain network take a portion of those exchanges, check their integrity, and record them in new blocks on the record.

The substance of the blockchain record is replicated over some geologically disseminated processing nodes. These handling nodes mutually work the blockchain framework, without the focal control of any single confided in the third party. In any case, the blockchain framework guarantees that all nodes, in the end, accomplish accord about the uprightness, what's more, the shared substance of the blockchain record. Exchanges between blocks, for example, installments, escrow, notarization, casting a ballot, enlistment, and procedure coordination are key in the tasks of government and industry. Generally, these exchanges are bolstered by trusted third parties, for example, government offices, banks, lawful firms, bookkeeping firms, and specialist organizations in explicit ventures. Blockchains give an alternate approach to help these exchanges. Rather than trusting outsiders, we would confide in a greater part of the system mutually working the blockchain, and the rightness of their mutual innovation stage.

The term, smart contract, alludes to any agreement prepared to do consequently implementing itself, without an outsider between individual members. Smart contracts are composed as computer programs as opposed to in lawful language on a printed archive. The program can characterize severe guidelines and results similarly that a customary authoritative report would, however not at all like a conventional contract it can likewise accept data as an input, process it through the guidelines set out in the agreement, and take any activities expected of it, therefore. The idea was characterized in 1994 by cryptographer Nick Szabo, yet practically speaking stayed unrealized in light of the fact that the mechanical framework expected to help it didn't yet exist. These days, the appearance of crypto conventions and the blockchain is evolving that, and subsequently, the thought is seeing a recovery. In a word, smart contracts are secluded, repeatable and autonomous scripts, normally running on a blockchain, which speaks to one-sided guarantees to give a determinate calculation. These contents are put away in the blockchain at a specific location, which is resolved when the agreements are sent to the blockchain. At the point when an occasion recommended in the agreement occurs, an exchange is sent to that address and the conveyed virtual machine executes the content's activity codes (or provisos), utilizing the information sent with the exchange. Smart contracts can be coded to mirror any sort of information-driven business rationale: from activities as basic as voting in favor of a post in a discussion to the more intricate, for example, loan collateralization and prospects contracts, and to the profoundly unpredictable, for example, reimbursement prioritization on an organized note. The exchanges put away on a blockchain can be more than straightforward records of the trading of advantages – a few blockchain frameworks additionally permit

computer projects to execute and be put away as a major aspect of exchanges on the ledger. These are regularly called smart contracts', in spite of the fact that the projects are normally not 'smart', and are in some cases not used to execute or screen legitimate contracts. The lawful status of smart contracts as legal contracts is as of now discussed. A legal contract is an understanding among parties, and a PC program is either the content of source code or an executing physical machine. So smart contracts, as PC programs, might be the wrong classification of things to be a lawful contract.

In any case, a smart contract may give proof for there being a lawful contract, and might almost certainly encourage the execution of a legitimate contract. Vitally as a system for the execution of arrangements of a legitimate contract, smart contracts can convey and conditionally transfer computerized money and other advanced resources or tokens between parties. This should be possible in an anticipated and straightforward path on the nonpartisan ground given by the automated foundation of a blockchain. The Bitcoin blockchain permits straightforward types of smart contracts, yet different blockchains, for example, Ethereum permit computer projects to be written in a 'Turing complete' language that is on a basic level as expressive as each other universally useful programming language. Thus, blockchains can be in excess of a straightforward appropriated database – they can be general computational stages. This capacity essentially grows the intensity of blockchain frameworks and increments their scope of utilization and potential for advancement. A few blockchains shun the utilization of Turing-complete smart contract dialects, so as to encourage the mechanized check of the rightness of smart contracts.

Thus, application using smart contracts will enable users to take and provide a loan without engaging with the third parties. Dealing in cryptocurrency makes matters more convenient or users. Users can simply log in and apply for a loan, and the loan can be provided by any user with spare cryptocurrency with however amount of interest he wants to give. Thus, the matters would remain into the hands of borrower and lender, we'll be providing the appropriate platform for the same. As opposed to traditional applications, this application using cryptocurrencies would prove to be more useful. The proposed framework gives a simple method to clients in applying for credit. Clients can apply for credit from anyplace and at whenever and get warnings. Clients can see their profile subtleties and can see every one of the subtleties of the credit.

