IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 1, January 2021

DOI 10.17148/IJARCCE.2021.10131

Peer-To-Peer Ride-Sharing System

Deepak K N[1], Aiswarya P S[2], Fathima T P[3], Savitha K F[4],Keerthana Gopi K[5]

Assistant Professor, Department of Computer Science And Engineering,Universal Engineering College ,Vallivattom, Thrissur, India.[1]

B.Tech Student, Department of Computer Science And Engineering,Universal Engineering College ,Vallivattom, Thrissur, India.[2,3,4,5]

Abstract: Ride-sharing is a service that enable drivers to share trips with other riders, contributing to appealing benefits of shared travel cost and reducing traffic congestion. Most current ride-sharing system, however, depend on a central third party to organizing the service, subjecting them to a single point of failure and privacy concerns about disclosure by both internal and external attacks. The proposed system makes without depending on a trusted third party, drivers to provide ride-sharing services. Both riders and drivers can learn if they can share rides while maintaining their travel information, including place of pick-up/drop-off, departure/arrival date and price of travel. However, Malicious consumers to send multiple ride requests or requests, exploit the anonymity given by the public blockchain In order to find a better deal or to make the offer, while not committing to either of them, offers unreliable structures. The proposed system addresses this issues by implementing a time-locked method. A ride-sharing deposit protocol by leveraging the smart contract and zero-knowledge collection evidence for membership. In a nutshell, a driver and a passenger will have to demonstrate their good will and commitment to the blockchain by submitting a deposit. Later, a driver must prove himself to the blockchain on the decided pick-up time that he/she arrived at the pick-up place on time. To protect the privacy of the rider/driver by hiding the exact pick-up spot, the evidence is performed using evidence of membership of the zero-knowledge set. To ensure equal payment, moreover, A pay-as-you drive methodology is applied depending on the driver's elapsed time of the rider and driver. Furthermore, we implement a model of reputation to rate drivers based on their history behaviour without any third party interference.

Keywords: Blockchain Technology, Decentralization, Consensus Algorithm, Distributed System, Cryptocurrency

0 INTRODUCTION

Steps to reduce ill effects of private vehicles are extremely necessary now-a-days .Mass transit system is the best solution if provided efficiently, but many persons do not prefer it because of its lack of door to door service, longer and fixed route and less reliable schedule. There should be any facilities or services established to provide customers with a convenient and reliable service and to decrease hazardous environmental impact such as noise, congestion, etc. Sharing the ride is one of the emerging technology have been implemented all over the same technologies. The destination of origin and time of travel are balanced and the trip is shared. Private cars have a versatile and convenient ride, but with a rise in price. Transport network, population and excess use of cars, face the limits of capacity, traffic congestion due to high peak hour demand, environmental efficiency, anxieties, and energy security. Specific motorised traffic adds to a considerable amount of part to worldwide emission and increases oil dependency and thus increases economy's dependence on fluctuating oil prices. Mass transit system is one of the widely used and effective modes of public transport system. While the mass transit system can reduce some of the negative effects, they do not provide the flexibility and reliability of private vehicles. The bilk of the ridership focuses on a few routes only. The downside that it also has that occupancy per vehicle is smaller and most vehicles move empty while they are off. Peak hours, and they are often overloaded during peak hours.so people who generally wanting a convenient trip does not benefit the conventional mass transit system. Ride-sharing is one of the strategies that can be adopted to reduce the drawbacks, in which users go for ride-sharing groups of users share a car pool or another mode of transport which suit their need best.

1 THEORY

0 Blockchain Technology

Blockchain is a data recording mechanism that makes it hard or impossible to alter, hack, or cheat the system. A blockchain is basically a digit transaction ledger that is duplicated and distributed on the blockchain through the whole network of computer system. Blockchain is a database that store all transaction grouped in blocks. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. When a fresh transaction is created, the sender broadcasts in the peer to peer network to all the other nodes. As the nodes are getting the transaction, they verify and keep it in their transactional pools. Verify the transaction means the execution of predefined controls about the structure of the transaction and its actions. Special types of nodes called miners create a new block and group some of their transaction pool's available transactions. Then the block is mined, which is a method of using variable data from the header of the new block to find the proof of work. The calculation of cryptographic hash that matches the given difficulty aim is to find the evidence of work. Each block stores meta-data and the hash value of the previous block in addition to transaction. So every block has its parent block with a pointer. That is how the blocks are linked, forming a block chain called Blockchain.

1 Decentralization

Decentralization is the process of dispersing functions and power away from central location or authority. Originally, the World Wide Web was established as a decentralized forum. Example of decentralized architecture and systems are blockchain technologies, such as Bitcoin and Ethereum.

2 Consensus Algorithm

A consensus Algorithm is a protocol through which a common agreement (consensus) on the current data state of the ledger is reached by all parties of the blockchain network and is able to trust unknown peers in a distributed computing environment. A consensus algorithm is a computer science method used to achieve agreement among distributed processes or systems on a single data value. In a network containing many unstable nodes, consensus algorithms are built to achieve reliability. The consensus algorithm plays a crucial role in maintaining the safety and efficiency of blockchain. The use of a correct algorithm will result in a significant improvement in blockchain application efficiency. In distributed systems, the consensus algorithm has been studied for several years .In blockchain, there are several transplantable consensus algorithms implemented. In this section, we present a detailed overview of the principles of these consensus algorithms.

