Sixth Int. Conf. on Computer Systems, Data Communication and Security, CDCS

Blockchain with Machine Learning

Suruchi Dedgaonkar[1], Dr. Priya M Shelke[2], Parth Kohli[3], Akash Kumar[4] and Hrithik Singh[5]
[1-5]Vishwakarma Institute of Information Technology, Pune, Savitribai Phule Pune University, Pune, India
Email: suruchi.dedgaonkar@viit.ac.in, priya.shelke@viit.ac.in, parth.21911195@viit.ac.in, akash.21911057@viit.ac.in, singh.21910952@viit.ac.in

***Abstract*—While machine learning algorithms have developed into effective tools for addressing real-world issues, some have begun to doubt their reliability. First off, data poisoning assaults may be a threat to machine learning systems. Hackers may attempt to modify system performance by changing the data that has been gathered or by adding poisonous instances that they have created. Second, if there are no traceable logs or training histories, it is challenging for humans to comprehend judgments made by machine learning algorithms. Thirdly, finishing the model training procedures still significantly depends on centralized servers. Finally, the steps of model creation are not automated, and human involvement may introduce biases into the final system. Smart contracts and blockchain technology have demonstrated a lot of promise in addressing these problems with a conclusion. The function of ML takes a lot of computing power and using them in real-time scenarios with IoT is difficult as IoT devices can't handle the high computations. Thus, MEC (Mobile Edge Computing) is a solution to the problem as it can perform offloading of workload to the Edge of Internet thus making it possible for IOTDs to carry out their function. Blockchain Technology helps in data privacy and its decentralized and immutable properties make it the best option to store data. The number of applications that blockchain and machine learning provide is immense as mentioned further in the paper making it the finest choice for several use cases.**

I. INTRODUCTION

Machine Learning and Blockchain are two of the prominent technologies that are widely used in current times. They are both powerful technologies on their own, so when combined, they can provide a variety of useful applications that can help us solve some crucial real-world problems. In this paper, we will look at some research that had the aim of combining blockchain technology and ML for the greater good and will also go over some interesting results. This paper will cover domains like:

1. Security of MPML systems using blockchain technology
2. Security in communication networks using Blockchain and ML technologies
3. Use of blockchain with ML in the healthcare domain
4. Using blockchain and ML to detect forgeries in the education sector
5. With mobile edge intelligence
6. Fraud detection
7. Supply chain management

Some of the technologies discussed in the paper are made open source like the Biscotti.

ABBREVIATIONS AND ACRONYMS Machine Learning (ML), Multi-party Machine Learning (MPML), Stochastic Gradient Descent (SGD), Verifiable random functions (VRFs), Deep Learning (DL), Application (app),(VR) virtual reality, (AR)augmented reality

Grenze ID: 02.CDCS.2023.6.506_1

II. LITERATURE SURVEY

Nowadays, Machine Learning has become an important part of the digital world. And, to get a good ML model we require a lot of data to train it on. It is like oil for the vehicle. The more you put it, the more it will run, also, one more thing that is to be noted is that you need to have a good quality of "oil" otherwise it damages the vehicle, similar to the fact that the data provided to the model must be clean and of good quality and not misleading.

Now, to get a huge amount of data, rather than using a single source, we can use multiple sources to feed the data and multiple people can train the model using their data. This is called multi-party machine learning in which multiple peers can train the ML and use their data. So, multi-party ML needs to use distributed systems, which have their own set of challenges. Mainly the security of both client and the model.

For training a multi-party ML (MPML) model, the users might need to share their data which can be potentially sensitive data with a centralized third-party service provider. Some users may refrain from sharing it as they might not trust the third party or their peers which is a very valid reason. Federated learning, the state-of-the-art in offering safe multi-party machine learning (ML), was developed to prevent this: In this approach, the model updates are integrated and aggregated using a secure protocol while the data is kept on the owner's device. Clients must have faith that the centralized service won't exploit their data's byproducts as part of its assumed to be a reliable infrastructure for coordination. Furthermore, certain harmful clients can carry out a poisoning attack and impair the model's overall performance.

Previous works have shown that in federated learning the attackers can make changes to the model's parameters which can negatively affect the whole model which is known as a poisoning attack as we have discussed before. Another way the attacker can attack is by appearing as an honest data source and attempting to deduce the sensitive training data's properties through observation of the target's peer-shared model updates.

