The Journal of Supercomputing
https://doi.org/10.1007/s11227-020-03251-9

Secure decentralized peer-to-peer training of deep neural networks based on distributed ledger technology

Amin Fadaeddini[1] · Babak Majidi[1] · Mohammad Eshghi[2]

Abstract

The accuracy and performance of deep neural network models become important issues as the applications of deep learning increase. For example, the navigation system of autonomous self-driving vehicles requires very accurate deep learning models. If a self-driving car fails to detect a pedestrian in bad weather, the result can be devastating. If we can increase the model accuracy by increasing the training data, the probability of avoiding such scenarios increases significantly. However, the problem of privacy for consumers and lack of enthusiasm for sharing their personal data, e.g., the recordings of their self-driving car, is an obstacle for using this valuable data. In Blockchain technology, many entities which cannot trust each other in normal conditions can join together to achieve a mutual goal. In this paper, a secure decentralized peer-to-peer framework for training the deep neural network models based on the distributed ledger technology in Blockchain ecosystem is proposed. The proposed framework anonymizes the identity of data providers and therefore can be used as an incentive for consumers to share their private data for training deep learning models. The proposed framework uses the Stellar Blockchain infrastructure for secure decentralized training of the deep models. A deep learning coin is proposed for Blockchain compensation.

Keywords Deep learning · Privacy-preserving · Blockchain · Autonomous self-driving car

✉ Babak Majidi
b.majidi@khatam.ac.ir

[1] Department of Computer Engineering, Khatam University, North Shiraz Street, Tehran, Iran

[2] Department of Computer Engineering, Shahid Beheshti University, Tehran, Iran

Published online: 19 March 2020

1 Introduction

The promise of deep learning models is to find the complex and nonlinear patterns in the datasets. This promise has been proven by acceptable results in domains like object recognition, synthesizing samples, image retrieval and many other applications [1–6]. However, in many of these applications, security and privacy of the training data for deep models are the vital issue. These aforementioned advances in deep learning are strongly dependent on the presence of big datasets. Without this large datasets, trained deep models will fail to achieve acceptable accuracy. Unfortunately, this valuable information cannot be accessed without considerable cost and effort. A large percentage of datasets are in possession of larger companies and are only available at a high cost. This cost makes it almost impossible for startups and researchers to train high accuracy deep models. Along with strict legal regulations which will restrict sharing of end user's data, there are also privacy concerns for ordinary individuals to share their personal data due to possibility of these private data to become available to the public. Using Blockchain technology, many of these problems can be solved. In this new decentralized ecosystem, everyone can process the data locally and only share the learned parameters of the deep models.

Beside its application for production of the cryptocurrencies, Blockchain has the ability to tokenize various assets. In this paper, a framework based on Blockchain for sharing deep neural network models between multiple entities is proposed. In the proposed framework, the data owners do not require to share their private data with the public. Instead, they train the shared model on their data locally and at the end of the training, they only share the learned parameters of the model. The first contribution of the paper is a novel framework for shared training of deep neural networks which has the following characteristics:

1. Every computing partner can leave the network at any stage of training while taking the proportionate rewards;
2. The malicious partner will be punished by paying more deep learning coin (DLC) (main currency of the proposed model) in order to cooperate in future training;
3. Deterring the malicious activities by the implementation of Know Your Customer (KYC);
4. Using the Stellar native assets to incentivizing the computing partners.

Incentivizing parties in cooperative learning also discussed in other recent works, e.g., [7]. The second contribution of this paper is that in contrast to the previous works, we designed a model in which parties can convert their incentivization directly to Fiat currencies using the exchange system embedded in the stellar framework. The third contribution of the paper is that by incorporating IPFS in our architecture, we can record any additional data of all the parties based on KYC, while by encrypting the data ensuring them of any abuse of data. As the final contribution of the paper, the proposed framework is implemented for the case study of training the deep neural model in a fleet of driverless cars.

The rest of the paper is organized as follows: In Sect. 2, related works are discussed. In Sect. 3, background analysis of some Blockchain concepts is provided. In Sect. 4, the proposed framework is described. In Sect. 5, the proposed model is used to implement a decentralized peer-to-peer training for autonomous self-driving car fleet. In Sect. 6, we discuss the deployment of the proposed framework on Stellar Blockchain ecosystem, and finally, we concluded the paper in Sect. 7.

