Possibilities at the Intersection of AI and Blockchain Technology

Smriti, Saru Dhir, Madhurima Hooda

Abstract. Artificial intelligence and Blockchain are the most trending technologies these days, where artificial intelligence offers intelligent decision-making capabilities to machines which is similar to human beings and blockchain technology allows a decentralised pathway for encrypted data sharing between ledgers in a secured manner. Integration of both technologies forms a decentralised AI which enables the process of decision-making on digitally encrypted platform for secure data sharing without involvement of any Third Party. This paper gives a detail on the possibilities of intersection of AI and Blockchain. The paper also contains the issues and problems related to the respective integration. An Algorithm is proposed in two parts, based on one of the given issues, which predicts the action plan of AI for destructing malware blocks in blockchain.

Keywords: Artificial Intelligence (AI), Blockchain, Decentralised AI, Technologies.

I. INTRODUCTION

AI and block-chain, the two powerful technologies that are benefiting mankind in numerous ways. So we can imagine their integration revolutionizing our future. AI or artificial intelligence is the cognitive functioning of machines which allows them to adapt according to the data collected or take respective initiation or decisions needed by machines.

Block-chain as we know that is the distribution and decentralized storage of bulky data at various levels without the involvement of intermediates. There are huge possibilities by the convergence of AI and block-chain. In-fact they compliment each other in every possible way. Like AI rely on centralized model of training which makes it prone to data tampering which make authenticity of the source unguaranteed thus integration of AI and block-chain would provide decentralized AI which could enable machine to process and make decisions on trusted, digitally, signed and secured shared data in a decentralized manner without involving intermediates thus we can say that block-chain provide secure data sharing and market-price for AI, explanation to AI and helps in coordinating untrusted devices. Whereas AI provides secure and scalable block-chain, privacy-preservation to block-chain and provides proper governance to its data, so we can infer that block-chain and AI provides more explanation and trustworthy aspects to each other. Convergence of AI and block-chain would help in gaining a lot of progress in healthcare, business develop and research field as well. Decentralised AI is applicable in vehicle routing which helps in traffic control. It not only guarantees in avoiding existing congestion but also prevent it. It is used in biomedical research and healthcare sector to accelerate biomedical analysis, empower patients to control their own data and helps in healthcare assistance by employing robots in elderly care [1]. Chain intel is an open source platform which aim in reinforcing the implementation of AI model to different fragment of networking. Thus helps in tackling the security threats faced by internet. Decentralised AI helps in intelligent precision farming as this technology can implement crop variety selection, irrigation
Possibilities at the Intersection of AI and Blockchain Technology

method, reduce cost thus enhancing profits in agriculture sector. Decentralised AI helps in ocean bed exploration as operations such as disaster relief mission, landmine detection etc are challenging for humans to work. Decentralised AI is used in banking industry in handling fluctuating range and inherent volatility of cryptocurrency. Decentralised AI is used in property management sector to abolish monopolistic power exercised by firms and by comparative market analysis. This technology is adopted by the Singapore government as “SMART NATION” to abolish the superiority of sellers above investors and buyers [2]. Decentralised EHR called MedRec is made to take part in POW. So that miners can extract data for targeted research and for proper medication purpose [3]. Partial homomorphic encryption based on integration of blockchain and AI provides stronger privacy to the applications. Blockchain reduces the expenditure on AI for providing data security by keeping an eye on its every possible steps. AI utilises blockchain for promoting a trustworthy and a secure platform for sharing of decision results as well as knowledge. Blockchain provide trustlessness, privacy and explainability to AI. AI and blockchain helps IOT in agriculture sector by providing AI agents which could increase the agro-supply chain process and to detect weather pattern and blockchain plays its part by decreasing the time consumed on agricultural commodity and food safety accidents. Decentralised AI plays a main role in finding malicious byzantine robots which prevents the possibility of data breach and preserves the authenticity of transactions. In future, Decentralised AI can help in resolving disputes without attending the courtroom procedures with more consistent and justifying data-driven decisions.