1.PoW(Proof of Work)

Proof of Work is a process of generating a cryptographic hash, and concept was first introduced in 1993 by Cynthain Dwork and Moni Naor ,and later re-introduced it in the Bitcoin whitepaper in 2008 by Santoshi Nakamoto. Historically, proof of work in blockchain systems derives from its use in Hashcash, which Adam Back designed as a framework to restrict email spam and denial-of-service.

To pick a miner for the next generation of blocks, this consensus algorithm is used. This PoW consensus algorithm is used for Bitcoin. The central idea behind this algorithm is to solve and easily give out a solution to a complex mathematical puzzle. This mathematical puzzle gets to mine the next block as soon as possible. Blockchain validators in a PoW system must take data from a block header as an input and run it through a cryptographic hash function on an ongoing basis. Every time the input data is run through the cryptographic hash function, validators by adding an arbitrary number called a nonce. PoW requires high processing power levels of electricity to determine which data gets added to the next block in a blockchain.

2.PoS(Proof of Stack)

The PoS consensus algorithm was developed in 2011 as an alternative to poW. Although PoS and PoW have similar objective, they present some fundamental differences and features, particularly during the validation of new blocks on the blockchain network. With the PoW mining consensus, the Proof of Stake (PoS) consensus algorithm varies with a system where blocks are checked depending on the stake of the participants in the network. Here, in contract to running hash functions, validators mainly spend capital in the form of digital cash or tokens. Each block validator is then randomly selected from the stakeholders on the basis of the amount of computational power allocated. Ethereum moved to PoS consensus from PoW.In this type of consensus algorithm, validators invest in the coins of the system by locking up some of their coins as a stake, instead of investing in expensive hardware to solve a complex puzzle. After that, the blocks will start validating all the validators. Validators can validate blocks if they discover a block that they think can be added to the chain by making a bet on it. All validator receive a reward proportionate to their bets and their stake increase accordingly based on the actual blocks added to the blockchain. In the end, a validator is chosen to generate a new block based on their economic stake in the network. Thus, PoS allows validators to reach an agreement through an incentive process.

3.DpoS(Delegated proof of stake)

Delegated Proof-of-Stake (DpoS) is another form of consensus algorithm, conceptualized by Daniel Larimer, which is focused on voting systems where "delegates" vote for their favourite validators to assist in the new blocks consensus state. These validators will also be responsible for validating transactions, maintaining the network of blockchains, and

DOI 10.17148/IJARCCE.2021.10130

will be rewarded with transaction fees in return. Also, the power of each voter is proportional to the size of the network's stake. for validating transactions, blockchain projects such as EOS, Bitshares, Steem, Tezos, etc. use the DpoS consensus algorithm. It is often considered a democratic variant of the Proof of Stack consensus system by many experts since it is based on a voting mechanism and elects members rather than autonomous nodes of the network. Due to a small number of network nodes or trusted witness, DpoS can handle a greater transaction volume and faster confirmation times than PoW and PoS consensus mechanism to validate data in each new block of the network chain.

4.PoET(Proof of Elapsed Time)

Intel created the PoET consensus method to address the "random leader election" computing problem.it was published as part of the programming reference manual for Software Guard Extensions(SGX).Many private blockchains, like Hyperledger Sawtooth, are now using PoET because it relies on a random timer system for network participants instead of using mining hardware, as in the case of Proof of Work(PoW).It is necessary for each participating blockchain node in the network to wait for a randomly chosen duration,and whoever wins the new block with finished time and validates it.

3 Distributed System

The distributed ledger is at the heart of the network, so the 'Decentralized Distributed System' is also known as the blockchain. The more general and nuanced area of research is a distributed scheme. A group of independent nodes that are linked in a coordinated way to achieve a common outcome and are structured in such a way that the group appears to be a single system for the end user. The nodes are programmable, asynchronous, autonomous and failure-prone. Every node has a memory and a processor of its own. They have common states and are able to work simultaneously. In order to provide a service, exchange data or simply store data, the nodes are linked to each other (e.g. blockchain).Using messages, all the nodes connect with each other. Both nodes are capable of sending or receiving messages to each other in the distributed system.

4 Cryptocurrency

A cryptocurrency (or "crypto") is a digital currency that can be used to purchase products and services, but to protect online transactions, it uses an online ledger with strong cryptography. Trading for profit is a major part of the interest in these unregulated currencies, with speculators driving prices skyward at times. It is a form of payment that can be exchanged online for goods and services. Many companies have issued their own currencies, often called tokens, and these can be traded specifically for the good or service that company provides. Cryptocurrencies run utilizing a blockchain-called technology. Blockchain is a decentralized transactions spread across many computers. part of this technology's appeal is its security. According to CoinMarketCap.com, a market analysis website, more than 6,700 separate cryptocurrencies are exchanged publicly. And the emergence of cryptocurrencies continues, increasing capital via initial coin offerings or ICOs. According to CoinMarketCap, the total value of all cryptocurrencies was more than $645.7 billion on Dec. 18, 2020, and the total value of all bitcoin, the most common digital currency, was pegged at about $421.7 billion.

