Marrying deep learning within blockchain technology for credit card fraud prevention

Imane Karkaba, El Mehdi Adnani, Mohammed Erritali
Data Science for Sustainable Earth (DataEarth) Laboratory, Faculty of Science and Technology, Sultan Moulay Slimane University, Beni Mellal, Morocco

Article Info

Article history:

Received May 29, 2024
Revised Sep 29, 2024
Accepted Oct 7, 2024

Keywords:

Credit card fraud
Deep learning
Blockchain architecture
Cryptocurrency
Chainlink

ABSTRACT

Over the last decade or so, an excessive turnout on e-financial transactions by companies and customers results in a pinnacle growth of credit card fraudulent acts, leading them to lose frequently huge amounts of money. In their trial to find the key to this issue, specialists and experts have founded a bunch of fraud detection and prevention models relied on data mining, machine learning and deep learning. Yet, the outcomes were not effective nor optimal. Thereupon, to foster these prototypes' function, Blockchain -a safe, decentralized and unchangeable database- was deployed to ban any sort of anomaly or data alteration after storing. For identifying malicious financial behaviours, our work managed to intermingle a pre-designed deep learning prototype with Blockchain. That is to say -for the sake of preventing fraudulence that concerns credit card- we applied the former prototype in Blockchain system. Still, Blockchain showed impotence in terms of using off-chain data, which embeds deep learning pattern, specifically through smart contract. Hence, we activated chainlink boosting our model to surmount this obstacle.

Corresponding Author:

Imane Karkaba
Data Science for Sustainable Earth (DataEarth) Laboratory, Faculty of Science and Technology, Sultan Moulay Slimane University
Beni Mellal, 23000, Morocco
Email: imane.karkaba@usms.ma

1. INTRODUCTION

Today, the online scope managed not only to minimize effort and conserve time for its users but also to maximize the services' quality; that is why companies and individuals dive deeply in what we call 'digital'. Nevertheless, falsifiers and fraudsters have become experts in swindling financial operations. Frequently, reports of financial institutions and banks show dramatic losses in billions [1], [2]. So, using online services as a blessing turns into a curse. In this regard, the increased pace of research on credit card fraud over the last two decades has attracted the attention of scientists and experts of financial sector for inventing effective systems that may resolve this issue; in the sense of detecting and stopping illegitimate interventions. Our interest in this study lies in fraud transactions of credit cards, as there are various scams that can threaten financial account owners, credit card holders, enterprises' accounts, and others.

Serious and extensive thinking about credit card fraud involves a mind-boggling journey through a labyrinth of reckoning operations and diagnosis -a puzzle that has to be deciphered radically. A malicious act is mutable and imitative. In addition, the fraud behaviours are dynamic; that is to say, they are not sticking to the precedent pattern when they are exposed to computational analysis. Scammers frequently duplicate the consumer's actions, too. For this reason, a fraudulent act is hard and remains complex all the time to be detected. Therefore -in their attempt to predict, detect and ban fraud threats- scientists have proposed a plethora of approaches. Data mining, machine learning and deep learning are deemed to be the most significant techniques because they are characterized with their detection system efficiency, especially when dealing with vast complexity matters [3]–[7].

For the first category, scientists resorted to a hybrid approach that holds data mining algorithms at several stages including the database level and network level to better the accuracy of fraud detection [3]. Another study combined multiple learned fraud detectors under a "cost model" to decrease loss due to fraud through distributed data mining of fraud models [7]. Besides, some researchers utilized Bayes minimum risk approach to reach optimal results and quantified by monetary saving for detecting credit card fraud [8]. The second category, studies focused on the performance of three different machine learning models: Logistic regression, decision tree and random forest, recommending the third algorithm for its high scores in classification, prediction and detection of fraudulent credit card transaction [5], as well as they adapted undersampling technique to overcome a class imbalance [9]. Also, they tried to enhance the performance of the existing credit card fraud detection system and suggested Approx-SMOTE federated learning credit card fraud detection system [10]. The last category, authors wielded a high performance, distributed cloud computing environment to navigate past common fraud detection problems like class imbalance and scalability [4]. In addition, they drew attention to Autoencoder as an unsupervised deep learning model (DLM) after proving its robustness when trained on a huge dataset -in comparison to ANN and CNN algorithms- for the sake of detecting fraud transactions [6].