2 Related works

Combining the Blockchain and artificial intelligence has gained the attention of many researchers in recent years. Almost all of these researchers are focused on the transparency and security that the Blockchain brings to artificial intelligence and in particular deep learning models. Before the Blockchain, there was a mistrust between the entities who own the data and the ones which process the data. It was Blockchain that gave individuals the guarantee that it is possible to trust a system. In this section, we take a look at some of these researches that incorporate these two technologies and also review recent applications that try to increase the performance of deep models by cooperative learning and sharing the processing power.

A security issue concerning deep learning models is the attack which could happen at any layer of the network during the training. This means that an external entity can manipulate the parameters or even the data in any blocks of a layer to divert the path of training which leads to a wrong decision by the model. In [8], by using the Blockchain technology, an architecture that uses the hash of the current and previous blocks to verify the authenticity of a block's performance is proposed. In [9], authors investigated the ability to deploy distributed training and also lack of transparency, security and privacy in big data infrastructures like cloud computing platforms. They designed a learning model fusion mechanism in a decentralized architecture which uses homomorphic encryption (HE) to ensure privacy-preserving. Salah et al. [10] reviewed the combination of artificial intelligence and Blockchain and discussed some of the emerging Blockchain applications that target artificial intelligence. They show that leveraging Blockchain can help artificial intelligence applications to enhance data security, improve trust on robotic decisions, enable collective decision making, bring high efficiency and the possibility to have a decentralized intelligence which involves multiple smart agents.

Mamoshina et al. [11] show the application and significance of Blockchain in the healthcare industry and the cost of acquisition of data in this context. In their ecosystem, they use an open-source framework called Exonum where patients can share their data, while they can manage the access privileges and receive a token currency as a reward in return for their contribution in sharing the data. With respect to cooperative learning, many research projects like [12–14] tried to create a model in which open-source Blockchain frameworks such as Etherium have been used. In order to update and converge the learned parameters, each of them uses and compares the possibility of a central pool of parameters or a decentralized one. For example in [15], the trade-off between the centralized and decentralized pool of parameters is investigated.

3 Background

3.1 1 Blockchain

Blockchain has been developed to increase the privacy and transparency among anonymous participants. In Blockchain, there is a distributed ledger technology (DLT) that contains the history of transactions and operations. After a set of data transactions added to the ledger, i.e., blocks in the Bitcoin network, they become irreversible, and every participant will be informed about them. Cryptography science plays a pivotal role to achieve anonymity and immutability in Blockchain technology. When a specific quantity of data aggregate to form a block, a hashing function such as SHA-256 is deployed to anonymize the data and to make it impossible to alter. This process is with reference to the previous block and will result in forming a chain of blocks. Because of this chain of blocks, if a malicious party at current ledger of M decides to alter an information in ledger N, it must compute the consensus algorithm from ledger N up to ledger M. This is theoretically impossible because as the chain of blocks are in progress, the hostile node either have to compute an infeasible quantum or have to attain consent of other majority nodes on $M - N$ ledgers [16]. The means that enable parties to update their information about the system and progress the ledger is called consensus. Generally, Blockchain networks are classified based on the algorithm that they use for consensus. Some networks prefer to perform the evaluation based on processing power scale known as proof of work and some of them prefer participant's credit known as proof of stake.

The most important concern about Blockchain is the increasing volume of data. As time passes, the infrastructure to store this big data becomes more important. Until the hostile parties do not hold the majority of the network, we can say that the data are authentic. In settings like a decentralized deep learning model, if one company which have access to great computing resources and owns the majority of the training power, it can break the procedure of training [17].

3.2 Concept of tokenization

The concept of tokenization is mostly dealt with liquidity in economics. Since by tokenizing an illiquid asset, we are promoting the chance of the asset to be traded by fragmenting it to tokens with a lower price [18]. However, the scope of tokenization is not necessarily limited to real-world and physical assets. Also, intangible assets can be represented as a unit of a token. Tokenization has been used to represent many parts of the proposed framework. For instance, as it is shown in Sect. 4, the donor of training data is credited by an abstract token known as (deep learning model) DLM that they can use to exchange with cryptocurrencies and fiat tethers.