2 RELATED WORK

Here we introduce each paper based on the technologies used in the ride-sharing and this are arranged in technologies bases
The aim of this paper [1], they propose a blockchain-based ridesharing framework utilizing brilliant agreements to alleviate the single purpose of disappointment issues introduced in traditional customer worker structures. In any case, other than being totally disseminated what's more, straightforward, the receptiveness of blockchain prompts a potential security concern where the information can be openly open. In spite of the utilization of mysterious verification, this isn't adequate to secure the protection of the end clients. For example, by following the action of a driver or rider, an aggressor with little foundation information on that client can sort out the entirety of his area follow. Additionally, since in open blockchains, anybody can join and execute in the organization namelessly, malignant client can upset the blockchain-based ride-sharing assistance by sending, for occasion, various solicitation/ offers while not focusing on any of them. Thusly, it is needed to monitor driver's practices and fabricate a standing framework that helps a ride to choose with certain a fitting driver for his ride demand. Therefore, to decentralize ride-sharing administrations in an important manner, security worry with regard to ride-sharing should be deliberately assessed and tended to. This predominantly requires setting two clashing targets/i.e., (i) the longing to have a straightforward framework while securing client protection, and (ii) guarantee responsibility while being unknown
.

The aim of the paper [2] is to manage the on the web/dynamic ride-sharing way arranging issue for PV frameworks, they proposes an answer based on a restricted potential quest territory for every vehicle to sift through the solicitations that abuse traveler QoS imperatives, for example, diversion, in this way, the worldwide hunt is decreased to a nearby inquiry also, the computational unpredictability is diminished. It additionally considers the solace of travelers (e.g., holding up time and diversion) and the complete travel distance of PVs. In this way, travelers can make the most of their distributed ride-imparting administrations to forfeiting a little ride comfort. Additionally, the proposed arrangement can be effectively reached out to the future worldwide ideal calculation (if it will exist) to speed the calculation time where all the planning can be changed just if the traveler has not been gotten. This article likewise investigates the decrease proportion of computational multifaceted nature utilizing the proposed arrangement. The reenactments dependent on Manhattan taxi informational collections assess the computational productivity of the proposed arrangement.

This paper [3] they introduced BlockV, a design which follows these four standards and gives a vigorous end to end arrangement. The method of employing a vehicle includes a arrangement for a passage against a ride, a reasonable installment instrument reasonable to all and a decentralized framework that guarantees reasonable, trusted, savvy exchanges. The framework which is being followed as of now is the application based vehicle imparting to many incorporated workers observing each part of the ride. The decency in current situation is trusted to be actualized by the fundamental specialist organizations, however not certain from the rider end. This sort of trust based framework makes disappointment as the internal computational techniques are not unmistakably known to rides. Thus, the vehicle sharing to be broadly acknowledged by all class of individuals, have appreciated the part of decentralized companion to peer organization of blockchain BlockV as the foundation of the design. The inspiration driving BlockV is first and foremost to guarantee the payment fairness where the separation of the passage i.e , the cost of the ride for a specific way is calculable by any companion of the organization with the way subtleties. Besides, we present the ridefairness where on account of any debate, tended to by the rider, the pernicious driver or the vindictive rider (in the event that of bogus charge) will be punished. BlockV works together with the Road Side Units (RSUs) to accomplish reasonableness in this regard.

In this work [4] the Ridecoin gives a decentralized commercial center to riders and travelers to interface and execute, taking out the dependence on a go between to control the exchange and set costs. Today, travelers hoping to book rides should associate with a unified organization who will at that point give a driver and set a cost for the outing. Likewise, drivers can't choose travelers straightforwardly however should rather depend on an incorporated company to discover and dole out travelers to them. At whatever point a guardian has the power to set costs on an exchange, the agent has gigantic force. This is a huge failure in the commercial center. Ridecoin dispenses with this go between and lets riders and drivers associate straightforwardly, and opens up value arrangement to the market members to guarantee reasonable rates while moving information proprietorship from the agent to clients. Ridecoin disposes of one size fits all estimating by opening up the value arrangement straightforwardly to showcase members. Drivers needing to work in a specific piece of town or drive towards their homes at the finish of their work day may be eager to take a somewhat lower admission. Rider who need to get some place as quick as conceivable may be eager to pay more to get gotten quicker. Ridecoin permits each market member to set the value that bodies well for them and arrange where essential. Furthermore, Ridecoin gives responsibility for to its client. Current rideshare organizations own what's more, control all client information. This unified control of information defenceless against hack and frequently adapted against the desires of client. Ridecoin flops this model around by utilizing the blockchain to give possession and control of all information to end clients.

This paper [5] proposes a plan to utilize blockchain innovation for rideshare administrations. This paper replaces the brought together power that matches drivers and riders, with block chain and a coordinating application that utilizes two sorts of coins, which supports the drivers transforming into diggers. To assess the proposed framework, this paper applies the proposed blockchain rideshare administration to a contextual analysis to mimic and locate the most un-coordinating likelihood to make drivers advantage from this framework. Besides, this paper sets up a numerical model of the fixed conveyance of drivers what's more, compute the fixed benefit of every driver in the blockchain rideshare framework.