In spite of the varied systems and frameworks have been employed for detecting credit card fraud, many shortcomings are still emerging. The frequent limitations concern mostly imbalanced data, adversarial attacks, real-time detection, and data confidentiality. To start with, the imbalanced or skewed class distributed is deemed one of the conventional hurdles that affect critically prediction accuracy. Additionally, alterations of fraud strategies, which means that scammers permanently conceive new attack and fraud tactics to defy credit card fraud detection systems, permitting them to avoid simultaneously the detection of the novel and the earlier-unseen falsified transactions. They use different opposing tricks like data poisoning, evasion attacks and falsifying the input data to deceit the system. Moreover, changes in cardholder's behavior in a continuous way challenges the systems to detect and prevent fraudulent operations. Last and not least, building real-time detection system becomes complicated in fields with huge transactions and giant datasets. So, any minute-delay in fraud detection can lead to financial losses for individuals (cardholders) and institutions.

After assessing numerous credit card fraud systems, we inferred that data mining, machine learning or deep learning systems take advantage of various techniques to boost their strength and efficiency. Yet, they possess pros and cons, the thing that allows machine learning and deep learning algorithms to excel in detecting one class of data but struggle with others, or they may perform well in a specific system and fail in another. Apart from, the common purpose of the majority of the proposed methods is only to detect fraud in new transactions.

In the view of these shortcomings, a proposed model embedded in consuming a DLM in Blockchain technology for many reasons. Blockchain is of key importance in storing data, tamper resistance, and traceability. Furthermore, it uses cryptographic knowledge to ascertain its immutability and unforgeability when treating fraud and data corruption. On the other side, to address the issue of imbalanced data, we have depended on Autoencoder as a deep learning algorithm for its effectiveness, showing optimal results since it does not demand data amendment. Therefore, we have relied on this double-key method to intensify security and data protection as tasks referred to Blockchain, while DLM is responsible of maintaining fraud detection accuracy. For this reason, our prototype is believed to be more resilient and robust in both detection and prevention of fraudulent transactions.

The rest of this article is proceeded as follows: The second section shows strengths and weaknesses of Blockchain architecture and sheds light on Chainlink as a network connecting Blockchain to the real world. The third section is devoted to a description to our proposed method. The visualization (results and discussion) and the conclusion are respectively afforded in the fourth and the fifth sections.

2. BACKGROUND AND MOTIVATION

Specialists and experts approach any new issue with an existing set of scientific research findings, through insight, logical interpretations, and various forms of hypothesis testing, call upon whatever prior experiments they have conducted and whatever research outcomes they own to attempt a solution. Thus, it is common for us to follow the same track, until we have discovered "Blockchain technology", as an efficient tool and optimal strategy for credit card fraud prevention. 'Blockchain' is almost associated with 'Bitcoin', this lets a dilemma for people to realize distinguishably the concept of both Blockchain and Bitcoin; in the sense, they often attain the idea of the first (Blockchain) only in the context of cryptocurrency, ignoring the genuine role of this novice technology. Nonetheless, Bitcoin rests the prime cryptocurrency that used Blockchain for tracing transactions via a network in a precise, confidential, and secure method beyond a third party intervention; the scenario that usually takes place in banks and investment companies [11]. The deployment of Blockchain firstly occurred in 2008, by the time Satoshi Nakamoto produced his article named "Bitcoin: A peer-to-peer Electronic Cash System" as shown in Figure 1 [12].

Figure 1. P2P electronic payment system

2.1. Blockchain concept

First of all, we will clarify the concept of Blockchain (what is Blockchain?), then we will demonstrate the key-motivation behind developing this novel technology. Blockchain is a prominent technology that facilitates the storage and the transmission of values through internet in a rapid, accurate, and safe way. It does not necessitate any interposition of a third participant nor refer to central organ control [13]. It functions as a database encompassing the entire historic of transactions made earlier. The most salient aspect of Blockchain system is 'decentralization' [14]. The latter stands for the multiplicity of the server hosting; in other words, the hosting is done by numerous nodes and not one sole server.

