Trusted AI with Blockchain to Empower Metaverse

Syed Badruddoja, Ram Dantu, Yanyan He, Mark Thompson, Abiola Salau, Kritagya Upadhyay
Dept. of Computer Science & Engineering
University of North Texas
Denton, TX, 76207, USA
E-mail: syedbadruddoja@my.unt.edu, ram.dantu@unt.edu, yanyan.he@unt.edu, mark.thompson2@unt.edu,
abiolasalau@my.unt.edu, kritagyaupadhyay@my.unt.edu

2022 Fourth International Conference on Blockchain Computing and Applications (BCCA) | 978-1-6654-9958-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/BCCA55292.2022.9922027

***Abstract*—The digital experience emerging in the virtual world is a reality with the advent of the metaverse. Augmented reality(AR), virtual reality(VR), extended reality(XR), and artificial intelligence(AI) algorithms would pave the way for an immersive experience for the users in the virtual space. However, the explosion of these technologies broaches new challenges to threaten the success of metaverse due to security risks. The blockchain technology augmented with AI promises to deliver a trusted metaverse for everyone. Nevertheless, smart contracts fail to produce a cognitive prediction, dissuading users from confiding in the metaverse. We arm smart contracts with intelligence to predict using AI algorithms. Moreover, we deploy the smart contracts on the Ethereum blockchain platform and produce a prediction accuracy of 95% compared to Python scikit-learn-based predictions. Our results show that the prediction delay can obstruct the growth of metaverse applications to accept blockchain technologies. Furthermore, the limitation of blockchain technology can make integration unreasonable. Therefore, we discuss possible scalability solutions that can be part of our future work to help more metaverse applications adopt blockchain solutions.**

***Index Terms*—Blockchain, Artificial Intelligence, Metaverse, Digital Twin, Decentralization, Trust, Security, Smart Contracts**

I. Introduction

Trustworthy Metaverse : Metaverse is a virtual world with flawless virtual story experiences, a mirrored world that reflects the physical world, and an augmented reality that provides the seamless experience of logging and augmenting data [1]–[3]. The captivating, hyper-spatio-temporal, and self-evolving virtual shared space amalgamates the virtual world with the real world. Metaverse allows anybody from the real world to conduct businesses, host shows, play games, interact socially, and do many other physical activities virtually with an immersive experience, even if the physical distance makes it impossible. Moreover, artificial intelligence (AI) makes metaverse tangible with augmented reality (AR), virtual reality (VR), extended reality (XR), and AI algorithms. However, the users cannot trust the metaverse unless the information is protected and safe [1]. For instance, misrepresentation of identity, fake information, and wrong prediction create superficial experiences in the virtual world. A trustworthy metaverse is evident to guarantee a trusted immersive experience.

New Economy for Digital Assets: For more than 30 years, digital technology has contributed to social transformation and subsequently uplifted the economy. The transformation has rapidly moved to the digital economy in the last decade. We are experiencing various blockchain applications being created in manufacturing, logistics, finance, automotive, sports, healthcare, and education [4]–[8]. Recently, cryptocurrency has been popular in creating and consuming digital assets. In the real world, an asset has physical matter, weight, and mass and is owned by a human. Whereas digital asset has information represented by bits, which several people can share. The creation and consumption of digital assets that can be traded in the digital economy is a paradigm that traditional economists have not encountered [9], [10]. On the other hand, machine learning algorithms control workers, citizens, workplaces, social behavior, and group behavior and influence the behavior of individuals. We know humans can learn from other humans. Similarly, humans can also learn from machine algorithms (AI agents or artists) and pass the learning to another human. In particular, humans learning from AI agents (e.g., solving some problems) can remove the bias (humans create preferences). Furthermore, learning from AI artists can evolve cultural evolution where human and AI algorithms work together and learn from each other. So, a symbiotic relationship between humans and machines has begun, and artificial intelligence and blockchain technology is accelerating this.

II. Motivation

Blockchain for AI in Metaverse: Artificial intelligence provides cognitive intelligence that requires responsible model development or prediction. For instance, any AI application user using AR, VR, and AI algorithms needs the model to be explainable and the events to be traceable. With explainable and responsible AI, trust in cognition can be assured [11] for metaverse users. However, current AI applications do not provide explainable AI as it is centralized and can be tampered with [12]. A metaverse user is expected to interact virtually with real-world entities to work, play, conduct business, and live day-to-day life. A user may want to see the weather forecast, diagnose health problems, analyze agricultural projections and analyze economic predictions. A flawed weather forecast may be produced with poisoned data. The tampered model may create a bad diagnosis outcome. Agricultural production may provide faulty projections due to erratic predictions. Economic sustainability prediction may get manipulated. Figure 1 explained all of these problems that

metaverse users may encounter, which will dissuade the user from using metaverse overall.