In this work [6] the Blockchain, the establishment of Bitcoin, has gotten broad considerations as of late. Blockchain fills in as a changeless record which permits exchanges happen in a decentralized way. Blockchain-based applications are jumping up, covering various fields including monetary administrations, notoriety framework and Internet of Things (IoT, etc. In any case, there are as yet numerous difficulties of blockchain innovation such as adaptability and security issues holding back to be survived. This paper presents a thorough outline on blockchain innovation. We give an outline of blockchain architecture right off the bat and analyze some common agreement calculations utilized in various blockchains. Besides, specialized difficulties and late advances are momentarily recorded. We additionally spread out conceivable future patterns for blockchain.
These days digital currency has become a popular expression in both industry and the scholarly world. As perhaps the best digital money, Bitcoin has appreciated a gigantic accomplishment with its capital market arriving at 10 billion dollars in 2016. With an exceptionally planned information stockpiling structure, exchanges in Bitcoin organization could occur

DOI 10.17148/IJARCCE.2021.10130

with no outsider and the center innovation to fabricate Bitcoin is blockchain, which was first proposed in 2008 and executed in 2009. Blockchain could be viewed as a public record and all dedicated exchanges are put away in top notch of squares. This chain develops as new squares are annexed to it persistently. Deviated cryptography and circulated agreement calculations have been actualized for client security and record consistency. The blockchain innovation for the most part has key qualities of decentralization, persistency, namelessness and auditability. With these characteristics, blockchain can incredibly save the cost and improve the productivity.

In this work [7] Interconnected keen vehicles offer a reach of refined administrations that advantage the vehicle proprietors, transport specialists, vehicle producers, furthermore, other specialist organizations. This possibly opens shrewd vehicles to a scope of security what's more, protection dangers, for example, area following or far off seizing of the vehicle. In this article, we contend that blockchain (BC), a problematic innovation that has discovered numerous applications from cryptographic forms of money to shrewd agreements, is a potential answer for these difficulties. We propose a BC-based engineering to secure the protection of clients and to expand the security of the vehicular biological system. Remote far off programming refreshes and other arising administrations, for example, dynamic vehicle protection expenses are utilized to represent the adequacy of the proposed security design. We additionally subjectively contend the strength of the design against basic security assaults.
Savvy vehicles are progressively associated with side of the road foundation (e.g., traffic the executives frameworks), to different vehicles in closeness, and likewise more by and large to the Internet, in this way fusing vehicles into the Internet of Things (IoT). This serious level of availability makes it especially testing to make sure about shrewd vehicles. Noxious substances can bargain a vehicle, which not just jeopardizes the security of the vehicle yet in addition the wellbeing of the travelers. Mill operator and Valasek introduced a refined assault on a jeep Cherokee utilizing the remote interface of the infotainment framework whereby they had the option to distantly control the centre elements of the vehicle. The information traded by the vehicle incorporate delicate information (e.g., area) and would thus be able to open up new security challenge.

In this paper [8] we are researching ride-pooling with no more than two passenger classes. That, in the same car, will share rides. We dynamically match randomly arriving passengers with available drivers and also determine pick-up and drop-off routes. The aim is to reduce the waiting time and travel delay time of a weighted sum of passengers. A heuristic spatial-and-temporal decomposition is implemented and each sub-issue is resolved using Approximate Dynamic Programming (ADP), for which at each point we view properties of the approximate value function. Our model is comparable to the one that optimizes vehicle dispatch without ride-pooling and the one that matches current drivers and passengers without predicting demand. Using test instances produced during one peak hour based on the New York City taxi data, we perform computational studies and sensitivity analysis to demonstrate I empirical convergence of ADP, (ii) advantage of ride-pooling, and (iii) value of future information on supply-demand. We found the issue of ride-pooling with no more than two at the same time, passenger groups share rides. We hired the ADP strategy for dynamically solving the problem and maximizing value function properties. To divide the entire space and operating time into sub-regions and several times, a decomposition heuristic was developed. Numerical findings showed rapid convergence and the stability of the use of results ADP. We compared ADP with two benchmarks and showed that it can serve the most passengers, demonstrating the significance of including potential volatility of demand in decision-making on ride-pooling. ADP also resulted in shorter waiting times per rider relative to the ride-pooling benchmark, highlighting the value of pooling rides in ride-hailing systems.

In this paper [9]we suggest a system for ride-sharing that takes place jointly in the standard of sharing and operator revenue account for although the cost of consumption is fixed. We are formulating a problem of weighted graph coloring optimization that has the versatility to integrate variables that facilitate efficiency of ride-sharing while optimizing operator revenue. Applying our methodology to the New York City, USA, taxi ride dataset provides encouraging results with regard to state-of-the-art approaches. We demonstrate that our system has the ability to increase vehicle occupancy, allowing larger vehicles to be shared while assigning naturally shared rides. In comparison, relative to no ride-sharing, the proportion of passengers sharing rides and the percentage of vehicles being shared on average is more than 85 percent and 75 percent, respectively, with a decrease in the number of vehicles being used of over 60 percent. The key insight obtained from this work is that incorporating quality and efficiency of shared rides has the potential to enhance operator revenue as well. We suggested a graph coloring based algorithm for the problem of ride-sharing in this paper that can easily integrate any necessary metric for ride-sharing constraints. We demonstrate the efficiency of the algorithm based on parameters that both imply the combined quality of rides and also factor in operator benefit and reduced riders' costs. These criteria include the number of necessary cars, the occupancy index and the proportion of shared rides. We have shown that these figures have a unanimous effect on the practicality of a ride-sharing system by enhancing the standard of sharing and by adding a significant economic component.