3.3 Smart contracts

A smart contract is a form of contract that is written in programming languages which is signed by all parties in the network that are involved [19]. This contract will be triggered in an appropriate situation automatically by itself without the interference of the users. For example, in the scenario of autonomous driving cars, after passing a certain distance, vehicles automatically upload their captured data for training purposes and receive a reward.

3.4 Stellar

Stellar is a permissionless Blockchain ecosystem that allow anyone to join the network. However, since Stellar is an open-source project by Stellar Development Foundation [3], it is also possible for industries to build a completely permissioned Blockchain ecosystem for their specific internal usages. The compelling side of Stellar is the embedded distributed exchange in its ledger. This embedded DEX makes it possible for anyone to not only define new assets but the ability to exchange them. In the proposed model, we use Stellar framework as the infrastructure for our decentralized deep learning.

3.5 Interplanetary file system (IPFS)

Interplanetary file system (IPFS) [20] is a new protocol designed for file sharing in a decentralized manner that does not have the deficiencies of current HTTP client–server architectures. The currently used client–server architecture stores the files in a central server and makes it available for other people in the world to access the files using location-based addressing. In client–server protocols, the stored files can be altered or even removed without the consent of data owners. The IPFS is a decentralized peer-to-peer protocol which will disseminate files between a list of trusted nodes known as bootstrap nodes and make it available to other users by content identifiers (CIs) and content-based addressing. Several advantages come along with this new distributed protocol. For example, denial of service (DDoS) attacks become very hard, since there is not a single centralized server anymore but multiple connected servers that updating the list of files and CIs. Because of the described advantageous of IPFS, in the proposed model, the IPFS is used to store the learned models' checkpoints.

4 Privacy-preserved decentralized deep learning

Privacy-preserving in training deep models is important because individuals and companies, who hold sizeable and useful sources of data, show reluctance to give their private data for research purposes if their privacy is not preserved. In order to solve this problem, the federated learning has been investigated by researchers [12, 13, 21, 22]. The federated learning or collaborative learning is a framework for decentralized computation and sharing of processing power among a group of participants. In federated deep learning, there is a central repository for the model. This model is updated based on the parameters that the participants sent periodically. This works an extended version of our earlier paper, which will focus on the application of the proposed privacy-preserved decentralized deep learning for autonomous driving cars with appropriate modifications regarding this application. In [23], the feasibility of the framework was discussed and demonstrated that it is possible to leverage an open-source Blockchain infrastructure to deploy a privacy-preserved deep learning framework. In this paper, we further discuss the framework by first extending its structure and algorithm and second considering a real-world application scenario that uses this framework to cooperatively train a model between different parties.

Some of the features that make this work distinguishing are (1) preparing a framework that enables the users to have a well-known cryptocurrency as an incentive that is ready to cash, (2) every individual, company or institution can join the program without the necessity of having an expensive infrastructure, (3) based on the capabilities of Stellar and by adding IPFS to our architecture, we made it possible to store any additional data as KYC information.

4.1 Tokens of the proposed framework

In the proposed framework, we define an asset called DLC as the base currency of the model. Beside this asset, all model initiators can issue assets that represent their own training model. Because of the embedded order book in the Stellar framework, known as Stellar Decentralized EXchange (Stellar DEX), it is possible for individuals to make an offer based on their balance of tokens. In the proposed framework, we treat models as a token issued by a model initiator.

As shown in Table 1, the proposed model has four classes of assets:

1. The deep learning model (DLM) that is issued by the model initiator and represents the model in the order book.
2. Verified learned model (VLM) which is also issued by the model initiator and is distributed to the validators that have been designated to validate the authenticity of the trained model.
3. Deep learning coin (DLC) which is the asset that computing partners must pay to cooperate in training procedures. Volunteers can buy this coin for a low price. The primary reason behind using this asset is to compensate the hostile participant to pay more DLC in future cooperation.
4. Stellar native asset (XLM) that is paid to computing participants.