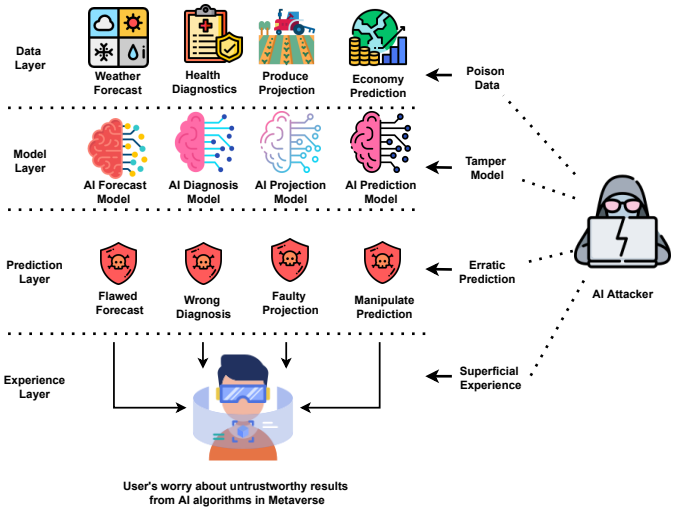

Fig. 1. An attacker can attack the data layer or model layer to manipulate the prediction layer that dissatisfies the users. Consequently, untrustworthy prediction results can dissuade metaverse users dissuade from the very immersive experience due to superficial predictions of AI algorithms

Making Smart contracts Smarter: Blockchain frameworks are known for making immutable, trusted, consensus-based transactions [13] on a distributed ledger consisting of smart contract functions as a set of rules. Smart contracts are computer codes of static rules that reside in blockchain that govern the process of a transaction without performing any intelligent computation. A smart contract does convert the paper contract to a digital one; however, it does not mean that smart contracts are intelligent [14]. The smart contracts are more like a black box or a vending machine set up for rules to be triggered once certain conditions are met. Due to the lack of libraries and development [15] in blockchain smart contracts, it is challenging to apply intelligent applications that require complex mathematical computations. *Most of the supervised machine learning algorithms require floating-point operations for classifying labels.* For example, k-nearest neighbor [16] distance calculation produces square root values, naive Bayes yields probability values [17], and decision-trees [18] use entropy with information gain where decimal numbers are inevitable. *The lack of standardized libraries and the support for a floating-point data type in blockchain smart contracts has made it challenging to develop intelligent applications with such complex computational requirements* [14], [15]. Hence, the decentralized application(DApp) development to learn and predict is limited.

III. Problem Definition

Metaverse is a diversified application with a symbiotic relationship between blockchain and AI, promising a trusted immersive experience for the digital twin. The plausibility of a metaverse to offer such a trusted escapade dwells on the progression of blockchain to provide cognitive services through AI algorithms. However, blockchain smart contracts are traditionally designed to execute simple transactions without learning capabilities. The transactions are verified by consensus nodes which delays transaction output. Due to the multiparty verification process, the transaction would also be expensive. Moreover, The absence of floating point data type makes the cognition incorrect and the prediction unreliable. Therefore, it is apparent that the metaverse immersive experience would have to address trust, reliability, affordability, cost, and delay of AI predictions to provide confident AI services.

IV. Our Contribution

- We have developed smart contracts for naive Bayes, linear regression, and artificial neural networks that can predict in the blockchain platform.
- Our solution offers trustworthy metaverse through immutable and consensus-based predictions.
- The prediction accuracy of smart contracts is 95% compared to Python scikit-learn libraries.
- We discussed challenges faced by the blockchain smart contract to predict using AI algorithm that hinders the progress of the virtual world.
- We discussed blockchain scalability solutions that aid the goal of trustworthy metaverse with faster predictions and cheaper transactions.

V. Literature Review

Trust in Artificial Intelligence: Artificial Intelligence (AI) facilitates intelligent decisions for various applications. AI models are designed with well-known algorithms proven to yield high accuracy with many learning modes. One of the critical problems in recent development involves the trust of the data and model [19], [20], [21]. For example, data poisoning attacks create untrustworthy applications where input data, the machine learning model, and output data can be questioned [21]. If the data and model of the machine learning process are altered, then we can not trust the results. *Similarly, we can not trust classification or prediction if it is not trained with immutable original data and model.* Another perspective of trust is the fairness and explainability of the learning models [22]–[24]. Moreover, the model's training is not auditable, making predictions untraceable. On the contrary, blockchain smart contract provides consensus-based, tamper-proof, auditable, and traceable transactions that can support AI applications to make AI trustworthy [12]. Furthermore, the distributed ledger of blockchain technology can chain the transactions in blocks and make the results immutable. Consequently, metaverse requires the blend of blockchain and AI to build a trustworthy virtual world for a reliable immersive experience [25], [26].

Challenges in Humans Learning from AI Agents: The next evolution can take us to digital asset creation, trading, consumption, and currency powered by AI. When AI agents/artists (models and algorithms) create digital content/objects, they learn about the trends and styles, food, and everyday life, and then AI artists express what they learned