The aim of this paper [10] in order to support both human satisfaction and resource efficiency, we propose a ride-sharing system with harmonic aggregation of user requirements and report the results of the simulation of our proposed system showing the efficiency of our process. Todays suggested ride-sharing framework modifies the time of user operation and harmonically aggregates user transfer by using versatile sections of the demands of users for their actions. They developed a demonstration framework that visualizes our future vision, portraying the proposed ride-sharing process as one scenario. The ride-sharing will be introduced in this scheme as a mix of many small personal vehicles. With simple scenarios, including part of the proposed method, it carried out our simulations and obtained results showing that without the method, the ride-sharing system with our proposed method has four times higher efficiency than that. Those who suggested a ride-sharing scheme in this paper with staggering action time and accumulation of user behavior. With many small personal vehicles in this scheme, it focused on transportation and described a ride-sharing scenario. In future work, people will inter-lock the simulation and demonstration framework. It presented the architecture of the system and a use case for this system. Then, with simple scenarios, including part of the proposed process, those who carried out our simulations. When two agents use two agents, they presume an agent shares a ride with other agents On the way to the destination, the same part of a journey and people will feel happiness supporting each other with the system's input of social rewards. It have obtained results showing that our proposed technique shows four times greater efficiency.

The main intent of this paper [11] is Blockchain, commonly regarded as one of the revolutionary technologies developed in recent years, is rapidly evolving and has the full potential to revolutionize applications with increasingly centralized intelligent transport systems (ITS). To build a stable, trustworthy and decentralized autonomous ITS ecosystem, Blockchain can be used to create better use of the legacy IT infrastructure and resources, especially effective for crowdsourcing technology. A preliminary analysis of Blockchain-based ITSS is carried out in this paper (B2ITS). It outline an ITS-oriented, seven-layer blockchain conceptual model and discuss the key B2ITS research issues on this basis. Blockchain is one of the stable and trusted architectures for the construction of the newly developed parallel transport management systems (PtMS) and the relationship between B2ITS and PtMS is thus discussed.
A preliminary review on the new blockchain technology and its future applications in transport research is discussed in this paper. It develop a seven-layer ITS-oriented conceptual model, propose the B2ITS research framework and address its main research issues. In the literature, also discuss the relationship between B2ITS and PtMS, and point out that B2ITS is a significant move forward for PtMS. Developers are now at the very start of the cycle of blockchain technology, and B2ITS through take years to come to fruition. Therefore, at this point, further research efforts are required to explore the underlying logic, novel business models and realistic B2ITS implementation scenarios.

This paper [12] computer vision, machine learning and decentralized technologies pave the way towards a future where, without humans in the loop, autonomous systems would be able to really communicate. Though self-driving technologies are a prime example of this phenomenon in its infancy. RiderS, a new privacy-first decentralized self-driving ride-sharing ecosystem, is proposed in this paper and consists of everything required to allow autonomous/self-driving vehicles to participate in a decentralized ride-sharing economy. RiderS relies at its heart on a self-sovereign biometric solution that leverages machine vision through a privacy-first biometric authentication algorithm to register and authenticate users. In order to support a self-sustained ride-sharing ecosystem, we then recommend a new decentralized architecture. This paper introduces a new geo-aware consensus algorithm for proof-of-matching, which is used to verify and reward self-driving vehicles. The main idea is that each vehicle uses its built-in computing resources to help validate transactions in order to keep the ecosystem under control while being paid for the job. Experimental results show that can perform about 10K Matches per second (KMs) using an NVIDIA Jetson AGX Xavier development kit. This analyzed the privacy aspects as well as the accuracy of our biometric solution with good matching rates. In addition, it assessed the efficiency and scalability of the proposed consensus algorithm and compared it to similar blockchains based on proof of work that produced promising results. Using reported statistics from Uber, it modelled the ride-sharing ecosystem and demonstrated that it can support Uber-scale ride-sharing through a what-if simulated exercise using our geo-location conscious consensus algorithm. RiderS, a novel privacy-first self-driving ride-sharing ecosystem, was introduced in this paper. The ability of systems to perform a proof-of-matching algorithm is at the heart of this ecosystem, which involves matching bloom filter data at high rates. This paper showed that, using embedded GPUs, it can achieve around 10K matches per second (10KMs) per node. We observed a true positive matching rate of 94.29 percent, while maintaining well over 98.68 percent rejection rates for users attempting to authenticate with other seeds of sommeone. When replacing proof-of-work with proof-of-matching, it also conducted a what-if analysis. This has shown that geo-location can certainly help increase the blockchain's scalability. Further scalability tests of the consensus algorithm, a bidding marketplace for cars, as well as a look at the economics of the ecosystem are included in future work. In order to improve the privacy intensity of the solution, it is also important to find an optimum combination of bit difference and matching speeds.