Table 1 List of assets used in the proposed model

Asset code	Issuer
DLM	Model initiator
DLC	Issued by the proposed model
VLM	Model initiator
XLM	Stellar native asset

4.2 Model fusion

The model fusion technique should be used when the training models aggregated to each other. Any cooperative learning architecture whether it is centralized like federated learning or decentralized like the proposed model must have a strategy for parameter aggregation. The two categories of model fusion are early fusion and late fusion. Late fusion works like most of the ensemble learning techniques. They are using average and majority voting between learned models for prediction. In early fusion, we must aggregate learned features to build another model for prediction [24]. In a scenario where the model needs to perform in real time, ensemble learning fails to work. This is due to the fact that the computation time is relatively high, and this is not suitable for real-time applications. In the proposed framework, the early fusion is used to create new models.

4.3 Incentivization versus compensation

A participant who contributes to the training of a model must have reasonable motivation. Therefore, implementation of incentivization is important in distributed deep learning. After the computing partner finished the process of training, the trained model should be approved by the validating nodes. Then a pre-arranged amount of XLM will be credited to partners account. Computing partner hence can use this XLM in online exchange platform to exchange it with others cryptocurrencies like Bitcoin, Ether or even with rest of the tokens already available in the global Stellar network.

Some computing participants can intentionally harm the quality of the model. For example, a computing participant can stop the process of training too early or can train the model on a completely irrelevant data set. In order to deter these malicious activities, the proposed distributed framework must have a plan to prevent these activities. In the proposed framework, we control this by two means. First, we issue an asset called DLC. The primary purpose of this asset is to control the authenticity of the computing partner's model. Any volunteer that wants to be involved in the training of a specific model must pay some DLC from his account. If the number of malicious activities by an account increases, in the future cooperation, it will be forced to pay more DLC. Secondly, we have an implementation of KYC in our framework to further control the authentication. Required information about the computing partners is recorded on-chain.

5 Decentralized training of autonomous driving cars

In this section, we describe the framework in which autonomous self-driving cars can securely share their data for training purposes. As shown in Sect. 3, previous cooperative architectures relied on a central authority. This authority either collects the data from all the parties and then starts the actual training, or lets the parties train the model and then collects the learned parameters in the central repository. Most of the available federated deep learning models have the second approach and act like a black box that stores the model in one central server. Although this is acceptable in many cases that participants want to only help the training by sharing their private data, sometimes this design is not useful for distributed computation when all participants like to have a copy of the model. In Blockchain, it is possible that we train the model in a way that the model is distributed between multiple participants. More importantly, using Blockchain, we can conceal the identity of participants and the model's owner. Figure 1 shows a graphical representation of this concept. Figure 1a shows a centralized approach to train a model where every self-driving car helps a central model by sharing their data in a non-private manner. In contrast, Fig. 1b shows the proposed model, in which every participant (manufacturers, research institutions, a body of governments and smart self-driving cars) joins a Blockchain network to train models in a private manner.

5.1 Scenario

We look at the scenario of the proposed model for three categories of end users:

1. A manufacturer, research institution or a body of government that aims to increase the accuracy of the deep models.
2. The owners of smart self-driving cars that want to share their daily data privately.
3. The validating nodes that appointed to assess the model of computing partners which can be either an institution or a body of government that test the model on their benchmark.

Consider that each vehicle is equipped with at least one recording camera and enough processing power for training the models. The vehicles capture the scenes like the roads, pedestrians, traffic lights, traffic signs, etc. There are three perspectives regarding the proposed framework:

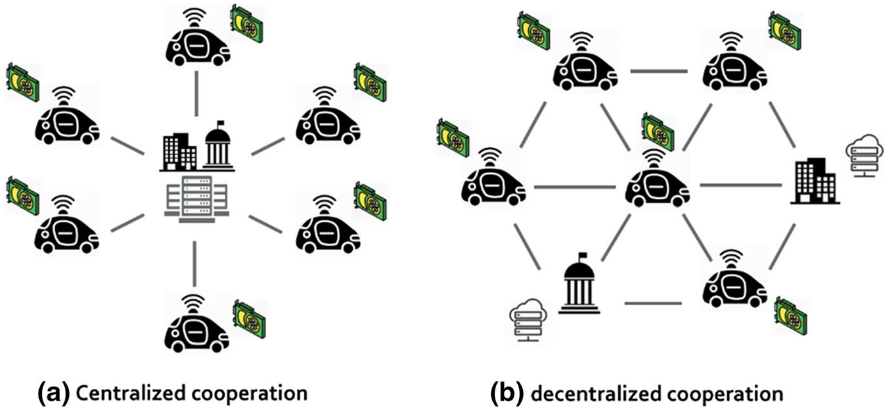


Fig. 1 Comparison between centralized cooperation and decentralized cooperation

1. *The perspective of the Model Owner* the model initiator uploads the predefined model to the IPFS and receives a 32-byte checksum hash. The issuer of the model will first issue the tokens that represent the model identity in the network and distribute it to the model validators that would like to scrutinize the authenticity of the trained model. Then, it will submit an offer in the Stellar DEX to pay considerable XLM in exchange with the model tokens.
2. *The perspective of the Data Owner* Based on the procedures that are embedded in the vehicle system, when certain distances of the routes passed away, the vehicles automatically go through the following procedures: 1- Select the best offer based on the available amount of DLC it has and XLM it will take. 2- Download the model checkpoint by the IPFS hash address available in the memo field. 3- Train the model in real time by feeding the online data that are being recorded. 4- When arrived at the destination, the learned parameters will be uploaded to the IPFS and receive a 32-byte checksum hash. 5- Create a transaction XDR for offer operation while putting the IPFS hash in the memo of the transaction. 6- Sign the created XDR with its ED25519 [25] private key. 7- Submit the transaction to the network.
3. *The perspective of the Validating Node* Since the model identity tokens are in the possession of the validating nodes, these nodes are responsible to (a) Periodically check the order book and scrutinize the trained model checkpoint on IPFS. (b) If the authenticity and baseline accuracy of the model verified, submit two transactions: (1) Submit an offer to buy DLM in exchange for selling VLM. (2) Send the appropriate VLM in payment transaction to the corresponding computing partner. The rest of the procedures perform as described earlier like the validation of the trained model and cross-assets payments. Figure 2 illustrates the proposed privacy-preserved decentralized deep learning framework, and Fig. 3 shows a chain of offers that are matched and crossed.

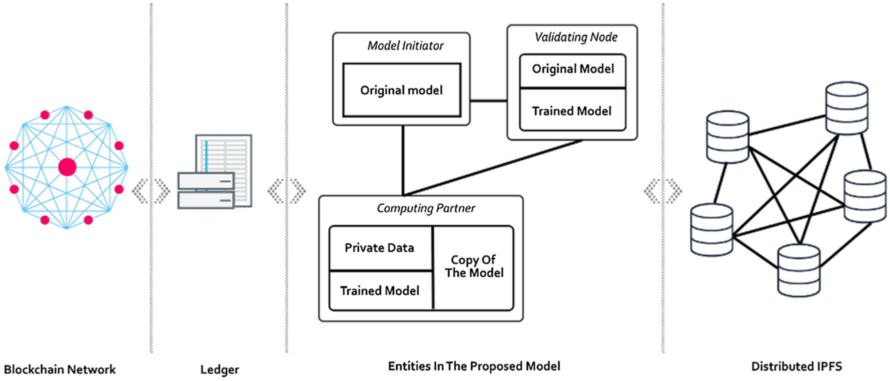
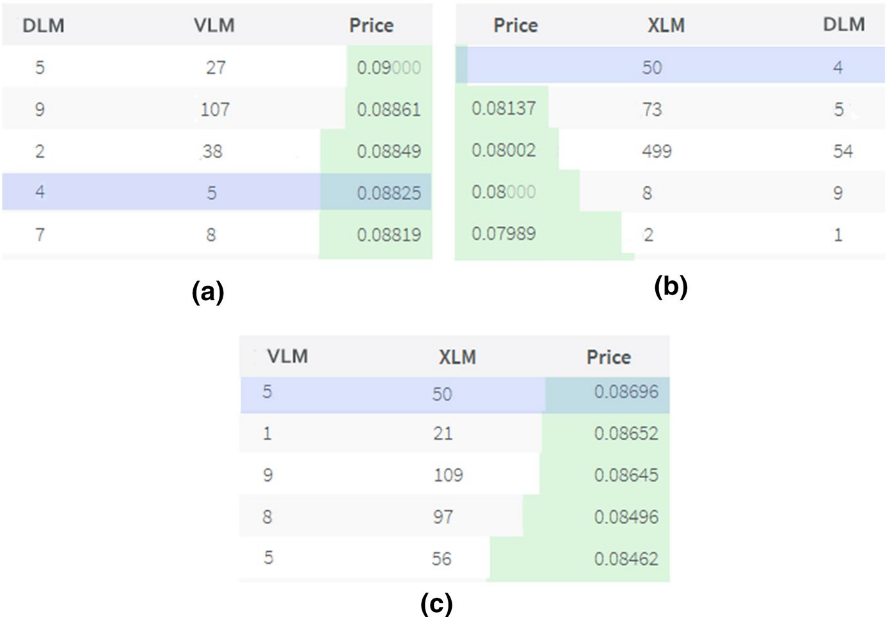