The problem of collateral security is solved by computing the hash rate of the applicant's system. The greater the computing power more amount applicant can apply. Once the hash rate or computing power is calculated, applicants are ranked according to their computer power. For ranking, we use Learning to Rank Algorithm [6]. Here, we will use the computing power data of the users to automatically learn about their computing power such that the ranking of our user pool is the one that maximizes the likelihood of scoring a high-ranking score. The better the rank greater the likelihood to get more coins in the loan. The steps include:

1. Generating the training data
2. Defining the probability function for ranking
3. Train the models

a. Logistic Regression
b. Decision Trees
c. Neural Networks

4. Comparing the results

Once we have our ranking, we save the results in the database for further processing and analysis.

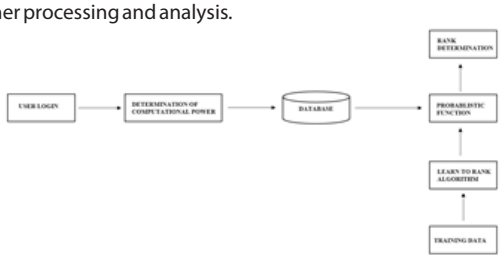

Fig 1: Flow diagram of ranking

The first step for the applicant for getting the loan is to register himself on the website. After the registration process is complete the computing power of the applicant's system is determined, and rank is given to the applicant's system. The learning to rank algorithm will divide the users into different clusters (groups) of applicants with similar rankings. These clusters of applicants can only apply for a specific amount of maximum loan based on their ranking. Other than this they are free to choose the rate of interest and time duration of the loan. The rate of interest and time duration is set each individual lender who is willing to lend money (cryptocurrency) to the applicant.

These clusters will be the basis of the mining pool in which the users will participate to pay off their loans. The mining pool coordinates the workers. It is like a lottery pool. The odds of winning a lottery are very low, so the applicants team up with other applicants and agree to split the winning. This makes the odds of winning much higher, but the amount won much lower. Each user in the pool has an almost equal ranking, i.e.; their computational power is almost equal which gives them a fair chance to compete against each other in mining and ensuring that they cannot cheat the pool.

Together these mining pools would hold a considerable amount of computing power which will be used for block mining. The pool will randomly verify the proof of work (Pow) submitted by each applicant. The applicants are not aware of which of their submission will be verified so they would not be able to cheat.

The payment of the block mined will be done on how many shares people get and set the Coinbase transaction to pay the block reward directly to them once a block is found.

Common pay-out schemes include:

PPS – Pay Per Share. Each submitted share is worth a certain amount of BTC. Since finding a block requires shares on average, a PPS method with 0% fee would be 50 BTC divided by. It is risky for pool operators; hence the fee is highest.

SMPPS – Shared Maximum Pay Per Share. Like Pay Per Share, but never pays more than the pool earns.

ESMPPS – Equalized Shared Maximum Pay Per Share. Like SMPPS but equalizes payments fairly among all those who are owed.

CPPSRB – Capped Pay Per Share with Recent Backpay.
Prop. – Proportional. When a block is found, the reward is distributed among all workers proportionally to how much shares each of them has found.

PPLNS – Pay Per Last N Shares. Similar to proportional, but instead of looking at the number of shares in the round, instead looks at the last N shares, regardless of round boundaries.