Through these two issues, poisoning attacks and data leakage have been dealt with separately before but not together. Also, the solutions were not private and decentralized, which opposes the idea of avoiding a third party or even a central authority. This is where "Biscotti" comes in. It is a public Peer-to-peer system that is decentralized that plays an integral part in designing the privacy-preserving MPML with a blockchain ledger. The point to be noted is that here instead of on-blockchain's layer-2, the ML applications, layer-1 is used in which a blockchain consensus protocol called "Proof-of-federation" (PoF) is used which combines avant-garde in defenses for federated learning and makes them usable in decentralized Peer-to-Peer environments. PoF is based on the PoS(Proof-of-Stake) consensus. Here, in Biscotti, the stake is defined as an indicator of a peer's value to the system. Peers' stake increases as they contribute more helpful model changes or help with the consensus building. Additionally, there are two important presumptions made here. The first is that the stake ownership of peers is openly accessible in the blockchain's current state. Two, the system as a whole has at least 70% of the honest and correctly bootstrapped stakes at any given time. The initial source of the stake allocation might be a reputation score that rival agencies provide, an online data-sharing marketplace, or supplementary data from a social network. Based on the stake, Biscotti coordinates the work among the peers.

By combining consistent hashing based on the PoF with verifiable random functions, Biscotti picks critical roles for peers (VRFs). The coordination of the privacy and security of model updates will be aided by these peers. A gang of complicit peers cannot take control of the system without a large enough stake thanks to PoF.

To prevent poisoning of the model, Biscotti uses the Multi-Krum defense which is a Byzantine-tolerant aggregation scheme to validate by comparing an SGD update to the updates supplied by other peers assuming baseline validation models are not available to peers. Other algorithms like median/trimmed mean and Buyan can be used here too but Biscotti uses Multi-Krum. Although not immune to all poisoning methods, Multi-Krum and associated aggregation methods are successful against some kinds of attacks. and any aggregation method that relies solely on model updates may typically be supported by Biscotti. Then how does Multi-Krum function? In essence, it disallows model modifications that significantly veer from the general trend of updates. In this version, the committee of validation peers is chosen by majority vote for each round, and each member utilizes Multi-Krum to eliminate anomalous updates, ensuring resolution against k Byzantine adversaries in a system with a total of m clients where $(2k+2<m)$.

For safe aggregation, Biscotti additionally makes use of Shamir secrets, and it offers privacy using differential private noise.

Why not use Byzantine Fault Tolerant (BFT) Protocols? A robust protocol like BFT is unnecessarily constrictive for ML workloads since ML does not require high consistency or a majority to converge. Blockchains (distributed ledgers) has emerged as a more suitable framework for enabling private, verifiable, crowd-sourced computing.

Biscotti's performance, scalability, capacity for resistance against attacks, and churn tolerance were evaluated on the Azure platform and it was found that it can train an MNIST (Modified National Institute of Standards and Technology dataset) softmax model on a 60000 picture dataset in 266.7 minutes with 200 peers, and it can resist up to around 30% of hostile peers. The architecture of Biscotti was also shown to be resistant to information spillage attacks in which the information about a client's SGD update is required, it was also resistant to attacks that poison a system with information from earlier works. Additionally, Biscotti demonstrated fault tolerance by handling nodes that churn every 1.875 seconds and offering model training that converges despite node churn. Go and Python was used to implement Biscotti, which was made available as an open-source project. Go was utilized to manage the networking and distributed systems parts of the design, while PyTorch, a Python ML framework, was used to provide SGD updates and noise while training.

A. Limitations of Biscotti

- In a decentralized system with node churn, Multi-Krum may not always be feasible since it requires a high number of sincere samples in each round to be successful. Additionally, it could disallow updates from peers that have non-iid data, such as a peer with just one class in the model.
- Due to communication overhead, large DL models with a huge number of parameters are not presently supported.
- Biscotti is susceptible to attacks that make use of privacy leaking from the aggregate model itself since updates already existent in the ledger are not given additional noise. In addition to differential privacy, a regularisation like dropout can be used to counteract these attacks.
- Stakes: A client may be chosen as an aggregator, verifier, or noiser depending on the stake. Because they participate more to build up more stake and their stake is linked to a financial incentive at the conclusion of training, it is expected that a large stakeholder won't cause the system to become unstable. These are only generalizations, however, they can occasionally be wrong. For example, a hostile client could seem to be honest in order to gain money and then flip to acting maliciously in order to topple the system [1].