Fig. 2 Proposed privacy-preserved decentralized deep learning



DLM	VLM	Price
5	27	0.09000
9	107	0.08861
2	38	0.08849
4	5	0.08825
7	8	0.08819

(a)

Price	XLM	DLM
	50	4
0.08137	73	5
0.08002	499	54
0.08000	8	9
0.07989	2	1

(b)

VLM	XLM	Price
5	50	0.08696
1	21	0.08652
9	109	0.08645
8	97	0.08496
5	56	0.08462

(c)

Fig. 3 List of offers in the order book where: **a** the offers submitted by model validators that will be used for completing computing partners offers through cross-assets payments, **b** the offers submitted by the model initiator, **c** the offers submitted by computing partners (offers highlighted in blue is one chain of offers that was matched)

6 Deployment

The batching and atomic transactions are two concepts in smart contracts that have close connection. The batching transaction involves grouping the transactions into a set. The atomic transaction is forcing all the transactions to perform together and failing all the transactions if any of them fails. There are several methods to implement smart contracts in the Stellar framework. If an implementation needs intricate logics and conditions which needs a programming language, cross-chain and Ethereum [6] can be employed to solve these challenges. In circumstances that simple sequence of transactions suffices the needs, Stellar Smart Contract (SSC) is a good alternative. The SCC is a sequence of transactions that are linked together under some constraints, e.g., setting time bounds, defining multi-signature transactions, etc. Each transaction has a unique sequence number. This sequence number starts from a large random number and increases only when the current transaction succeeds. A sequence number is a great tool in Stellar that ensures a specific transaction happens only if the preceding one has completed.

Both cross-chain and SSC can be used for the implementation of the proposed framework. However, we choose to use Stellar python SDK to implement an embedded program on autonomous self-driving cars. This embedded python program has a group of operations and functions that are dependent on each other and have a strict sequence order. Table 2 describes the implementation of the proposed model

Table 2 Sequence order of proposed framework implementation from the perspective of the data owner

Sequence	Operation/function	Description
–	–	Computing partner (smart vehicle) find the public key of the model initiator that wants to contribute
1	Call horizon endpoint (/accounts/”public-key”/offers)	Fetch offers of the model initiator ordered by date and select the ledger that contains the offer
2	Call horizon endpoint (/ledgers/”ledger-number”/transaction)	Fetch all the transactions for the selected ledger
3	–	Check the signature of transactions using envelope XDR, model initiator public key and the signature fields
4	Call IPFS gateway	If verified, download the model checkpoint using the IPFS hash address available in the memo field
5	Run the deep learning algorithm on the data	Train the model in real-time by feeding the online data that are recorded (the actual training performs by self-driving car)
6	Call IPFS API	When arrived at the destination, the learned parameters will be uploaded to the IPFS and a 32-byte checksum hash will be received
7	Call horizon transaction endpoint to submit a Manage offer operation	Submit an offer to buy VLM over DLC

from the perspective of the data owner in more details. A cross-chain smart contract can be used to automate the deal between vehicles owner and third-party retailers. For example, the vehicles can automatically purchase new parts if the current parts becoming damaged.

6.1 Requirements

If a new party would like to join the network, there are five infrastructures to be setup:

1. *The stellar core* that holds the copy of the ledger and is responsible for joining the global network and consensus.
2. *The horizon* which is a web API service and enables the interaction with Stellar core, e.g., submitting new exchange offers.
3. *Compliance* that holds the regulations, any request to the network first get checked here for legal obligations.
4. *The bridge* that automates the submitting of transactions on behalf of the account owner.
5. *Federation* since it is hard to remember an address of an account federation acts to resolve a username to an ED25519 public key.