Score – Score based system: a proportional reward but weighed by time submitted. Each submitted share is worth more in the function of time t since the start of the current round. For each share score is updated by: score += exp(t/C). This makes later shares worth much more than earlier shares; thus, the miner's score quickly diminishes when they stop mining on the pool. Rewards are calculated proportionally to scores (and not to shares). (at slush's pool C=300 seconds and every hour scores are normalized)

Property	Proposed Solution	Traditional Approach
Scalability	Scalability of perusing from the blockchain can be great since every member can hold their own full duplicate of the blockchain.	The hassle of going through the paper works and regulations imposed by the financial institutions limits the scalability.
Interoperability	Blockchain simplifies these collaborative processes requiring a higher level of integration. One can use many cryptographic currencies like BTC, ETH, XMP etc.	User is limited with only one currency.
Latency	Systems ordinarily include the physical exchange of cryptocurrency, such huge numbers of inactivity prerequisites on data exchange are ordinarily on the request of minutes to hours. Neither of the structures ought to experience the ill effects of latency surpassing these time spans	Initially paper works can take months, but after approval all transactions are instantaneous which depends on the availability of the server of the financial institutions
Integrity	Integrity is a solid inherent element of blockchains: data caught as a major aspect of submitted exchanges would be exceedingly difficult to change.	Currently, financial institutions are more trusted due to involvement of paper works and trust in the system by the people.
Confidentiality	Data and transactions are encrypted thus, data and transactions cannot be accessed. It does not have any physical records associated with it.	Here all the proceedings are done on the paper and all transactions are visible. Thus, government has the full control on the transactions.

Fig 2: Comparing the proposed solution with the traditional approach

I. FUTURE WORK AND CONCLUSION

The fundamental motivation behind smart contracts is to empower individuals to work with outsiders, generally over the web, without the requirement for a confided in middle person. The thought is that the product can computerize a great part of the process, permitting the implementation of legally binding guarantees without human contribution. The blockchain guarantees that everyone is seeing a similar thing without one side confiding on the opposite side to be straightforward since anything that is in the blockchain is unforgeable. This may seem like we won't require legal counselors any longer. In any case, smart contracts are a development of the lawful framework, not its substitution. The job of legal advisors might move from arbitrating singular contracts to delivering smart contract layouts on a focused showcase. Contract selling focuses would be their quality, how adjustable they are, and their usability. In the long haul, we could see the flood of composed smart contract commercial centers that, thus, would be completely overseen through smart contracts, along these lines shutting the circle. The application we have proposed on structure competitors may not be legitimate, in light of the fact that they are yet to be generally utilized and contemplated for blockchain-based frameworks. Be that as it may, the abnormal state subjective methodologies we utilize have been recently utilized in an assortment of other innovation areas, so we trust it is sensible to utilize them to bolster the demonstrative subjective discoveries in our proposal. Blockchain advances are under dynamic improvement all around, and there might be ongoing advances that sway our discoveries. To moderate this, we have attempted to pursue propels in blockchain advances by checking universal innovation papers, and white paper writing.

V. REFERENCES

[1] Adewale O Adebayo, Aibangee Zandra, Lufadeju Oluwatosin & Maradesa Adepeju "Creation of Loan Automation Application" G.J. E.D.T., Vol.3(1): 52-61, 2014, School of Computing and Engineering Sciences, Babcock University, P.M.B.21244 Ikeja, Lagos, Nigeria

[2] T.Subbareddy, M.Meghana and K.Swathi "Online Banking Loan Services" Volume 2, Issue 7, July 2013, International Journal of Innovative Research in Science, Engineering and Technology

[3] Limin HuBabak Khanpour Ting-Hu Wu "Online system for fulfilling loan applications from loan originators" Patent Number: US7444302B2, United States

[4] V.R Jenusha, R. Karthiyayinn "Smart loan application for bank using android" Volume 6, Issue 5, May 2016, International Journal of Innovative Research in Science, Engineering and Technology

[5] Richard J. Heiston, Frederick T. Dykes "System and method for transmitting and processing loan data" Patent Number: US8117117B2, United States

[6] Zhe Cao, Tao Qin, Tie-Yan Liu, Ming-Feng Tsai, Hang Li "Learning to Rank: From Pairwise Approach to Listwise Approach" Tsinghua University, Beijing, Microsoft Research Asia, Beijing , National Taiwan University, Taipei.