II. LITERATURE REVIEW

When blockchain is combined with AI, this integrated structure provide users with innovative data models which is controlled by both AI and blockchain and results in achieving an improved authenticity on data. Chain-intel P2P network [4] are the set of active nodes which works on decentralised AI applications for works such as face, voice, picture recognition, smart homes, smart cities. Ethereum and IPFS handles resource and data repository by giving huge level of confidentiality and safety to records. Therefore, they abolish centralised nature of AI by big companies such as APPLE, GOOGLE, FACEBOOK[5]. Partially homomorphic encryption such as Goldwasser-Micali, Pallier encryption scheme provides protection for safer transaction and protects confidential aspect of trading parties[6]. Mylrea and Gourisetti explored the potential of blockchain in modernizing and automating energy and IOT. They highlighted on AI solutions in energy resource transfer in a decentralised environment by encryption technology [7]. Strobel et al [8] proposed a concept of resolving issues concerned with swarm robotic ecosystem using blockchain. In this, Author used smart contracts as it is decentralised in nature to build a systematized swarm mechanism to eliminate Byzantine members. Ekblaw et. al developed a decentralised EHR MedRec. It encouraged medical associations and EHR stake-holder participate in POW as miners and in return allowed to access the data. This prototype was developed and tested under an association with Harvard Medical school teaching hospital [9]. Dubovitskaya et al advanced a different prototype in distinction to MedRec. It provided a convenient access to the controlled EHR system. Thus it leads to the acceptance of cloud storage and access key transfers for encryption[10]. Peterson et al recommended that by using decentralised AI single diagnostic reports performed on a patient can be obtained [11]. 12th Annual international conference is going to be held in 2019 which would emphasis security, safety and sustainable issues from global perspective. It would provide opportunity for system scientists researchers, operators to update their knowledge and resolve challenges while networking [12]. Dutch land registry departments use decentralised AI technique in real estate industry. It aimed to use AI for predicting the outcome and used blockchain for handling bulky data produced by the department [13]. Satoshi first applied P2P e-cash system which ensures knowledge management and trading decentrally[14]. Woods stressed on the importance of decentralised AI to resolve the threats faced by internet. As in near future bot-bot interaction would increase human-bot interaction. Thus, authentication will be much needed [15]. Decentralised AI uses C4.5 classification method for predicting pollution levels.
which is further used by artificial decision trees named “KEEL” for predicting traffic Jam and pollution level in a city [16]. Osaba et al executed experiments for predicting pollution level in Pisa italy[17]. Nebula Genomics,a start-up cofounder by HARVARD UNIVERSITY’s George church,brought a marketplace that connects people who want their genome sequenced with companies who require this data [18]. Snips AIR to be launched in 2019 is considered as the alternative to Siri to ensure user’s data safety.It ensures that personal data of user to remain within connected home instead of storing in clouds[19]. Yu et al designed an efficient blockchain platform combining smart devices. The platform forms a firm inter-connection between devices through node mechanism using decentralised AI technology [20]. Longenesis provide a platform to allocate and coin data such as health data, Medical records [21]. Common trends in decentralised AI such as Automated Machine learning which is applicable in Big data analytics, Industry 4.0 systems and Massive production of intelligent devices uses blockchain and AI to automate the process of machine learning to reduce manual work and increased efficiency. Digital Twins applicable in Wind Turbines, Aircraft Engines, offshore vessels is one of the trends of decentralised AI these days which works on translating data into applications. Hybrid learning Models is the decentralised AI trend which works on Real time, Data source and decision [22]. GOOGLE DUPLEX, AI’s recent development which could make automatic phone calls, it is an ongoing project whose optimum achievement could be utilised with the future advancement in AI algorithm and blockchain security [23]. Tshilidzi Marwaha and Bo Xing concludeD about decentralised AI and reflect issues about smart-contract. The author emphasised that AI is the core of Industrial revolution and blockchain is the tool to make it more powerful [24].