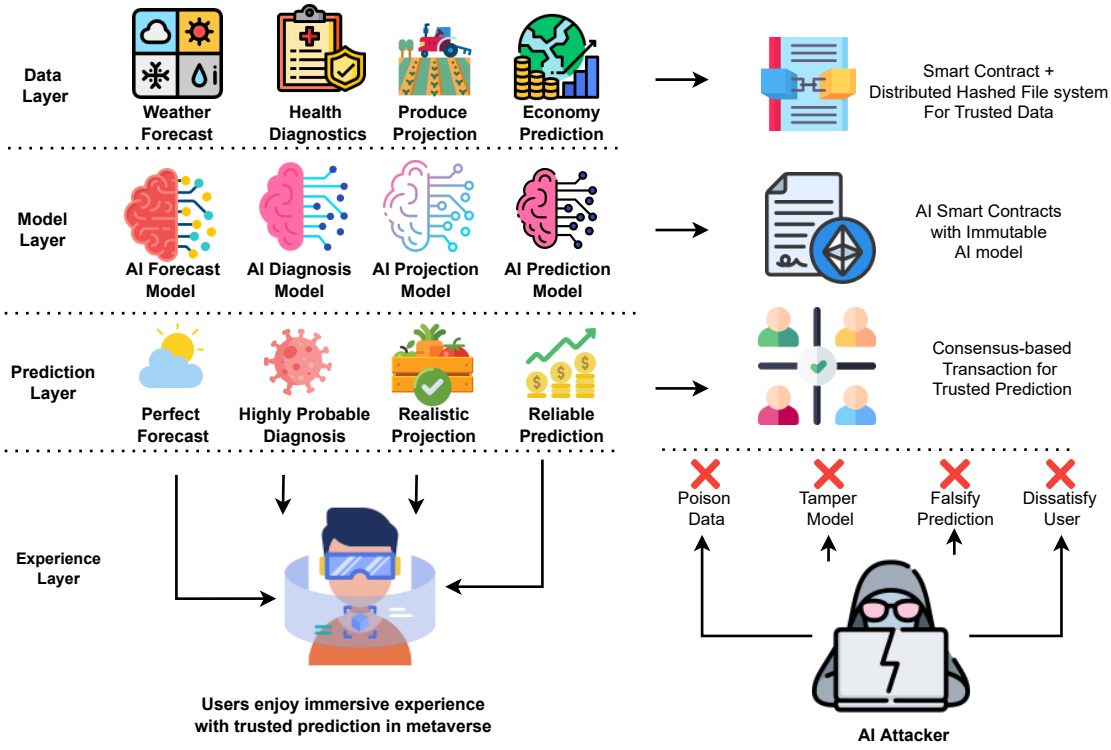

Fig. 2. Blockchain smart contracts to record data for integrity from different sources, train AI algorithms for cognitive intelligence with different models, and produce trusted predictions through consensus-based transactions to protect metaverse.

for creation [27]. Artificial intelligence artists store the data in the distributed ledger so that intelligence can be reused. Also, AI artists can learn how humans create data, consume data, and transact on the blockchain. In parallel, humans can learn how AI artists create digital objects [28]. It is possible and probably scary to think that the human culture would acquire problems and solutions originating from machine learning algorithms in the future. *Here, we have clear challenges about the reliability of data, how to audit if the asset is being represented accurately in the real world, identity/authenticity of management, the trustworthiness of sustainability, tracking the health of the asset and how to include a watchdog to avoid any tampering of the asset.* Additionally, the AI algorithms that rely on these assets should offer trustworthy projections. So, trust in technology is emerging as an important issue. We can think of blockchain as one of these trust technologies.

Recent Applications: Fake identity, fake news, fraudulent transactions, tampering with data, and repudiation are some key security concerns while moving to the metaverse [1], [36]. Salau et al. propose methods to engineer smart contracts for neighborhood watch to alert neighbors with trusted information. [46]–[48]. Upadhyay et al. converts legal contracts to smart contracts for trusted contract execution [42]–[45]. In [41], smart contracts secures IoT devices through threshold-based malfunctions. However, such applications fail to forecast events for neighbors, estimate decisions in legal contracts, and also predict security breaches in IoT sensors.

VI. Methodology

A. Design

AI smart contracts: The trust in metaverse application requires the adaptability of blockchain technology to provide cognitive intelligence with reliable prediction. For this, smart contracts require to predict with high-quality accuracy. AI algorithms should be developed with smart contracts for prediction on the blockchain. We have chosen three AI algorithms to test our hypothesis for securing prediction through blockchain smart contracts. The algorithms are K nearest neighbor, linear regression, naive Bayes, and artificial neural network. Our design can achieve immutable data (subvert data poisoning), a tamper-proof model (deny model tampering), and consensus-based prediction (reject malicious central control) to provide a trusted immersive experience to metaverse users. Figure 2 shows an example of our protection features that can persuade the users towards a trusted metaverse experience. We have derived numerical methods that help smart contracts predict. The derivations require further development and are expected to be published in the future.

Design Properties: We aim to provide provenance of data, the integrity of the model, data, and prediction through our design. The data will be stored in the distributed storage. An interplanetary file system (IPFS) [29] is a distributed file system where data can be stored with a hashed value. Any change to the data will create a change in the hash value, ensuring the integrity of the data. The untampered data

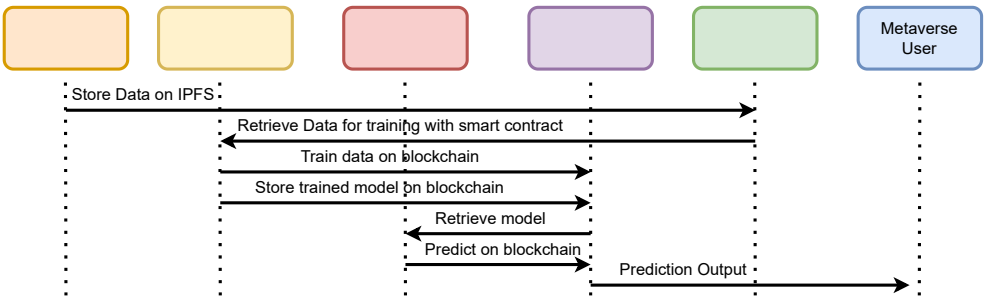

Fig. 3. Event flow for a smart contract to predict with AI algorithms in a blockchain network. Step 1: Data is stored on IPFS storage. Step2: Smart contract retrieves data for training. Step3: Smart contract store model on the blockchain, Step 4 : Smart contract fetches model to predict, Step4: Prediction output is shown to metaverse user

is trained through blockchain smart contracts, and the final model is stored on-chain. The smart contracts developed for predicting on-chain can load the model parameters to predict on-chain, ensuring integrity. The retrieved trained model can predict and provide the output to metaverse users. Figure 3 provides the event flow between the components as described in this section.