Machine learning used with Blockchain systems can produce wonderful results. One such application is an Intrusion Detection System (IDS). IDS is used to identify cyber threats and possible incidents and of course intrusion detection by some malware. The traditional works employed a signature-based approach to detect a certain sort of pattern, hence a robust IDS is necessary in their stead. But, to detect the attack patterns and intrusions ML models can be used to analyze the data traffic. Now, blockchain-based smart applications usually have a huge amount of data traffic, So, creating effective and efficient algorithms to evaluate the data is necessary. ML models are used because it basically finds a pattern in the data. In supervised ML models, both input and output are given, whereas, in unsupervised ML algorithms, only the input is given, and based on that the algorithm finds a pattern in the input data and both of them predict the output or in this case find the patterns in which malicious attacks happen.

Security concerns are addressed layer-by-layer in the communication network of blockchain-based smart apps. Malicious packets can be used to force the network to build bogus consensus in specific situations, which are addressed at the network layer. Malware is an example of an issue that is handled at the application layer. A naive approach to the network layer problem may be to employ a firewall to make sure that packets adhere to certain security requirements. However, assaults are becoming more complex and less predictable, which allows them to mislead and get around the simple answer. This may be avoided by utilizing ML models to evaluate packet header data in real-time using previous data, which enables the detection of new and evolving attack behaviors. Malware that affects endpoints like workstations, servers, and mobile devices can also be categorized using ML techniques [2].

This approach, which combines these two radiant technologies, is recommended as a solution to problems like fake certificates and academic transcript forgeries. The theory behind this is that, if these technologies can be combined, a system can be developed that uses blockchain to store student data and ML to precisely predict the future job roles for students after graduation, thereby preventing the problems of further counterfeiting and insecurity in student achievements. Furthermore, ML models will be used to train and forecast authentic data. The school will have access to a formal, decentralized database of the records of its former pupils through the usage of this technology. This approach also gives employers a platform to look into the academic records of potential hires. Students can upload academic material in their e-portfolios on websites like LinkedIn, a platform for keeping professional profiles. Students, companies, and other industries will find it easier to obtain consent for student data as a result. Any ML-based project must begin by gathering information about the relevant subject. 1540 students who had completed the computer programme at India's Vishwakarma Government

Engineering College were polled to create the dataset using a Google form that asked various questions regarding their academic backgrounds. It contains the student's cumulative grade point average (CGPA) as well as other data, such as grades from the 10th and 12th grades, participation in technical projects and quizzes, rank, gender, the number of backlogs, other technical events, and the number of athletic successes. Another element of the information is the name of the student's school board.

Out of all the machine learning (ML) classifiers evaluated on the dataset to predict the employment position based on the student's academic records, the SVM and Extreme Gradient Boosting generated the best results. After then, blockchain was introduced into the ML project to provide a novel perspective on security for an established centralized database system. The exact and validated data that is accessible for model training is made more interesting by a source of data that is genuinely dependable, such as blockchain [3].

Recent advances in machine learning, mobile edge computing (MEC), and the Internet of things have helped artificial intelligence (AI) become a viable technology (IoT). According to conventional machine learning techniques, the training data must be obtained and processed on centralized servers. Recently, new decentralized machine learning techniques and mobile edge computing have made it feasible to teach IoT devices utilizing device data. IoT devices can assign training responsibilities to MEC servers to apply AI at the network's edge. However, those distributed edge intelligence frameworks also bring forth some fresh difficulties, like data security and user privacy. Blockchain has been viewed as a potential solution to these issues. Blockchain is well known for its high scalability, privacy protection, and decentralization as a distributed smart ledger. This technology also includes trusted immutable data records and automated script execution. For IoT devices, machine learning is a type of computational task that has a high workload (IoTDs). These inexpensive IoT gadgets often run on batteries. On the one hand, running computational processes requires a lot of energy, such as when training machine learning models. On the other hand, IoTDs with small physical sizes cannot use the necessary powerful microchips. The aforementioned problems can be solved by mobile edge computing (MEC). IoTDs might implement machine learning algorithms to actualize AI by outsourcing complicated learning processes to the edge of the internet. IoT data breaches might result in harmful assaults on people. Thankfully, blockchain has promise and is appropriate for MEC. MEC and blockchain integration is a beneficial combination. Blockchain, for instance, gives MEC data protection and privacy. For another, MEC can increase the efficiency and scalability of blockchain [4].