### III. TECHNOLOGIES BASED ON DECENTRALISED AI

The combination of AI and Blockchain is called Decentralised AI. Since AI is centralised in nature, it has the possibility of data tampering which un-guarantees the authenticity of data from the source. On the other hand, Blockchain being decentralised in nature provides immutable, trust-worthy characteristic to AI when integrated with blockchain. Hence, this powerful combination is providing number of innovations and technologies in various fields.

| TECHNOLOGY | OBJECTIVE | APPLICA TION | METHODOLOGY |
|------------|-----------|--------------|-------------|
| snipAIR    | Protection of personal details of user’s | AMAZON Echo, GOOGLE Home | secure data within the boundary of inter-connected homes rather than storing on clouds |
| Chain intel | Tackling security threats faced by internet | Networking | by executing AI models |
| MedRec     | encourage Medical community to take part in POW as miners and access the data | in Research and Medication field | data extraction by Miners |
| KEEL (decision tree) | to predict traffic congestion and pollution level | to solve traffic congestion problems | C4.5 classification technology |
| Nebula genomics | providing secure platform for sharing and | Marketing | connecting people who want their genome sequence |
Possibilities at the Intersection of AI and Blockchain Technology

| monetize life data | and companies that want the data |
|-------------------|----------------------------------|
| Neuromation       | To allow developers to train NNs |
|                   | Medical detection, industrial robots |
|                   | by training models to empower the distributed computational power and blockchain |

IV. INTERSECTION BETWEEN AI AND BLOCKCHAIN

Intersection between AI and blockchain is of two types, based on how one technology can benefit the other one. Fig. 1 elaborates the benefits of intersection between AI and Blockchain as given below:

- Blockchain for AI
- AI for Blockchain

![Fig1. Benefits of intersection between AI and Blockchain](image)

V. BLOCKCHAIN FOR AI

A. Secured data sharing and Marketplace
The mining nodes hold the replica of entire ledger that contains chained blocks of all transactions and require respective private keys for accessing the data. Thus, it provides a safer place for storing sensitive and personal data in a disk-free area. Since it provides transparency and accountability in data access, it encourages data sharing of various components of AI including data, algorithm and computing power. Thus blockchain can establish decentralised and coordinated platform for Marketplace.

B. Decentralised AI
Multiple agents are involved in taking high level decisions and they have access to common training data in supervised learning program. As for organising the cybersecurity, individual AI agents coordinate together to provide security across network to solve tackle issues.

C. Explanation to AI
Today, AI programs are blackbox system because all the data and programming is hidden from sight. AI is all based on bulky data, algorithms, computing power. So, decision taken by AI is tough to understand. Blockchain can track every step of data processing as well as decision-making chain. So, it could impart more confidence and clarity in decision made by AI.

D. Synergise untrusted devices
Swarm robotics, Internet of Thing, cell phones are considered as untrusted devices. In this scheme, Blockchain can provide a coordinating platform in which compromise can only be done if maximum profit is gained. Application of this plot could provide a range of possibilities from upgrading refrigerator’s software to assembling swarm robotics.

E. Enhancing trust on Bot decision
In recent times, 52% of web traffic is generated by bots which are the product of AI. But half of the bots online are malicious rather than useful. So, for controlling this, a secured and trusted platform is needed which is provided by Blockchain. It would eliminate...
the defective part of these technologies and would increase the transparency. Finally, it would help in gaining public trust in bots’ decisions.

F. Collective decision making
The decentralised decision making results have been applied in many robotic applications without the requirement of a chief authority. In robotic swarm ecosystems, Robots make verdicts by ballot and results are set by majority guidelines. Every robot can drop their vote on transaction form, verification of voting results can be done by all participating robots as blockchain is public for them. This procedure is replicated by all robots until a conclusion is drawn.

G. Increases Efficiency
Involvement of Multiple stakeholders in business sector such as government organisation, business firms are basically feeble due to multipartite authorization of transactions. Decentralised AI technology enables clever decentralized self-governing agents for fast and automatic approval of data for different stakeholders.

VI. AI FOR BLOCKCHAIN

A. Enhance Security
Security in blockchain system cover applications such as smart contract, data encryption mechanism. For application, IDS (intrusion detection system) and IPS (intrusion protection system) are two important elements to monitor threats. For increasing the efficiency of IDS, swarm intelligence approach is applied. AI plays a major role in cryptographic systems, their application ranges from cryptography, cryptanalysis, hash function. AI is involved in improving blockchain system’s resilience by creating more robust ciphers and improves the system attack-defense process.