B. AI Algorithms

Linear Regression: Multiple linear regression [32] involves learning multiple parameters to form a line of the equation that can best fit a model. Equation 1 shows the prediction formula for linear regression where we have to learn and optimize weights and biases which are $B_1, B_2, ...Bn$ and c. The learning of parameters is performed through the iterative optimization method. The same equation is referred to as $\overline{y}$(referred to as $yhat$) for training purposes. The $\overline{y}$ is computed repeatedly with updated weights and biases.

$$y = B_1x_1 + B_2x_2 + B_3x_3..... + B_nx_n + c \tag{1}$$

We have considered a fraction-based approach for computing equation 1 in our experiment since smart solidity contracts do not support floating-point operations.

Naive Bayes: In supervised machine learning techniques, the Naive Bayes algorithm is one of the least complex algorithms for classification tasks. The training involves computations of means, variance and prior probability concerning each class and prediction involves simple Gaussian probability computations. Moreover, the training time complexity of the Naive Bayes algorithm is *O(n*d)* and prediction complexity is *O(c*d)* where n is the number of samples, d is the number of features, and c is the number of classes [30]. Due to its low complexity, the cost of training and prediction is expected to be low, enabling more applications to use this algorithm with blockchain smart contracts.

$$p(C|x) = \frac{p(x|C)p(C)}{p(x)}. \tag{2}$$

The posterior probability term $p(C|x)$ will be calculated in our case for all the classes to obtain the highest probability for the prediction. The C stands for class and x stands for features in the test dataset. The term $p(C)$ is the probability of class in the training dataset. This term will take the number of the same targets in the training class. Developing smart contracts for the Naive Bayes algorithm is still not plausible due to the absence of floating point operations. We have devised a novel method using Taylor's series expansion to compute the posterior probability of classes for prediction.

Artificial Neural Network An artificial neural network is part of deep learning algorithms that handles a large amount of data for prediction and cognition. The deep learning algorithms of AI possess a complex computational approach for learning information and prediction. The technical operation of a neural network can be found at [31] for better understanding. In our experiment, we have considered a 3-layer neural network with one input layer consisting of inputs, one hidden layer with a sigmoid activation function, and one output layer with a softmax activation function.

$$\sigma(x) = \frac{1}{1 + e^{-x}} \tag{3}$$

$$\text{softmax}(x_i) = \frac{e^{x_i}}{\sum_{j=0}^{k} e^{x_j}} \tag{4}$$

$$L1 = \sigma(W1.X + B1) \tag{5}$$

$$L2 = \text{softmax}(L1.W2 + B2) \tag{6}$$

Equation 3,4 represent the sigmoid and softmax activation function. Equation 5,6 are the computations of hidden layer neurons along with the activation function. To predict a given unknown sample, we first multiply the weights at layer 1 (*W1*) with input features (*X*) and add it to bias (*B1*). The sigmoid ($\sigma(x)$) activation function computes the output at layer 1 with equation 3. In the next step we take the output from layer 1 (*L1*) and multiply with layer 2 weights(*W2*) and add bias(*B2*). This output is normalized through $softmax$ activation for prediction.

C. Expected Result

Intelligent smart contract-based prediction reliability mandates a sound prediction capability that requires high prediction accuracy. The positive results will shift the AI application to adopt smart-contract-based prediction for their applications. We plan to record the prediction accuracy of individual AI algorithms and compare them with built-in scikit-learn-based predictions. Moreover, the blockchain network transactions incur a cost for smart contract functions, which can provide the cost of prediction. Furthermore, we plan to record the prediction delay that can help propose suitable applications for the AI smart contracts.

VII. Performance Evaluation

Dataset: To prove our hypothesis, we have considered three datasets which are banknote authentication, diabetes progression, and digit recognition. The banknote dataset is used for naive Bayes classification, diabetes progression for linear regression, and digit recognition for the artificial neural network.

Scikit-learn Benchmark Performance: Scikit-learn [33] is a python package with tools for AI algorithms with simplified library functions. We have implemented the scikit-learn-based AI algorithms for naive Bayes, linear regression, and artificial neural networks to record a baseline performance accuracy to compare with the smart-contract-based prediction.

Accuracy of Prediction We have previously implemented a naive Bayes algorithm in smart contract [42] and published preliminary results. Figure 4 shows the prediction accuracy of the different AI algorithms with improved algorithms. The new, improved naive Bayes algorithm predicts with an accuracy of 75% with smart contract function compared to Python scikit-learn library which predicts with 78%. Moreover, linear regression has a prediction accuracy of 85% compared to 93% of non-smart contract implementation. Furthermore, Artificial neural network smart contracts predict with 80% accuracy, similar to Python sickit-learn library-based prediction.

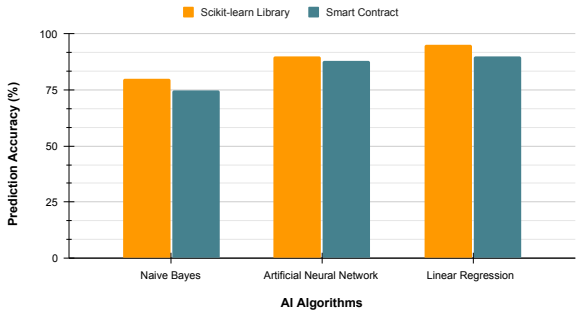

Fig. 4. Prediction accuracy of AI algorithms with smart contracts on Ethereum Blockchain. Smart contracts produce more than 75% of prediction accuracy for Naive Bayes, linear regression, and artificial neural network algorithms

Transaction Delay The prediction delay for each of these algorithms depends on the number of functions and the delay in the Ethereum network to process transactions and create a block. Figure 5 shows a line plot of the prediction time required in the Ethereum network. Out of all the AI algorithms, linear regression has the least delay, with an average prediction time of 15-20 seconds. Conversely, an artificial neural network requires a high amount of time for prediction, with an average between 65-75 seconds. The higher delay is due to more computational operations needed for the artificial neural networks to process a prediction. However, naive Bayes has a lower prediction time than an artificial neural network, with an average value of 30-45 seconds.