In e-banking and online transactions, fraud and anomalies are widespread issues. These issues also exist in the Bitcoin network. However, just as the financial industry develops, fraud and anomaly strategies do as well. Additionally, blockchain technology is being touted as the safest way to combine finance. However, numerous scams are also on the rise each year along with this cutting-edge technology. Thus a secure method of fraud detection that is based on blockchain and machine learning. XGboost and RF are two machine-learning algorithms that are used for transaction classification. The dataset is trained using machine learning approaches based on integrated and fraudulent transaction patterns, which also anticipate future incoming transactions. To identify fraudulent transactions in the Bitcoin network, machine learning algorithms are linked with blockchain technology. The XGboost and random forest (RF) algorithms are employed in the proposed model to categorize transactions and forecast transaction trends. To evaluate the models' correctness, their precision and AUC are computed.

An analysis of the suggested smart contract's security is also done to show the dependability of the solution. In order to protect the recommended system against attacks and vulnerabilities, an attacker model is also provided. In machine learning, data imbalance is a major problem if the distribution of classes is seriously out of balance. Machine learning algorithms lose accuracy when the amount of data is unbalanced. An increase in size occurs when one class has more instances than another. . In order to address this problem, SMOTE is used, and fictitious samples are generated at random for the minority class. With this approach, the overfitting problem caused by data random oversampling is resolved. It is based on the principle of random sampling, which involves choosing a data point from a minority class.

SMOTE's major task is to synthesize minority class samples. The algorithm is able to discern between real and counterfeit data owing to this categorization. The simulation results show that the recommended strategy successfully identifies transaction fraud. Two attacker models are also tested to see how effectively the system can defend itself against vulnerabilities and attacks. The suggested approach is resistant to Sybil and double-spending attacks [5].

Medical knowledge may be found in abundance in healthcare data, which is a valuable resource. Medical databases will be huge, complicated, diversified, and time-varying if they are constructed appropriately. The key problem today is to effectively store and interpret this data so that people can profit from it. One of the largest obstacles for researchers is heterogeneity in the healthcare industry, namely in the form of medical data. This

data may also be referred to as huge or large-scale data. Separately, both blockchain technology and the cloud environment have demonstrated their viability. Although there is interesting potential for combining these two technologies in the healthcare sector. Blockchain is a distributed, extremely secure networking system made up of several nodes or computers. It is altering how medical data is exchanged and kept on hand. It streamlines the process, monitors the data's quality and security, and lowers maintenance costs. The management and storage of digital medical records in a cloud environment are made possible by a platform built on the Blockchain.

To complete a transaction, the user will send a request. The request will be submitted to the planned blockchain-based cloud architecture, which would employ the cryptographic credentials to confirm the user's identity. A request to store, process, transport, or retrieve medical data from the network may be made when the request and user are validated by the system. When the verified request is approved, a new block with the details of this transaction and the updated data state is added to the blockchain. The user receives what he or she requested, and the transaction is finished [6].

Medical data must be shared across institutions for patients to get excellent collaborative care and clinical choices. Medical data privacy entails making sure that only authorized individuals, acting with the knowledge and consent of the patients, are able to access the health records. Because it is both an ethical and legal need to secure patient clinical data, it is essential to any healthcare system. Despite the significance of exchanging medical data, current healthcare systems have not done enough to prevent the misuse of patients' sensitive information, whether on purpose or accidentally. The need for a clinical transaction system that enables people to access, track, and control their medical information is critical. In this work, the study suggests suitable improvement in healthcare systems by addressing information security and privacy, (ii) resolving the issue of provider distrust, and (iii) promoting scalability of healthcare interoperability. It offers numerous elements of a patient-centered healthcare system employing smart contracts via blockchain technology, building on these core findings [7].