In the proposed model, a computing partner is not obliged to establish an infrastructure to contribute to a model. The computing partner can only create an account in the Stellar network and start submitting the required transactions. However, for the model initiators and validating nodes, it is highly recommended to establish the above-mentioned infrastructures. The validating nodes require an automated payment service which requires a Bridge server. In Fig. 4, we modified

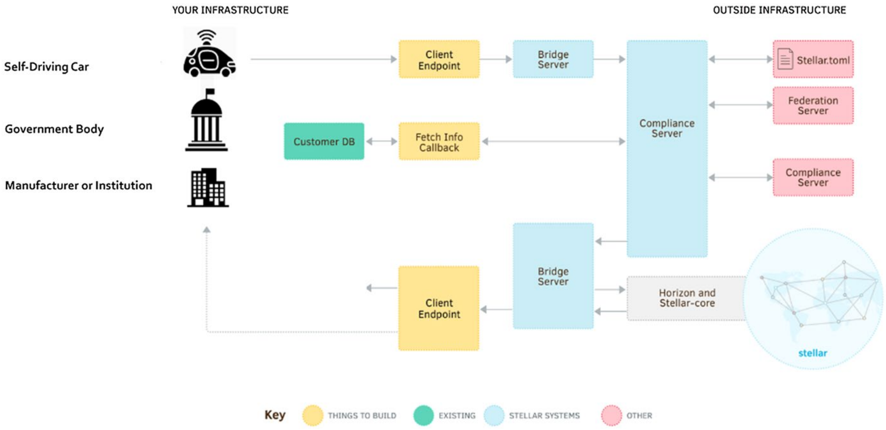


Fig. 4 Stellar infrastructure from the Stellar website with a minor modification according to the proposed model

a figure already available in the Stellar website to represent the requirements for Blockchain infrastructure.

6.2 Blockchain global settings

Another advantage of using Stellar in addition to embedded DEX and asset definition is the high speed of the network and the low time needed for consensus (in average close to 5–10 s). Stellar Consensus Protocol [7] which is a construction of Federated Byzantine Agreement (FBA) enabled this fast performance. Since in the proposed model we used IPFS for storing the large model checkpoints, these data will not affect the ledgers closing time. Furthermore, if the whole infrastructure deployed in a private permissioned ecosystem, it is important to choose an optimal value for the maximum number of transactions to be included in a ledger in such a way that the new transaction set size do not affect the ledger close duration. Figure 5 shows the ledger close time of a well-established network.

7 Contribution to large-scale data analysis

The main factor in large-scale data analysis that enables researchers to make a better decision is the amount of data that they have at their disposal. But the question is how these data should be acquired. It would be great if they can just ask for the data they need and companies, institutions or even ordinary people who hold the data share this information with them. This objective requires an assurance to the users that their data are safe and will not be exposed publicly. By guaranteeing this safety, we can expect that a sizeable data be acquired.

In analyzing large-scale data, lack of adequate processing powers is another challenge and of great importance. If a deep model trains in a decentralized and distributed environment, this efficiency could be diminished. These two characteristics were the objectives in designing the proposed model to ensure the users that their data are safe and out of any abuse and also enables the researchers and companies to train sophisticated models faster and more easily.

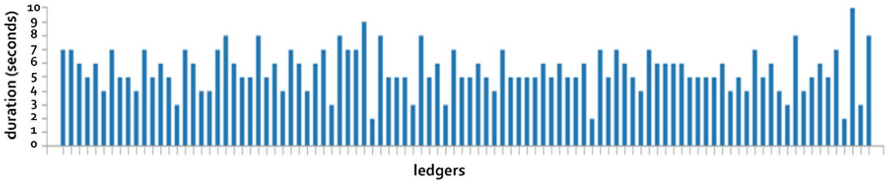


Fig. 5 Duration of the ledger close time which in the normal situation must be between 3 and 10 s

8 Conclusion

In this paper, we proposed a secure decentralized mechanism for training of self-driving cars that incentivizes the data owners to contribute to the accuracy of self-driving cars by sharing their private data. Implementation of incentivization and compensation also have been taken into account by including paying of XLM to computing partners and also controlling the authenticity of their contribution. It is essential to note that some part of this mechanism like many proposed distributed learning methods is still performing off-chain. For example, like [14], the model learned by computing partners will be saved on IPFS.