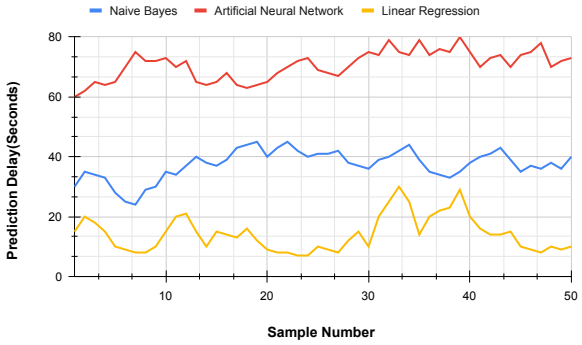

Fig. 5. Prediction delay of AI algorithms with smart contracts on Ethereum Blockchain. The higher delay reveals more computational operations that are executed through the blockchain network for prediction

Cost of Prediction Table I provides a preliminary result of the cost of prediction for each of the algorithms with Ethereum smart contracts. For example, the naive Bayes algorithm charges 8.211$ for each prediction count. Whereas linear regression charges an additional 2$ making a total of approximately 10 & for prediction counts. On the other hand, an artificial neural network charges 16.54$, which is more than twice the cost of a Naive Bayes algorithm.

Prediction Cost	Naive Bayes	Linear Regression	Artificial Neural Network
Ethers	0.00524	0.0006469	0.010687
Dollars	8.211	10.13	16.54

TABLE I
COST OF ETHEREUM SMART CONTRACT FUNCTION TO COMPUTE PREDICTED CLASS FOR DIFFERENT AI ALGORITHMS

VIII. Limitations

One of the significant barriers to integrating with blockchain and AI for metaverse is the immense amount of data processing requirements. AI algorithms demand a lot of data for training purposes, especially deep learning algorithms, to produce highly accurate predictions. Moreover, the complexity of deep learning algorithms requires high computational resources resulting in expensive AI applications. While blockchain can help in some aspects of AI problems, they do not handle ample data storage and high complexity very well. When considering the Ethereum blockchain platform for

AI, the network has limitations on block gas limit, floating-point computations, and delay of transactions that obstructs the development of metaverse for trusted AI applications. Figure 6 shows some of the limitations of the Ethereum blockchain network that restricts the smart contracts from possessing cognitive intelligence.

Programming Limitation: One of the significant limitations of Solidity-based smart contracts is the unavailability of floating-point computations support. As of the current release of the Solidity version 0.8.14 [31] , the Solidity still did not add support for fixed-point number computations. Due to this reason, the application that requires probabilistic outcomes involving floating points stays away from Ethereum blockchain applications [34]. Unlike the standard programming language assignments, the empty dynamic arrays in Solidity programming language require push and pop of elements. Due to this, the reuse of the array requires the deletion of the array, raising the cost of applications.

Block Gas Limit: Ethereum blockchain has a public test network and the main network to deploy smart contracts for decentralized applications. These networks are responsible for creating blocks for transactions that are being executed by the smart contract functions. However, there is a limit to the block gas usage, and it depends on the weight of the smart contract function. Furthermore, the gas consumption in a smart contract function can rise for operations that require loops, an excessive amount of data input, and a high number of instructions in the Solidity smart contracts. Currently, the ropsten test network caps the gas limit at $30,000,000 Gwei$, restricting the number of loop execution and the number of inputs the smart contracts can take. Moreover, the Ethereum main network gas limit range between 15 million to 30 million t [35], blocking the amount of instruction that can be executed by the smart contract [35]. The cap on block gas limit affects the scalability of trusted metaverse applications and hampers the user's overall experience.

Cost of Computation: The transaction fee of every function execution in a smart contract is measured by a formula of $transaction\_fee = gas\_used * gas\_price$, where gas_used is the measure of fuel required to execute a function and gas price is the price of the fuel [35]. After the London upgrade, the transaction fee has an additional cost that involves a base fee. The new formula for the transaction fee is given by $transaction\_fee = gas\_used * (base\_fee + gas\_price)$. Currently $1 Ether = 10^9 Gwei = \$1761$. The Ethereum gas price is variable and is set by the supply and demand of the miners in the Ethereum network. If the gas price of the Ethereum gas rises, the cost of computation will rise too.

Time Complexity: The average block creation time of the Ethereum network is 12-14 seconds. Moreover, Ethereum supports 14-16 transactions per second, which is very low compared to the Visa network, which has 1700 transactions per second. On the contrary, the AI algorithms require a training algorithm with several functions with iterative optimization to optimize weights and biases with high transactions per second requirement. For instance, multiple linear regression and neural network training require iterative optimization to optimize weights with 1000 to 10000 iterations. These iterations involve various functions to update parameters concerning the error of learning. Given the network delay and transaction throughput of the Ethereum network, the training of such algorithms will take days or months [35].