Recently, a tremendous wave of interest towards IoT has taken place. In parallel, Blockchain has known an unprecedented spread in the financial sector. Several technologies hold Blockchain particularly Ethereum that involves ether (eth) as the main cryptocurrency, unlike Bitcoin that sufficiently stockpiles financial operations. So, the precedent stows smart contracts -unconnected cryptograph functions as soon as pre-finite factors emerge. Allowing users to get in touch and circulate their data independently of any supreme organism's intermediation, the smart contract gets into effect as a novice aspect maintaining decentralization beyond the supremacy exerted on users' data by Google, Amazon, Facebook, Microsoft (GAFAM) [15].

2.2. Blockchain functionality

The Blockchain system inquires varied elements of paramount importance for sustaining its efficiency as Figure 2 demonstrates. Primarily, the 'block' notion is pivotal as 'blocks' depict the principal holders carrying a storage of transactions on Blockchain database -transactions cannot be inverted when they are appended to the block. Similarly, the blocks cannot be altered once a block is adjoined to the chain. Since Blockchain is accessible, the whole information storage in blocks will rest changeless [16]. Because of the linear way blocks are located, very close to each other, they are protected with a coding rule computationally labelled 'hash function'. So, reinforcing what was indicated earlier, every single block contains a series of transactions with a source referred to the 'hash' of the precedent block; each individual block is appended to Blockchain after being mined by miners, which are a bunch of computers the purpose of which is achieving the adequate 'hash' for the block aiming at the transaction approval. The process is termed mining which is grounded on a decentralized protocol named 'proof-of-work' [17].

'Transaction' presents the second element. When the transaction takes place, it is stored as a block of data. It demonstrates the mobility or shifting of an asset. The data block can record information related to the user's choice: who, what, when, where, how much, and even the circumstance describes a service or a product. Concerning Bitcoin, a transaction is a cryptocurrency exchange, but in Ethereum, it is any operation may change the status of the data saved within the Blockchain system.

'Consensus' is the third element. It is a gadget tolerating failures effected in Blockchain [18]. It deploys proof-of-work (PoW) protocol. This makes the nodes -of both Ethereum and Bitcoin- in agreement on the status of all data stored on Blockchain, and then forbid some types of fraudulent acts. PoW and Proof-of-Stake (PoS) are the famous kinds of consensus [19]. Ethereum and Bitcoin use PoW because the miner, who first accomplishes forming a novel block charged with transactions, distributes the outcomes in the residue of the system network and gains cryptocurrency. The miner signifies the quickest computer which is able to form a new block by deciphering a cryptographic riddle.

'Smart contracts' represent the ultimate component. They can be defined as recorded programs on Blockchain. The major function of smart contracts is not only to automatize effecting operations without the interposition of the third party but also to automatize the work-flow, by doing the upcoming process when the permitting conditions are available. Their first use was by the Ethereum Blockchain typically when conditions were added to transactions [20].

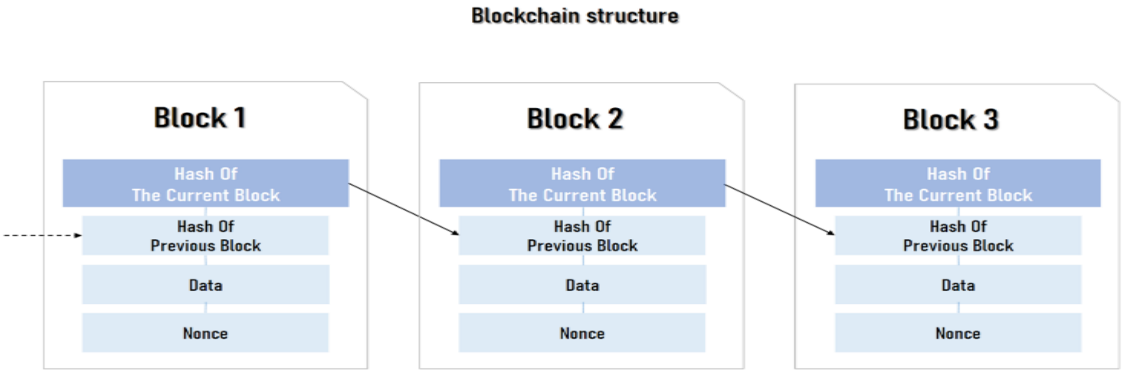


Figure 2. Structure of Blockchain

2.3. Blockchain strengths

The efficiency of Blockchain lies in its security, confidentiality, and speed. The system matches in the alterations accompanied with the digital wave. It is useful in terms of gaining time and effort as making financial operations nowadays needs time and effort to replicate storage, depending on a third interposer approvals. It also stops fraudulence since the storage-saving mechanisms are vulnerable in front of the huge tide of malicious acts. Moreover, doubt and lack of trust can slow data verification. Therefore, Blockchain possesses the for coming characteristics [21]–[23]:

- Decentralization: The aim of this trait is to decrease the control enjoyed by a central entity that has an absolute authority over data users. It brings authority from one central organ to the split network.
- Transparency: The decentralized nature of Blockchain permits transactions to be seen by all the nodes of the network; so, the transparency rate augments equally for the system organs. The relation between blocks and nodes provides a track of each transaction arises in the network. The combination of transparency and consensus renders the Blockchain system virtually unbreakable. Therefore, there is no room for fraud behaviours since every user watches over the network.
- Efficiency and speed: Because of the shared ledger among all organs of the system, time-wasting record reconciliations are removed off. Thus, the transactions approval lasts seconds to be done.
- Immutability and security: All users are required to afford data-accuracy and all validated transactions are immutable as they are stored enduringly. Neither a modification nor a deletion of a transaction can occur -even by a system administrator. Each block of information runs on a hash value. The latter is made-up of a set of alphanumeric characters generated by every single block. Each block includes a hash for itself and a hash of the precedent block. Moreover, each chain of blocks is duplicated on all knots. This feature makes Blockchain technology solid and ensures safety; that no one can alter the data stored in the block.

2.4. Weaknesses of blockchain

For adopting Blockchain, it is essential to comprehend profoundly its working mode, considering its potentials and weaknesses. All scientists and we admit that no system is purely perfect. That is why; we should recognize the barriers might appear before using this architecture. The considerations we emphasize accordingly are [24]:

- Scalability: Pace of transactions in this technology is usually instable. It refers to the dimension of the network; in other words, the more users (nodes) are engaged, the slower the procedure gets.
- High-energy consumption: All the actual Blockchain-based clues, as Bitcoin and Ethereum employ PoW protocol to get and validate transactions, the matter that needs excessive energy for computing.

Fees increase since resources are mandatory to refresh the hardware. Thus, if PoW remains the only available option, we need to pay with energy costs. However, in the next version of Ethereum, PoS is more likely to be used.

- Access to off-chain data: The recorded smart contracts on Blockchain exploit just the local data (data on the chain). It only attains access to the executed transactions and the account's balance. As a result, to recover data from reality stays an impossible task.

2.5. Chainlink

Because of the weak-spots involved within the technology of Blockchain as cited antecedently, we suggest -in our work- 'Chainlink' [25] which purposes to trigger a global network of computers in order to afford authentic data from reality to smart contract streaming on the uppermost area of Blockchain system [26], as clarified in Fgure 3.

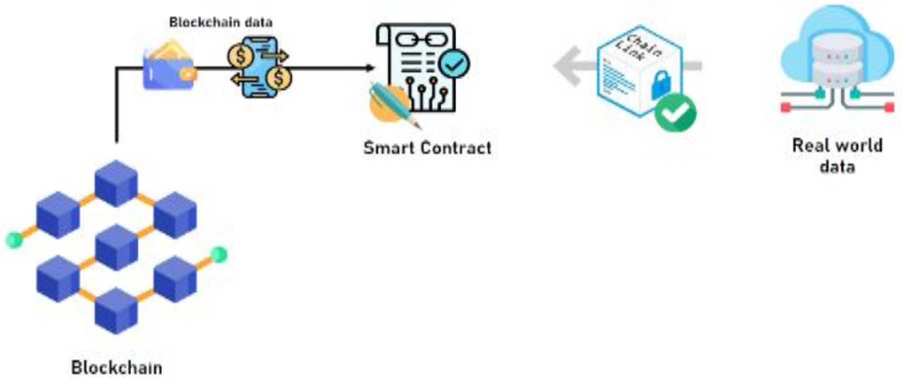


Figure 3. Chainlink to afford off-chain data

2.5.1. Smart contracts and on-the chain data

Smart contracts can not engage in agreements relied on data from reality (off-chain). The thing which restrains smart contracts deployment. This defeat stimulates 'Oracle': an operating system that functions as an overpass letting a double-manner transmission of data between smart contracts and the concrete world. Thus, it is the Oracle that allows us to surmount the issue of getting outer data in a pattern on the chain.