In recent years, blockchain technology has become widely deployed across a range of application industries to enhance data privacy, system reliability, and security. Despite being an effective tool, the blockchain is not impervious to cyberattacks. For instance, recently (January 2019), a successful 51% assault on Ethereum Classic exposed security flaws in the technology. Attacks may be viewed from a statistical standpoint as an aberrant finding that strongly deviates from the norm. The objective of the science of machine learning is to identify insights, patterns, and outliers in massive data sets. Consequently, it may be used to identify blockchain attacks. This study develops an anomaly detection system based on a deep learning encoder-decoder model that is trained using aggregate data gleaned from monitoring blockchain activity. In-depth historical logs of the Ethereum Classic network have been used in experiments to demonstrate the model's capacity to accurately identify assaults that have been made public. Its strategy is first to offer a complete and workable method to monitor the security of blockchain transactions [8].

Pharmaceutical businesses have struggled to track their products through the supply chain for a few decades now, allowing counterfeiters to include their bogus pharmaceuticals in the request. Inauthentic medications are considered to be a serious problem for the pharmaceutical industry worldwide. According to estimates, US pharmaceutical businesses suffer an annual business loss of almost $200 billion as a result of these phoney medications. These drugs may not enable the cases to recover the complaint but have numerous other risky side effects.

III. Proposed Methodology

A new blockchain and machine literacy-based medicine force have been proposed and put into effect.

system for chain operations and recommendations (DSCMR). The system has two components. The two key modules are machine literacy-based medicine and blockchain-based medicine. consumer suggestion system

In the first module, the Hyperledger fabric-based medicine force chain operation system is installed and is capable of continuously monitoring and tracking the medication supply process in the intelligent medical system. On the other hand, the machine learning module uses the N-gram and LightGBM models to suggest the best-rated or fashionable medications to the visitors of the pharmaceutical establishment.

These models were trained using a well-known, widely accessible dataset of medical reviews provided by UCI, an open-source repository for machine literacy. Finally, also perform several tests to evaluate the efficiency and usability of the system, and the machine learning module is also integrated with this blockchain system with the aid of the REST API. This system aids pharmaceutical firms in excluding the issue of phoney pharmaceuticals and a large growth in revenue. Can expand the network as it develops and use it in real-time pharmaceutical

firms to test the effectiveness and authenticity of the approach. Additionally, can improve the sensitivity and effectiveness of the machine literacy models [9].
Automotive assiduity is supposed to gain some advantages grounded on three main parameters, i.e., translucency, trust, and traceability. Generally, technology is divided into two main corridors: limited access and free access for druggies. It's like a book accessible to the whole world, but it isn't possible to make any changes to it. The elaboration of using smart contracts simplified force chain operation. Blockchain in the automotive assiduity provides translucency and vehicle payload optimization grounded on digital connections, furnishing logistic process, and price control information. Using the distributed tally gives a high translucency position.
Presented as an ongoing database that limits the number of answers from guests to store a large quantum of information. This fashion arranges the business records, authorizing purchases and vehicle dealers to go through the vehicle lifecycle. result in swapping the suppliers, manufacturers, and guests' relations [10].