In this paper [13] , B-Ride proposes a decentralized public blockchain based ride-sharing service called B-Ride. Without depending on a trusted third party, B-Ride allows drivers to provide ride-sharing services. Both riders and drivers can

learn whether they can share rides while maintaining their travel information, including Place of pick-up/drop-off, date of departure/arrival and travel price. However, the anonymity granted by the public is abused by malicious users.
To find a better deal or to make the system unstable, blockchain to send multiple ride requests or deals, while not committing to any of them. By implementing a time-locked deposit protocol for a ride-sharing by leveraging smart contract and zero-knowledge set membership proof, B-Ride solves this issue. Later, on the agreed pick-up time, a driver has to prove to the blockchain that he/she arrived on time at the pick-up spot. The proof is done using zero-knowledge set membership proof to protect rider/driver privacy by covering the exact pick-up spot. In addition, a pay-as-you-drive methodology is applied depending on the driver and rider's elapsed distance to ensure equal payment. Furthermore, without involving any third parties, we implement a reputation model to rate drivers based on their previous behaviour to enable riders to pick them based on their device experience. Finally, it implements the protocol and deploys it on the Ethereum test network. The experimental findings illustrate our protocol's applicability to current real-world blockchains.
The decentralization of ride sharing services using the groundbreaking public blockchain called B-Ride has been proposed in this paper. In order to test the B-Ride, research and experiments were carried out. The findings suggest that both on-chain and off-chain overheads are realistic for B-Ride. In addition, it illustrates the feasibility of addressing two key goals in the use-case of the decentralized ride sharing atop the public blockchain: one between transparency and privacy and the other between the accountability and anonymity of device users. The proposed time-locked deposit protocol guarantees that all fraudulent drivers/riders are secured against malicious conduct. Furthermore, in BRide, the proposed reputation management system monitors the actions of drivers, encouraging them to act honestly in the system. Otherwise, for future journeys, they will not be chosen. Finally, the passenger will have a ride and the driver will collect the fare using the pay-as-you-drive methodology in a trust-less environment.

In this paper [14] propose a new ride-sharing model in this paper, where each driver needs that when sharing with a passenger, the shared route percentage (SRP, the ratio of the shared route's distance to the total traveled distance of the driver) exceeds her estimated rate (e.g., 0.8). This takes two versions of this dilemma into account. The first takes several drivers and several riders into account and tries to quantify a collection of driver-rider pairs in order to optimize the overall SRP. As the maximum weighted bigraph matching issue, model this issue. This implies an accurate, precise algorithm and an effective approximate solution with an error-bound guarantee. The second takes multiple drivers and a single rider into consideration and tries to find the top-k drivers with the highest SRP for the rider. They develop pruning methods and suggest a best-first algorithm to gradually pick drivers that are highly likely to be in the top-k performance.

In this paper [15] One of the famous e-commerce operations, the E-auction, enables bidders to bid the goods directly over the internet. As for sealed bid, for the intermediaries, the extra transaction cost is required because the third party is the essential position between the buyers and the sellers during the auction to help trade both. Moreover, it never guarantees the confidence of a third party. To address the issues, the low transaction cost blockchain technology is used to build the public bid and sealed bid smart contract. The smart contract, proposed in 1990 and implemented through the Ethereum blockchain, will ensure that all transactions are registered in the same yet decentralized ledgers to ensure the bill is secure, private, non-reputable and inalterable. The smart contract consists of the auctioneer's address, the start time of the auction, the deadline, the current winner's address, the current maximum price. The accounts are generated in the experiments via the Ethereum wallet. In the miner point, the MinerGate is used to receive cash to pay the transaction fee in the miner process. The blockchain nodes are synchronized at the recorder level to create smart contracts. This paper offers a blockchain-based E-auction system to ensure confidentiality, non-repudiation, and unchangeability of electronic seals. In carrying out this work, also expect to face possible challenges. In the implementation of this job, the expect to encounter possible problems. In smart contracts for sealed orders, the bidders and bidders come because of the complexity of the deal, say they can call the wrong contract feature. For eg, to open all bids, the bidder unintentionally calls Reveal(), so that the bid must be terminated and re-arranged. It will set the authority judgment for various functions for this purpose and will execute the function before first deciding if the caller can perform this function.

In this paper [16] the decentralized technology of transaction and data management that characterizes the blockchain can have a huge effect on supply chains of production. The aim of this paper is to investigate the applicability of blockchain technology in the composite materials/carbon fibre supply chain, in particular the manufacture of semi-finished material structures and components such as pre-pregs (preimpregnated) requiring temperature-controlled transport and storage conditions. For the purpose of tamper-proof history of product development, provenance, shipping, handling and storage, distributed ledger/blockchain technology may be used in composite materials. A main supplier to many industries is the composite materials industry. Components and structures made of composite materials using semi-finished prepregs are used in applications that, as is the case with aerospace and medical equipment, must comply with stringent regulations. The use of blockchain technology in the manufacture of composite/prepregs structures and components has the ability to meet any conceivable requirements in highly regulated industries including tamper proof and provenance-tracking. In the supply chain of composite materials, specifications for raw materials are sent to suppliers. The blockchain can be used to record any request for inspection concerning the specifics of raw materials until they arrive and are ready to be used in the manufacture of semi-finished materials. In the blockchain, the production of pre-pregs and their use in the production of components and structures are documented. In addition, some main operations that can be submitted to the blockchain during the development of finished products are the quality of cutting and drilling, bonding, surface treatment, and assembly, as indicated in the work by Wang et al. Furthermore, basic activities that facilitate development activities, including procurement, inspection and quality audits, may be able to issue certificates that can be stored in the blockchain. While in many conventional applications, the adoption of composite materials and, in particular, carbon fiber is still prohibitively costly, the use of blockchain technology can be the catalyst necessary for the manufacturing industry to achieve operational benefits. This may include: reduction of lead times, processes that are tamper proof, transport, storage, and provenance.