B. Provide Scalability
Scalability points towards the scale capabilities with the increment in number of users. The efficiency of blockchain system is limited by scalability issues such as response time, initiation time, cost brought forth per confirmed transaction. So, the mining techniques are suffering with these issues. However, AI can figure out scalability from decentralised data sources and provides optimal answers for the blockchain system.

C. Personalized privacy preservation by optimising hash function
With increase in the amount of private data in blockchain system, the data encryption becomes an issue for assuring user’s intimacy. Different AI algorithm can be used for finding the secret keys for tackling this problem. For example, bitcoin blockchain system uses elliptical curves based on generation of private as well as public key.

D. Automatic governance
AI can govern the attacked component from blockchain platform as well as if it found any increase in the transaction number, AI is clever enough for the increment of block creation rate and identify the site of infection and could take effective steps to protect it. Thus it manages and protect blockchain platform.

E. Optimized energy consumption
AI methodologies are applied to enhance mass scale system such as power system planning and operation. Blockchain and micro-economics are similar in nature such as different interconnected subsystems, decentralised computation. The basic tool for analysing microeconomics is intelligent optimization algorithm. Microeconomics is concerned with the allocation of resources among numerous uses with the goal of maximizing user’s utility and producers’ Profit. Thus, AI can provide optimized energy consumption from the large scale complex system perception.

F. Enhance efficiency by predicting the utility of a node for fulfilling mining
In Blockchain, getting the maximized output is not enough for sustaining a desire-able transaction performance. AI can execute fast and active learning so as to speed up resource calculation and enhance overall system performance. Data can be automated fully. AI in this context can provide AI-assisted online learning which would help in training and nurturing needed talent of Blockchain.
VII. ISSUES OR PROBLEMS
INTERCONNECTION OF AI AND BLOCKCHAIN SYSTEM:

AI and Blockchain are one of the innovative technologies that can restructure the world in which we live in. As no technology and their integration is completely free from issues and challenges, decentralised AI is facing the following challenges:

A. Privacy
As Public Blockchain ledger provides secured and authenticated data accessible by all the readers publically. This could be manipulated by hacking invaders. On the other hand, untrusted technologies such as IOT, collects and put the consumer’s sensitive and personal data on open ledgers. This could be a serious threat to the security of data. Private Blockchain ledgers are comparatively safer than public as it ensures the data encryption and supervised access to ledgers. But private platform limits the entry and vulnerability to the hefty quantity of data necessary for AI to process and perform its functions.

B. Side chains and scalability
Scalability is among the major concerns for blockchain platform today. Bitcoin blockchains can perform a fair transaction of 4 in every second whereas Ethereum can perform 12 per second for cryptocurrency platforms Which is highly undesirable with Facebook or big companies as they handle millions of transactions per second including likes, comments, post, Side chains or side channels settle transactions among parties in a quicker way beside the fundamental chain and relocate them on main chain once every day. New and more efficient blockchain platforms such as Algorand and IoTA are emerging for more improved consensus algorithm for mining nodes. However, works are still going on for improving scalability at least being as comparable to Facebook.

C. Blockchain security
Blockchain systems are 51% sensitive to cyber-attack though it provides robust scheme to secure IoT. Thus, we can refer that decentralised power can be converted into centralised when the consensus mechanism depending on hash encryption strength of mining can be compromised by few firms that accord and finalise settlement. The mining nodes surroundings are less protected exclusively in Private Blockchain as they contain few mining nodes whose outcomes can be tampered smoothly. To tackle the issue, freshly arising platforms are well equipped with hardware to be executed in TEEs (Trusted Execution Environments). For example-Intel SGX [25]

D. Trusted oracles
Smart contracts are designed to be pushed data by outside events, it cannot pull the data on its own. To remedy this, the trusted intermediates or third parties or nodes called Trusted Oracles was proposed to push events and data to the smart contracts. Oracle surplus level of insecurity and complexity in managing trust by centralizing system from decentralized system around Oracle group but they must be trusted. Voting is done among trusted Oracle appointed to achieve consensus.

E. Emerging AI-specific consensus protocols
Active protocols consider network and middle layers of blockchain systems by enabling different proof of X protocols. A huge area of research opportunities are present for upcoming researchers to utilise if application level of protocols could be program to recognise testament on the basis of learning model quality, methods for efficient search, quality of data and optimization quality.