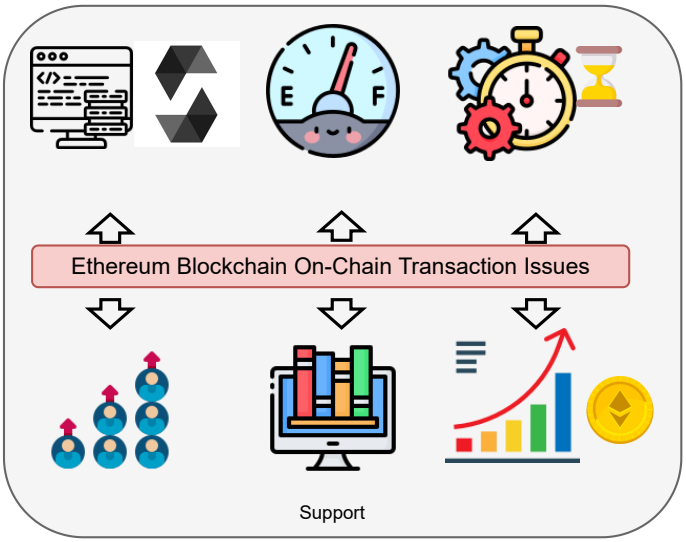

Fig. 6. Challenges of Ethereum blockchain network that hinders the development of AI algorithm with smart contracts. Metaverse cannot provide a seamless, immersive experience with the current performance metrics of the Ethereum blockchain network

IX. Future Work

Scalability Solutions Due to a high requirement of computations and scalability issues, the Ethereum blockchain introduced off-chain computation that can solve many problems mentioned earlier. As per literature, these solutions are termed layer two blockchains, whereas on-chain computation is referred to as layer one blockchain. Therefore, metaverse applications can adopt these solutions for faster prediction and cheaper solutions. Table II shows some of the scalability solutions and their performance metrics that can help metaverse to offer faster blockchain transactions for AI algorithms.

Rollups: Roll-ups are one of the layer two solutions of the Ethereum blockchain that executes transactions out of the chain but appends the final transaction on the main chain. These roll-ups still follow Ethereum security specifications and are considered to be secure. Furthermore, the roll-ups as a part of layer two solutions provide faster transaction time, 100x lower cost of transactions, and support extensive data input. There are mainly two kinds of roll-ups currently available: optimistic roll-up and zero-knowledge rollup [35].

Optimistic Roll-ups And Fraud Proof: Optimistic roll-ups [37] execute transactions parallel to Ethereum main chain. After all the transactions are complete, the last state change is stored on the main chain. The scalability is increased from 10 -100x by adding this solution to the Ethereum main chain. "Optimistic" refers to the aggregate of bare minimum

Scalability parameters	Optimistic Roll-up [37]	Zero-Knowledge Roll-up [37]	Sharding [39]	Sidechain [38]
Method	Off-chain	Off-chain	On-chain	On-chain
Consensus protocol	Fraud proof	Validity Proof	PoS	PoA, DPoS, BFT
Cost saving	100x	Yes	No	Limited
TPS	500	2140	10000	20000
Complexity	Low	High	High	High

TABLE II
THE TABLE SHOWS THE COMPARISON OF SCALABILITY SOLUTIONS FOR THE ETHEREUM BLOCKCHAIN NETWORK THAT CAN ENHANCE THE IMMERSIVE EXPERIENCE OF METAVERSE WITH FASTER PREDICTIONS AND CHEAPER TRANSACTIONS [35]

information required to be stored without proof, assuming no fraud is committed. Optimism and Arbitrum are two of the platform that implements optimistic roll-ups with layer two blockchain solutions. The proof is provided only when fraud is committed [35].

Zero Knowledge Roll-ups & Validity Proof: Zero-knowledge roll-ups or ZK roll-ups [37] work based on validity proof or zero-knowledge proof. A cryptographic proof is provided for hundreds of transfers off-chain. By definition, zero-knowledge refers to the establishment of cryptographic proof between two parties where each party tries to prove to the other the knowledge of something without revealing it. For example, the prover usually proves to a verifier that the prover knows the information and does not reveal it [35]. Moreover, these proofs are made in the form of succinct non-interactive arguments of knowledge (SNARKs) or scalable transparent arguments of knowledge (STARK). Consequently, the ZK roll-ups maintain the state of all the transactions on layer two, and validity proofs can only update the states. Furthermore, ZK roll-up provides a faster and cheaper way of validating a block. For instance, the ZK roll-up account is represented by an index rather than an address that reduces a transaction size from 32 to 4 bytes.

Sidechains: A sidechain [38] is a separate blockchain that runs parallel to the Ethereum main chain and executes independently. Sidechains have consensus algorithms: proof of authority, delegated proof of stake, and byzantine fault tolerance. Sidechains are supported on the Ethereum network as their operations run on Ethereum virtual machines. Some sidechains implementations that can be used to scale the Ethereum blockchain are Polygon PoS(Proof of Stake), Skale, and Gnosis Chain [35]. Side chains also support Proof of Authority(PoA), Delegated PoS and Byzantine fault tolerant(BFT) consensus protocols.

Sharding: Sharding [39] is the concept of splitting a database horizontally to spread the load of the database. In Ethereum, sharding will reduce network congestion and increase transactions per second by creating new chains. Moreover, with the proof of stake consensus protocol released by 2023, sharding will improve the network performance to accommodate faster transaction requirements. Currently, shard chains are available in two versions: data availability and code execution. Data availability will not handle any transactions but will still offer incredible improvements to transactions per second. The code execution version will consist of smart contracts where each of the shards will consist of its chain and accounts with balances [35].