In this paper [17], according to statistics from the Taiwan Ministry of Education, around one million graduates go to nations, high schools or tertiary institutions every year, some to continue attending and some to be ready to enter the workplace. All sorts of outstanding performance certificates, score transcripts, diplomas, etc., will become an important guide for the admission of new schools or new works during the course of study. As schools create different awards or diplomas, only the names of the schools and the students are given. Events that enable the graduation certificate to be forged are frequently found because of the lack of an efficient anti-forge system. A digital certificate scheme based on blockchain technology will be proposed to address the issue of counterfeiting certificates. The digital anti-counterfeit and verifiability certificate could be created by the unmodifiable property of blockchain. The process in this method for issuing a digital certificate is as follows. First, create a paper certificate electronic file followed by other relevant data in the database, when calculating the electronic file for its hash value. A related QR-code and inquiry string code will be generated by the device to affix to the paper certificate. Via cell phone scanning or website inquiries, it will include the demand unit to check the validity of the paper certificate. The framework not only improves the integrity of different paper-based certificates through the unmodifiable properties of the blockchain, but also electronically eliminates the failure risks of different types of certificates. One of the main aspects of blockchain technology is data protection. The Blockchain is a massive, open-access online ledger in which the same data is stored and validated by each node. Using the suggested blockchain-based framework decreases the risk of forgery of certificates. In the method, the certificate application process and the automated certificate awarding process are open and transparent. Thus, businesses or organizations may ask for information from the system on any certificate. In conclusion, information quality and confidentiality are guaranteed by the framework.

In this paper [18], Blockchain is gaining ground and it is possible to name one of the omnipresent trends these days. Despite the fact that fault finders question their durability, protection and stability, due to its disproportionate effect on projects, it has officially changed the way of life of numerous people in a few regions, as well as organizations.
In addition, given that the highlights of blockchain innovation ensure stronger and more convenient administrations, it is imperative to think about the security, security issues and complications behind innovative innovation. he selection of applications for blockchain includes both open and public health, environmental, automotive, Internet of Things (IoT) and risk management services are included. In the spotlight, many speak about using the blockchain data framework for different applications. However, a systematic study of advanced technologies and applications has not yet been carried out by an expert. In this paper, by studying its architecture of varying consensus algorithms over and above security and data protection problems and opportunities within blockchains, we aim to conduct a comprehensive analysis on blockchain technology. Blockchain can be compared to a degree with the internet a few decades ago. Since the core of blockchains is safe and stable, this invention will progress step by step with many essential applications that involve protection and non-disavowal. Despite the fact that there are still a few barriers to blockchains and it is difficult to upgrade various imaginative applications, blockchain is likely to end up with the breakthrough that everyone will step towards with its development.

This paper [19] deal with different consensus algorithm in blockchain. The core technology of Bitcoin is Blockchain. Blockchain is gaining more and more interest in many places with the appreciation of value and stable activity of bitcoin. The features of Blockchain are decentralization, stability, confidentiality, and non-modifiability. It has the ability to change the design of the network. The consensus algorithm plays a crucial role in preserving blockchain protection and performance. The use of a correct algorithm will result in a significant improvement in blockchain application efficiency. We reviewed the basic concepts and features of consensus algorithms in this paper and examined the efficiency and implementation scenarios of various consensus mechanisms. It also provided a technical guide to choosing an acceptable consensus algorithm and summarized the shortcomings of blockchain technology and future development. It also provided a technical guide to choosing an acceptable consensus algorithm and summarized the shortcomings of blockchain technology and future development. The features of decentralization, stability, security, non-modifiability and so on are present in Blockchain. The blockchain is gaining more and more interest in various fields with the growth of technology. This paper reviews the normal consensus algorithms that are used in the blockchain systematically. The central blockchain technology is the consensus algorithm, but current research on the consensus process is still in its infancy. There is still a very unusual consensus algorithm specifically built for various scenarios.

In this paper [20], Blockchain is behind the crypto-currency and Bitcoin backbone technology. Blockchain is, by definition, a distributed ledger in which transactions are documented in an incorruptible and non-modifiable way. Blockchain technology is currently envisaged as a powerful platform for open-access networks, decentralized collection and exchange of information systems, etc. Due to the lack of an extensive survey on the current decentralized consensus processes in Blockchain technology, this analysis is motivated. Therefore, a detailed analysis of the distributed consensus processes has been given in this paper. A comparative study of the consensus protocols based on the Blockchain form is also seen in addition to this. The Blockchain technology has drawn interest from different dimensions with the evolution of ICT. The key Blockchain technology is the Consensus algorithm, but ongoing research into consensus algorithms is still in its initial stage. Hence, a detailed review of the existing consensus algorithms has been presented in the paper. It is easy to achieve robust consensus among large numbers of untrusted nodes using complex computations in the case of permissionless systems, although the finality of the transaction remains non-deterministic. On the contrary, permissioned Blockchain offers high efficiency while losing the degree of decentralization in less time.

3 CONCLUSION

We have suggested in this paper that ride sharing services be decentralised using the revolutionary blockchain for the public. Study and experiments were carried out in order to determine proposed plan. In the use-case of the decentralised ride sharing atop public blockchain, the system can resolve two main goals: one between transparency and privacy and the other one between the accountability and anonymity of system users. The proposed time-locked deposit protocol guarantees that all fraudulent drivers/riders are protected from malicious action. In addition, the proposed system of reputation management monitors the actions of drivers, encouraging them to act honestly in the system. Otherwise, for future journey ,they will not be chosen. Finally, in a trust-less setting, the ride will have a trip and the driver will get the fare using the technique of pay-as-you-drive.