F. Fog computing model
Fog computing is an arising computer model that permits localized computing and storing the data source close to IoT devices or where it is generated by customers. Fog nodes builds long delay arise from storage and computing at cloud environment. Fog nodes are basically a local small-scale cloud. In decentralised AI context, upcoming fog nodes are prepared with AI and Machine learning credentials with Blockchain integration to perform management of localised data access and control.
G. Quantum computing
It is predicted that upcoming quantum computing will be capable of breaking encrypted public key and private key can also be resolved. By 2027, experts predict that quantum computing could break the fundamental Blockchain security. So, serious researches are going to formulate quantum-secure and safe Blockchain.

H. Malware files in decentralised Blockchain
Blockchain being decentralised in nature are more reeling to Malware programs. Thus here Decentralised AI comes into rescue. AI detects viral signals sent by the ledger and take suitable decisions by killing the malware blocks instead of killing all the blocks including malware as well as non-malware.

VIII. ALGORITHM AND RESULTS
A. AI decision making on Malware blocks in interconnected blockchain system
Since, blockchain is a decentralised control system, this makes it more prone to malware programs and killing all the blocks one-by-one could be a recovery to this problem. But AI plays an important role here by taking appropriate decisions when it detects any malfunction. Irrespective of killing all, it focuses on malware blocks - detects them and kill them. So, here decentralised system and the stored data is preserved by the application of decentralised AI. An algorithm is proposed in division of two parts-Algorithm-1 and Algorithm-2 on the basis of the ideas of signal sent by the ledger blocks, when malware blocks are aimed to be detected and destroyed by AI. In Algorithm-1, suspected malware blocks are detected by the signals received by AI. In Algorithm-2, it is proposed that the malware block signals are detected and destruction command is given to AI.

Let us assume AI system to be ‘A’, Decentralised blocks as ‘a’ and malware blocks to be ‘m’.
\[ a \subseteq A \]
\[ m \in a \{ m: m \text{ is a block of decentralised blocks } 'a' \} \]

Let us find the possibilities of blocks being malware or containing virus;

\[ p(m/a) = \frac{p(m|a)}{p(a)} \]
where \( p(m/a) \) = possibilities of block being malware

Then, Selecting malware blocks from the possibilities
\[ C_p^{\text{m}} = m! / p(m/a) ! (m-p(m/a)) ! \]
To find the position of suspected malware blocks, we use Heisenberg equation
\[ \Delta X \geq h/\Delta p (4\pi) \]

Now by using FLT(Fuzzy logic theory), we would detect whether the malware block is actually malware or not or over a decentralised network. FLT theory is applicable for block signal to whether the signal is malware or not. Let \( s_a \) and \( s_b \) be the block signals and ID-7 indicates safe signal ID-8 indicates virus affected signals. SSR stands for Primary System Response which is signal produced by blocks and SSR stands for Secondary System Response which is destruction of virus-infected blocks.

\[ S_2 = \{ s_a, s_b, \ldots, s_7 \} \]

B. RULES
RULE 1: IF \((s_a \text{ is safe}) \text{ and } (s_b \text{ is low-danger}), THEN (FLS(S_2)) \text{ is ID-7).} \]
RULE 2: IF \((s_a \text{ is safe}) \text{ and } (s_b \text{ is high-danger}), THEN (FLS(S_2)) \text{ is ID-7).} \]
RULE 3: IF \((s_a \text{ is low-Virus}) \text{ and } (s_b \text{ is low-danger}), THEN (FLS(S_2)) \text{ is ID-7).} \]
RULE 4: IF \((s_a \text{ is low-Virus}) \text{ and } (s_b \text{ is high-danger}), THEN (FLS(S_2)) \text{ is ID-8).} \]
RULE 5: IF \((s_a \text{ is high-Virus}) \text{ and } (s_b \text{ is low}), THEN (FLS(S_2)) \text{ is ID-8).} \]
RULE 6: IF \((s_a \text{ is high-Virus}) \text{ and } (s_b \text{ is high-danger}), THEN (FLS(S_2)) \text{ is ID-8).} \]