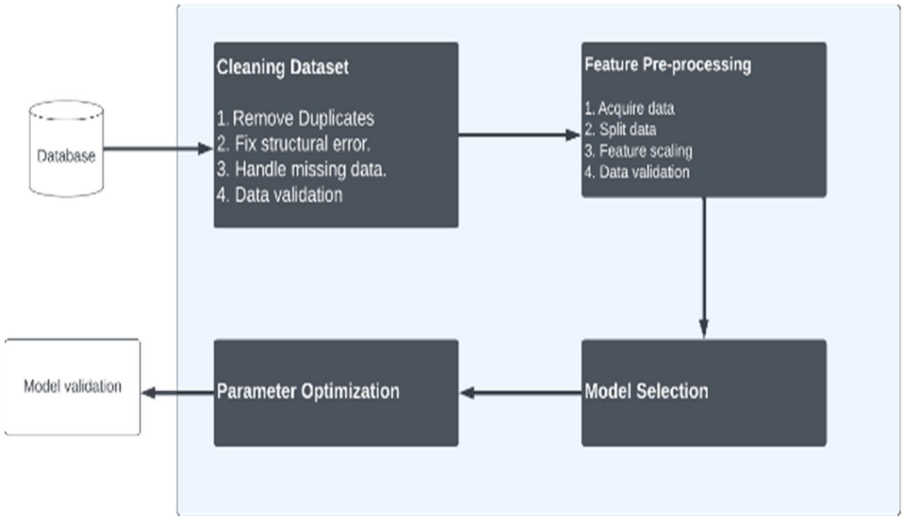

Figure 1: Validity process in the automotive model

In fact, with the present technology breakthroughs, fraud incidents are increasing. Real fiscal sale information is rarely available due to the lack of an inter-organizational community and sequestration initiatives. However, for data-driven technologies like machine literacy to function accurately in real-world systems, they need real data. In order to facilitate inter-organizational collaboration and establish a robust Machine Literacy (ML) algorithm for e-commerce fraud discovery, this study suggests a blockchain and smart contract-based strategy. The suggested solution secures the sequestration of the data using blockchain. The network's smart contracts enable total system automation. From cooperative data provided by the organizations linked to the blockchain, an ML model is gradually enhanced.
Implemented an incentive mechanism that adapts to the difficulty position when simplifying a model to encourage the associations. The difficulties encountered in simplifying the ML model are cited as the basis for the associations. The Blockchain network is benchmarked under many unusual circumstances and under random quantities of data to evaluate its authenticity. Mining criteria have been created to make it easy to mine the block.[11]
Amongst the most popular forms of artificial intelligence, algorithms derive conclusions by analyzing vast large datasets. It consists of algorithms that allow information on their own, without assistance from humans.
AI technology is an overall phrase for the health sector that brings together a range of technologies that enable robots to sense, comprehend, move and grow. Options presented by ai - powered span a range of medical specialties, diagnosis, wearables, and virtual assistants, assisting hospital businesses in meeting rising connectivity standards with online client needs.
In 2015, medication administration errors and misinterpretation caused 10% of all fatalities in the US. The use of AI technology in diagnostics and medical imaging has grown dramatically, giving healthcare practitioners and scientists ideal practical practice. Neural learning can improve assessment in medical imaging to detect malignancies and visual impairment, but also eliminate problems and errors in test outcomes, via quickening standardization or measurement (DR).

It is the world's fourth AI firm that creates healthcare machine learning algorithms technologies to enhance radiological diagnosis. By purpose of studying a system's health information including radiological images, electrocardiograms, and blood tests, the platform enables doctors to better understand a patient's current health.

A. Disease Prediction

Numerous patient data are managed by the health industry. Medical practitioners can cure a wide range of diseases before they manifest using ml algorithms to store and evaluate the data. Data harvesting is now employed to develop early detection systems.
AI is used by Freenome in preventive care, blood work, and medical testing. This enables the early detection of cancer and the later development of novel therapeutics.

B. Surgery and Emergency Department

The da Vinci Surgical System, which was created 15 years ago, was the first surgical robot to be FDA-approved for general laparoscopic surgery. Since then, more surgical robots with AI and machine learning capabilities have been unveiled. Preoperative medical information and operational parameters can be combined with cognitive robots to direct and enhance the accuracy of physician tools.
IBM Watson can respond to the needs of surgeons thanks to its excellent medical cognition and NLP skills. The AI-powered technology can track blood pressure in real time, offer guidance during arthroscopy and open surgery, and identify the body's pain threshold.
More than 176 million patient records, including medical information, credit card information, and bank information, were compromised between 2009 and 2017. Security is becoming the most susceptible area of healthcare digitization because of these depressing facts. By securely encrypting and sending patient data, controlling medicine supply chains, and even preventing the spread of dangerous diseases, the adoption of blockchain technology helps reduce these risks. Estonia is one of the nations with the most blockchain potential. Since 2012, the nation has used blockchain to protect medical data and carry out transactions. Currently, 99% of Estonia's prescription information and 95% of its health data are digital, and the whole nation's health billing is carried out on a blockchain. Other uses of blockchain in healthcare include:

C. Supply chain transparency

Healthcare providers may create a single system to store and regularly update medical records, ensuring safe and quick retrieval by authorized users, by utilizing blockchain technology. The availability of this integrated system makes it easier to prevent mistakes and misunderstandings, enables quicker, more precise diagnoses, and offers more individualized treatment for each patient.