References

1. Li G, Yu Y (2018) Contrast-oriented deep neural networks for salient object detection. IEEE Trans Neural Netw Learn Syst 29(12):6038–6051
2. Abbasi MH, Majidi B, Eshghi M, Abbasi EH (2019) Deep visual privacy preserving for internet of robotic things. In: 2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI), pp 292–296
3. Kumar K, Shrimankar DD (2018) F-DES: Fast and deep event summarization. IEEE Trans Multim 20(2):323–334
4. Fadaeddini A, Majidi B, Eshghi M (2018) A case study of generative adversarial networks for procedural synthesis of original textures in video games. In: 2018 2nd National and 1st International Digital Games Research Conference: Trends, Technologies, and Applications (DGRC), pp 118–122
5. Nazerdeylami A, Majidi B, Movaghar A (2019) Smart coastline environment management using deep detection of manmade pollution and hazards. In: 2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI), pp 332–337
6. Fadaeddini A, Eshghi M, Majidi B (2018) A deep residual neural network for low altitude remote sensing image classification. In: 2018 6th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS), 2018, pp 43–46
7. Weng J, Weng J, Zhang J, Li M, Zhang Y, Luo W (2018) Deepchain: auditable and privacy-preserving deep learning with blockchain-based incentive. Cryptology ePrint Archive, Report 2018/679, 2018
8. Goel A, Agarwal A, Vatsa M, Singh R, Ratha N (2019) Deepring: protecting deep neural network with blockchain. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops
9. Mendis GJ, Wu Y, Wei J, Sabounchi M, Roche R (2018) Blockchain as a service: a decentralized and secure computing paradigm. arXiv preprint arXiv:1807.02515
10. Salah K, Rehman MHU, Nizamuddin N, Al-Fuqaha A (2019) Blockchain for AI: review and open research challenges. IEEE Access 7:10127–10149
11. Mamoshina P et al (2018) Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. Oncotarget 9(5):5665
12. Konečný J, McMahan HB, Yu FX, Richtárik P, Suresh AT, Bacon D (2016) Federated learning: strategies for improving communication efficiency. arXiv preprint arXiv:1610.05492
13. McMahan B, Ramage D (2017) Federated learning: Collaborative machine learning without centralized training data. Google Research Blog, vol 3
14. Mendis GJ, Sabounchi M, Wei J, Roche R (2018) Blockchain as a service: an autonomous, privacy preserving, decentralized architecture for deep learning. arXiv preprint arXiv:1807.02515
15. Addair T Decentralized and distributed machine learning model training with actors
16. Liu Z et al (2019) A survey on applications of game theory in blockchain. arXiv preprint arXiv:1902.10865

17. Saad et al M (2019) Exploring the attack surface of blockchain: a systematic overview. arXiv preprint arXiv:1904.03487
18. Westerkamp M, Victor F, Küpper A (2018) Blockchain-based supply chain traceability: token recipes model manufacturing processes. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, pp 1595–1602
19. Wang S, Yuan Y, Wang X, Li J, Qin R, Wang F-Y (2018) An overview of smart contract: architecture, applications, and future trends. In: 2018 IEEE intelligent vehicles symposium (IV). IEEE, pp 108–113
20. Benet J (2014) Ipfs-content addressed, versioned, p2p file system. arXiv preprint arXiv:1407.3561
21. Konečný J, McMahan HB, Ramage D, Richtárik P (2016) Federated optimization: distributed machine learning for on-device intelligence. arXiv preprint arXiv:1610.02527
22. Shokri R, Shmatikov V (2015) Privacy-preserving deep learning. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pp 1310–1321
23. Fadaeddini A, Majidi B, Eshghi M (2019) Privacy preserved decentralized deep learning: a blockchain based solution for secure AI-driven enterprise. In: International Congress on High-Performance Computing and Big Data Analysis, pp 32–40
24. Ye G, Liu D, Jhuo I-H, Chang S-F (2012) Robust late fusion with rank minimization. In: 2012 IEEE Conference on Computer Vision and Pattern Recognition. IEEE, pp 3021–3028
25. Bernstein DJ, Duif N, Lange T, Schwabe P, Yang B-Y (2012) High-speed high-security signatures. J Cryptogr Eng 2(2):77–89

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.