Future Design strategy: The AI algorithms in metaverse can rely on off-chain training options for training purposes, making the training 100 times faster and cheaper as per the layer two solutions discussed earlier. Optimistic roll-ups such as Arbitrum can handle such off-chain training with Ethereum smart contract to produce training parameters with faster training time. After a model is trained on-chain, there will not be many iterations or functions to be executed for prediction purposes. Instead, it will be an iteration for the prediction function to classify or predict values. We propose the prediction performed on-chain to maintain a higher level of integrity.

X. CONCLUSION

Metaverse promises to deliver an immersive experience with AR, VR, XR, and other AI technologies that provides an authentic, real-world experience with virtual life. The virtual world brings many more new vulnerabilities than the existing ones since every transaction will be through a digital experience. Hence, metaverse adopts blockchain technology to protect data and information in the virtual world. However, securing AI components has not been scientifically studied or implemented. In our work, we devised a novel architecture to integrate AI with blockchain that can aid metaverse to proliferate. We proposed smart contracts that can predict or classify based on AI algorithms making the smart contracts intelligent and prepared for the metaverse. We developed smart contracts for AI algorithms and deployed them in Ethereum smart contracts for prediction. Our smart contracts produced a good 95% accuracy for prediction compared to python scikit-learn library-based functions. Though the blockchain smart contracts can predict, many limitations need special attention before metaverse can integrate blockchain. We discussed the challenges and scalability solutions of blockchain technology that can soar the success of the metaverse system with the immersive virtual world.

XI. ACKNOWLEDGEMENT

We thank National Security Agency for partially supporting our research work through grants H98230-20-1-0329, H98230-20-1-0403, H98230-20-1-0414, and H98230-21-1-0262.

REFERENCES

[1] Wang, Y., Su, Z., Zhang, N., Liu, D., Xing, R., Luan, T. H., Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. arXiv preprint arXiv:2203.02662.

[2] Gadekallu, T. R., Huynh-The, T., Wang, W., Yenduri, G., Ranaweera, P., Pham, Q. V., ... Liyanage, M. (2022). Blockchain for the Metaverse: A Review. arXiv preprint arXiv:2203.09738.

[3] Pham, Q. V., Pham, X. Q., Nguyen, T. T., Han, Z., Kim, D. S. (2022). Artificial Intelligence for the Metaverse: A Survey. arXiv e-prints, arXiv-2202.

[4] Abou Jaoude, J., & Saade, R. G. (2019). Blockchain applications–usage in different domains. IEEE Access, 7, 45360-45381.

[5] Tasatanattakool, P., Techapanupreeda, C. (2018, January). Blockchain: Challenges and applications. In 2018 International Conference on Information Networking (ICOIN) (pp. 473-475). IEEE.

[6] Antonucci, F., Figorilli, S., Costa, C., Pallottino, F., Raso, L., & Menesatti, P. (2019). A Review on blockchain applications in the agri-food sector. Journal of the Science of Food and Agriculture, 99(14), 6129-6138.

[7] Dujak, D., & Sajter, D. (2019). Blockchain applications in supply chain. In SMART supply network (pp. 21-46). Springer, Cham.

[8] Mackey, T. K., Kuo, T. T., Gummadi, B., Clauson, K. A., Church, G., Grishin, D., ... Palombini, M. (2019). 'Fit-for-purpose?'–challenges and opportunities for applications of blockchain technology in the future of healthcare. BMC medicine, 17(1), 1-17.

[9] Brynjolfsson, E., Kahin, B. (Eds.). (2002). Understanding the digital economy: data, tools, and research. MIT press.

[10] Carlsson, B. (2004). The Digital Economy: what is new and what is not?. Structural change and economic dynamics, 15(3), 245-264.

[11] Salah, K., Rehman, M. H. U., Nizamuddin, N., Al-Fuqaha, A. (2019). Blockchain for AI: Review and open research challenges. IEEE Access, 7, 10127-10149.

[12] Dinh, T. N., Thai, M. T. (2018). AI and blockchain: A disruptive integration. Computer, 51(9), 48-53.

[13] R. Stephen, A. Alexa "Review on Blockchain Security",2018 IOP Conf. Ser.: Mater. Sci. Eng. 396 012030

[14] Stuart D. Levi and Alex B. Lipton, Skadden, Arps, Slate, Meagher Flom LLP,"An introduction to Smart Contracts and their Potential and Inherent Limitations" https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/, Accessed September 2021

[15] "Solidity Programming guide, https://docs.soliditylang.org/en/v0.8.9/, Accessed September 2021

[16] Peterson, L. E. (2009). K-nearest neighbor. Scholarpedia, 4(2), 1883.

[17] Rish, I. (2001, August). An empirical study of the naive Bayes classifier. In IJCAI 2001 workshop on empirical methods in artificial intelligence (Vol. 3, No. 22, pp. 41-46).

[18] Safavian, S. R., Landgrebe, D. (1991). A survey of decision tree classifier methodology. IEEE transactions on systems, man, and cybernetics, 21(3), 660-674.

[19] A.C. Bantis , "Is your ML model Secure", https://medium.com/slalom-technology/is-your-ml-model-secure-fe10b8589b71,Accessed September 2021.

[20] M. Brundage et al., "Towards Trustworthy Ai development" mechanisms for supporting verifiable claims" year=2020,eprint=2004.07213,archivePrefix=arXiv, primaryClass=cs.CY,https://arxiv.org/abs/2004.07213

[21] N. Pitropakis, E. Panaousis, T. Giannetsos, E. Anastasiadis, G. Loukas,"A Taxonomy and Survey of attacks against machine learning",Volume 34,2019,100199,ISSN 1574-0137, https://doi.org/10.1016/j.cosrev.2019.100199.

[22] Liao, Q. V., Singh, M., Zhang, Y., Bellamy, R. (2021, May). Introduction to explainable AI. In Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems (pp. 1-3).