Input: Input suspected malware blocks and its signals
Output: detection of virus affected blocks
while {Malware block i= NULL do
extract virus;
if {virus exists in block then
withdraw the stored virus index} ;
verify input virus;
if{ virus is found in suspected blocks & virus presence >= threshold then}
 Nine possibilities at the Intersection of AI and Blockchain Technology

Algorithm 1. Security monitor and SSR Pseudocode

Input: Input virus and its signals
Output: virus context initialize block;
initialize block;
call fuzzy logic system;
if {output > threshold, then
virus context is 1;
else if virus is not found in suspected blocks
add virus to suspected blocks;
create virus counter;
virus counter equal 1;
else
increment virus counter;
} else{
virus context is 0;
if virus is found in suspected blocks
decrement virus counter;
} kill block;
return context to SSR;  // Algorithm 1

Proposed Algorithm 2: PSR pseudocode

Proposed Algorithm 2: PSR pseudocode

X. FUTURE SCOPE

This paper has introduced a self-defensive, efficient and self-organizing intelligent algorithm by using blocks and fuzzy logic theory (FLT) to protect ledger of blockchain from malware attacks by the application of Artificial intelligence. In the near future, AIFA (Artificial Intelligent Fuzzy Logic Algorithm) will be tested and evaluated using more network specified decentralised parameters such as Optimization, Reasoning, Perception, learning etc to make the decentralised network more efficient and error-proof. In addition, more work and research will be designed and done to verify the capabilities of AIFA to resist virus-infected malware blocks with different attacker radio range. The integration of both the technologies may provide a better secured and malware free network in future. There are huge possibilities in the area of intersection of AI and blockchain which would be exercised and discovered in the future.

XI. CONCLUSION

In this paper, the possibilities and current technologies of the intersection of AI and Blockchain are discussed, how these technologies complement and strengthen each other’s weaknesses are discussed. Issues and problems in decentralized AI are discussed and based on these issues’ algorithm is proposed which could help in obtaining a malware-free blockchain network governed by AI technology.

REFERENCES

1. Salah, Khaled, et al, “Blockchain for AI: Review and Open Research Challenges.”, pp. 10127–10149., vol. 7, IEEE, (2019).
2. A. Couse , "How Drones, Data and AI are changing the property sector". [online].Available:http://www.weforum.org/agenda/2018/01/proptech-drones-data-ai-property-sector/2018).
3. Youssef Wehbe, Mohamed AL Zabbi, and Davor Sventinovic, "Blockchain AI framework for Healthcare Records Management: Constrained Goal Model", 26th Telecommunication forum TELFOR 2018, 978-1-5386-
Dr. Madhurima has done her Ph.D in IT, M.Tech in IT and MBA in HRM from University of South Wales, United Kingdom and B.E (Information Technology). She has published many research papers in national and international journals and conferences of repute. She has published a book titled “Computer Networks” with laxmi publications and contributed as an editor in global edition of the book “Absolute

AUTHORS PROFILE

Ms Smriti Jojo is a student of B.Tech in Information Technology, from Amity School of Engineering & Technology, Amity University, Noida, Batch (2018-22). Her area of interests are Machine Learning, Artificial Intelligence, Deep Learning, Blockchain Technology and Data Science. She is an active member of Dean’s Students Welfare Association at Amity University. She has attended various workshops and seminars at national level.

Retrieval Number: AI0301191S19/2019©BEIESP
DOI: 10.35940/ijitee.A1030.1191S19

Published By:
Blue Eyes Intelligence Engineering & Sciences Publication
Java", Pearson Education. Her area of research is video object tracking, software testing, IoT, AJAX Applications and Machine learning. Her M.Tech work has been published as a book titled “Video Object Tracking” by LAP LAMBERT Academic Publishing GmbH & Co. KG, Germany. She has currently three patents and two copyrights on her name.

Dr. Saru Dhir has done her Ph.D in CSE, M.Tech in CS and M.Sc. She has more than 14 years of experience in teaching and research. Her research areas are: Software Engineering, Agile Development, Software Testing, Cyber crime. She has published many research papers in national and international journals and conferences of repute. She has completed Microsoft technology associate certification in DBA, C#, Networking and visual basic.