D. Smart Contracts for Supply Chain and Insurance Settlement

Healthcare providers, insurance companies, pharmaceutical companies, and wholesalers use blockchain-based systems to verify their identity as organizations, track transactions and payments,
and keep an agreement's specifics. Fraud prevention problems for medical pharmaceuticals or other products are being drastically reduced thanks to a totally electronic or controlled system. According to Documented, in response to fluctuations in price arrangements, more than a million chargeback claims are lodged annually amongst parties.

E. Patient-Centric EHR

Per a 2016 Harvard University research, medication administration errors brought on by poor treatment control rank as the third most common cause of death in the US. Patient records disparities are becoming a concern that many countries' healthcare institutions are dealing with. A blockchain-based medical record system linked to conventional Ehr systems might easily fix this problem. Within this is a fantastic company that aids health personnel in using the blockchain Ehr system.

F. Virtual and Augmented Reality

Several medical organizations are able to communicate and reach their patients with remote and individualized care relevant to the outbreak by utilizing Ar technology solutions. The day when these technologies were only employed in the gambling sector is long past. VR and AR will be actively employed for health teaching, rehabilitation programs, article stress disorder rehabilitation, and a variety of other uses in 2021 and well beyond:
medical immersion to meet the demands of various patients

By including patients in clinical tasks, healthcare practitioners are actively utilizing Ar technology technologies to enhance patient experiences. Employing VR applications in aesthetic medicine and orthodontics to schedule appointments and view outcomes is an excellent example. These options can also be utilized to improve the identity
of self-directed care in rural locations where telemedicine is the main form of healthcare. A map that identifies the closest clinic in an unknown region is another application of augmented reality that is particularly helpful in emergency cases [12].

IV. Conclusion

Blockchain can be used with Machine Learning like in the education sector where ML can be used for career guidance while blockchain technology can be used for storing the important documents of the candidates securely. ML can be combined with IoT technologies that typically require higher computational power therefore it is implemented with MEC and secured with blockchain technology.
Blockchain technologies like Biscotti can be used to secure Machine Learning algorithms like the MPML algorithm to protect it from various types of attacks and data leaks. Blockchain can also be used in healthcare applications like sending data to different medical institutions via blockchain and also using it as storage while using ML to detect different kinds of diseases using the data.
Although blockchain is fairly secure because it is immutable and distributed, attacks can happen on the blockchain, to prevent that an ML system can be used to predict attacks using previous attack patterns and build an IDS.
Blockchain can be used for transparency and tracking the data flow in various places like in the healthcare domain for tracking medicines and patient data and so on.
These various use cases of blockchain with ML was studied in detail in the respective paper and we were successfully able to compile the essence of each paper in the literature survey.

References

[1] Biscotti: A Blockchain System for Private and Secure Federated Learning
[2] Machine Learning Adoption in Blockchain-Based Smart Applications
[3] Integrating machine learning and blockchain to develop a system to veto the forgeries and provide efficient results in education sector
[4] Blockchain-Empowered Mobile Edge Intelligence, Machine Learning and Secure Data Sharing
[5] A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism
[6] A Proposed Solution for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment
[7] Smart Care: Integrating Blockchain Technology into the Design of Patient-centered Healthcare Systems
[8] DL Approach for Detecting Security Attacks on Blockchain
[9] Drug Supply Chain Management and Recommendation System for Smart Pharmaceutical Industry, Khizar Abbas , Muhammad Afaq, Talha Ahmed Khan and Wang-Cheol Song.
[10] Smart Manufacturing Real-Time Analysis Based on Blockchain and Machine Learning Approaches, Zeinab Shahbazi and Yung-Cheol Byun
[11] Blockchain and Machine Learning for Fraud Detection A sequestration- Conserving and Adaptive incitement Grounded Approach, Tahmid Hansan Pranto , Kazi Tamzid Akhter MD Hasib , Tahsinur Rahman, Akm Bahalul Haque, A. K. M. Najmal islam , Rashdur M. Rahmen
[12] Machine Learning and Blockchain Techniques Used in Healthcare System ,V. M. Deshmukh ,Nilima V.Pardakhe.