[23] Gade, K., Geyik, S. C., Kenthapadi, K., Mithal, V., Taly, A. (2019, July). Explainable AI in industry. In Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery data mining (pp. 3203-3204).

[24] IBM Article, "Explainable AI", https://www.ibm.com/watson/explainable-ai, Rai, A. (2020). Explainable AI: From black box to glass box. Journal of the Academy of Marketing Science, 48(1), 137-141.

[25] Yang, Q., Zhao, Y., Huang, H., Xiong, Z., Kang, J., Zheng, Z. (2022). Fusing blockchain and AI with metaverse: A survey. IEEE Open Journal of the Computer Society.

[26] Jeon, H. J., Youn, H. C., Ko, S. M., Kim, T. H. (2022). Blockchain and AI Meet in the Metaverse. Advances in the Convergence of Blockchain and Artificial Intelligence, 73.

[27] Dellermann, D., Calma, A., Lipusch, N., Weber, T., Weigel, S., Ebel, P. (2021). The future of human-AI collaboration: a taxonomy of design knowledge for hybrid intelligence systems. arXiv preprint arXiv:2105.03354.

[28] Kohda, Y. (2020, July). Can humans learn from AI? A fundamental question in knowledge science in the AI era. In International Conference on Applied Human Factors and Ergonomics (pp. 244-250). Springer, Cham.

[29] Benet, J. (2014). Ipfs-content addressed, versioned, p2p file system. arXiv preprint arXiv:1407.3561.

[30] Danny Varghese, "Comparative Study on Classic Machine Learning Algorithms", https://towardsdatascience.com/comparative-study-on-classic-machine-learning-algorithms-24f9ff6ab222, Retrieved March 2022.

[31] M.Ardi, Simple Neural Network on MNIST Handwritten Digit Dataset", https://becominghuman.ai/simple-neural-network-on-mnist-handwritten-digit-dataset-61e47702ed25, Retrieved March 2022

[32] J. Neto, "Multiple Linear Regression from Scratch using Python", https://medium.com/analytics-vidhya/multiple-linear-regression-from-scratch-using-python-db9368859f, August 2021.

[33] Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., ... Duchesnay, E. (2011). Scikit-learn: Machine learning in Python. the Journal of machine Learning research, 12, 2825-2830.

[34] Buterin, V. (2013). Ethereum white paper. GitHub repository, 1, 22-23.

[35] "Ethereum whitepaper",https://ethereum.org/en/developers/docs/gas/, Accessed July 2022

[36] Di Pietro, R., Cresci, S. (2021, December). Metaverse: Security and Privacy Issues. In 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA) (pp. 281-288). IEEE.

[37] Schaffner, T. (2021). Scaling Public Blockchains. A comprehensive analysis of optimistic and zero-knowledge roll-ups. University of Basel.

[38] Singh, A., Click, K., Parizi, R. M., Zhang, Q., Dehghantanha, A., Choo, K. K. R. (2020). Sidechain technologies in blockchain networks: An examination and state-of-the-art review. Journal of Network and Computer Applications, 149, 102471.

[39] Wang, G., Shi, Z. J., Nixon, M., Han, S. (2019, October). Sok: Sharding on blockchain. In Proceedings of the 1st ACM Conference on Advances in Financial Technologies (pp. 41-61).

[40] S. Badruddoja , R. Dantu, Y. He, K. Upadhayay, M. Thompson (2021, May). Making smart contracts smarter. In 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 1-3). IEEE.

[41] S. Badruddoja, R. Dantu, L. Widick, Z. Zaccagni, K. Upadhyay, (2020, May). Integrating DOTS With Blockchain Can Secure Massive IoT Sensors. In 2020 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW) (pp. 937-946). IEEE.

[42] K. Upadhyay, R. Dantu, Z. Zaccagni, S. Badruddoja, (2020, November). Is your legal contract ambiguous? Convert to a smart legal contract. In 2020 IEEE International Conference on Blockchain (Blockchain) (pp. 273-280). IEEE.

[43] K. Upadhyay, R. Dantu, Y. He, A. Salau, S. Badruddoja. (2021, December). Make Consumers Happy by Defuzzifying the Service Level Agreements. In 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA) (pp. 98-105). IEEE.

[44] K. Upadhyay, R. Dantu, Y. He, A. Salau and S. Badruddoja, "Paradigm Shift from Paper Contracts to Smart Contracts," 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), 2021, pp. 261-268, doi: 10.1109/TPSISA52974.2021.00029.

[45] K. Upadhyay, R. Dantu, Y. He, S. Badruddoja and A. Salau, "Can't Understand SLAs? Use the Smart Contract," 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), 2021, pp. 129-136, doi: 10.1109/TPSISA52974.2021.00015.

[46] A. Salau, R. Dantu, K. Morozov, K. Upadhyay, S. Badruddoja, "Multi-Tier Reputation for Data Cooperatives", The 3rd International Conference on Mathematical Research for Blockchain Economy, 2022

[47] A. Salau, R. Dantu, K. Morozov, K. Upadhyay, and S. Badruddoja (2022). Towards a Threat Model and Security Analysis for Data Cooperatives. In Proceedings of the 19th International Conference on Security and Cryptography - SECRYPT, ISBN 978-989-758-590-6; ISSN 2184-7711, pages 707-713. DOI: 10.5220/0011328700003283

[48] A. Salau, R. Dantu and K. Upadhyay, "Data Cooperatives for Neighborhood Watch," 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2021, pp. 1-9, doi: 10.1109/ICBC51069.2021.9461056.