ACKNOWLEDGMENT

We utilize this opportunity to convey our gratitude towards all those who have helped us directly or indirectly for the completion of our work. We deeply and wholeheartedly thank **Mr. Sreeraj R** -HOD, Computer Science and Engineering for his extreme valuable advice and encouragement. We especially thankful to our guide and supervisor **Mr. Deepak K N** -Assistant Professor, Computer Science and Engineering for giving me valuable suggestions and critical inputs in the preparation of this paper. We would like to extend our sincere gratitude to all faculty of Computer Science and Engineering department for the support and suggestions that helped us in the development of our work to what it is now. We thank our parents and friends for the mental support provided during the course of our work at the times when our energies were the lowest.

REFERENCES

[1] Mohamed Baza, Noureddine Lasla, Mohamed Mahmoud, Gautam Srivastava and Mohamed Abdallah, “B-Ride: Ride Sharing with Privacy-preservation,Trust and Fair Payment atop Public Blockchain,” 2019, IEEE

[2] Ming Zhu , Xiao-Yang Liu , and Xiaodong Wang, “An Online Ride-Sharing Path-Planning Strategy for Public Vehicle Systems,” 2018 Transactions On Intelligent Transportation Systems, IEEE

[3] Panchalika Pal and Sushmita Ruj, “BlockV: A Blockchain Enabled Peer-Peer Ride Sharing Service,” 2019 International Conference on Blockchain (Blockchain), IEEE

[4] RideCoin-Whitepaper “An incentivized, blockchain-based peer-to-peer transportation platform,” 2018 February Article on Ridecoin

[5] Kosuke Kato, Yutong Yan, Hiroshi Toyoizumi, “Blockchain Application for Rideshare Service,” 2018 International Conference on Blockchain, IEEE

[6] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, 2017, pp. 557-564.

[7] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A distributed solution to automotive security and privacy," IEEE Commu- nications Magazine, vol. 55, no. 12, pp. 119-125,2017.

[8] Xian Y^{u} ,Sigian Shen, “An Integrated Decomposition and Approximate Dynamic Programming Approach,” 2019

DOI 10.17148/IJARCCE.2021.10130

[9] Saatvik Jain, Pravesh Biyani, “Improved Real Time Ride Sharing Via Graph Colouring,” 2019, IEEE Intelligent Transportation Systems Coference (ITSC) 27-30-2019

[10] Satoko Itaya, Rie Tanaka, Naoki Yoshinaga, Taku Konishi, Shinichi Doi, Keiji Yamada, “Proposal of Ride-Sharing System using Harmonic aggregation of user Demand,” 2011 IEEE 36th Conference

[11] Yong Yuan, Fei-Yue Wang, “Towards Blockchain-Based Intelligent Transportation Systems,” 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)

[12] Luis Angle D. Bathen, German H. Flores, Divyesh Jadav, “RideS:Towards a Privacy-Aware Decentralized Self-Driving Ride-Sharing Ecosystem,” 2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)

[13] Mohamed Baza, Noureddine Lasla, Mohamed Mahmoud (Member IEEE), Gautam Srivastava (Senior Member IEEE), Mohamed Abdallah (Senior Member, IEEE), “B-Ride: Ride Sharing with Privacy-preservation Trust and Fair Payment atop Public Blockchain,” 2019

[14] Na Ta, Guoliang Li, Tianyu Zhao, Jianhua Feng, Hanchao Ma, Zhiguo Gong, “An Efficient Ride-Sharing Framework for Maximizing Shared Routes,” 2018 IEEE 34th International Conference on Data Engineering

[15] Y. Chen, S. Chen and I. Lin, "Blockchain based smart contract for bidding system," 2018 IEEE International Conference on Applied System Invention (ICASI), Chiba, 2018, pp. 208-211

[16] Adrian E. Coronado Mondragon, Christian E. Coronado Mondragon, Etienne S Coronado, “Exploring the Applicability of Blockchain technology to Ehance Manufacturing Supply Chains in the Composite Materials Industry,” IEEE International Conference on Systems Innovation 2018

[17] J. Cheng, N. Lee, C. Chi and Y. Chen, "Blockchain and smart contract for digital certificate," 2018 IEEE International Conference on Applied System Invention (ICASI), Chiba, 2018, pp. 1046-1051.

[18] Dr S. Velliangiri, Dr P. Karthikeyan, “ Blockchain Technology: Challenges and Security issues in Consensus algorithm," 2020 ”nternational Conference on Computer Communication and Informatics (ICCCI-2020), Jan 22-24, Combtore,INDIA

[19] Du Mingxiao*, Ma Xiaofeng*, Zhang Zhe**, Wang Xiangwei*,Chen Qijun*, “A Review on Consensus Algorithm of Blockchain,” 2017 IEEE International Conference on Systems, Man and Cybernetics (SMC) Banff Center, Banff, Canada, October 5-8-2017

[20] Soumyashree S. Panda, Bhabendu Kumar Mohanta, Utkalika Satapathy, Debasish Jena, Debasis Gountia, Tapas Kumar Pantra, “Study of Blockchain Based Decentralized Consensus Algorithm,”