We can consider centralized Oracles as a loophole that decreases the advantages of smart contracts. So, they cannot be trusted. Consequently, Chainlink has come to light. The system is a decentralized network made up of Oracles whose role is to carry data from off-chain sources to on-chain contracts which abolish trustworthiness issue that can happen by the time of utilizing one centralized source as shown in Figure 4 [27].

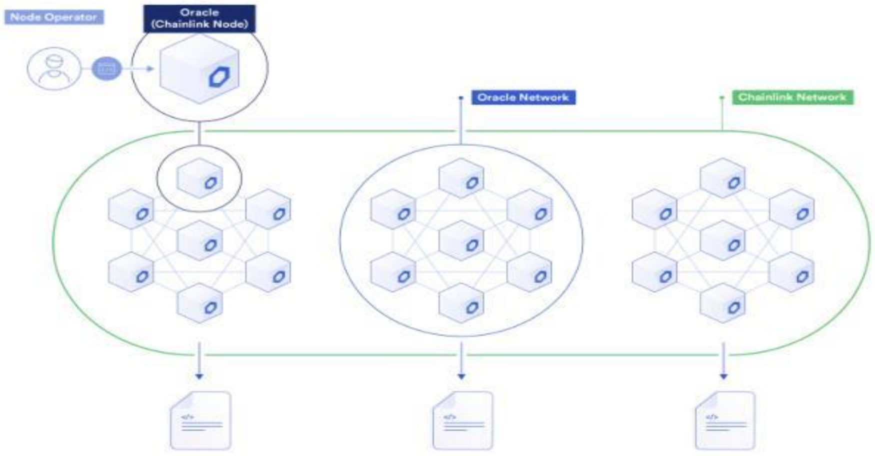


Figure 4. Different components of chainlink's Oracle Network [28]

The smart contracts are unable to interact nor to interconnect directly with the real world when obtaining data. The reason why a smart contract is considered the consumer number one of Chainlink. As a result, the process is achieved via a system where the inquiry for external data is conveyed through transactions' happening. Thereafter, an extrinsic party is intimated and gathers the demanded data, proceeds it, and ultimately transfers the reply via the chain as it is shown in Figure 5 [29], [30].

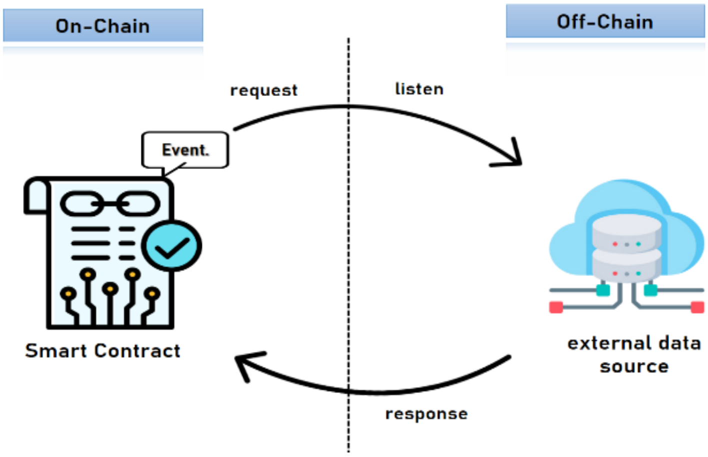


Figure 5. Off-chain data request mechanism

Again, when a smart contract requests data by emitting a transaction event, the Chainlink protocol records this event and creates an service level agreement (SLA). The SLA generates three subcontracts: (1) a Chainlink Contract Reputation, whose function is to check the tracking way (history) of an Oracle provider, to determine accuracy and performance, then to evaluate and exclude less reliable nodes. (2) The Chainlink Order Matching Contract, whereby the nodes retrieve the request provided by the precursor contract (the Reputation Contract), selects the number and type of nodes that are necessary to meet the request. Finally, (3) Chainlink Aggregation Contract which corrects inaccurate data. It takes all the data selected by the Oracles and approves or reconciles them to obtain a precise result, as Figure 6 shows.

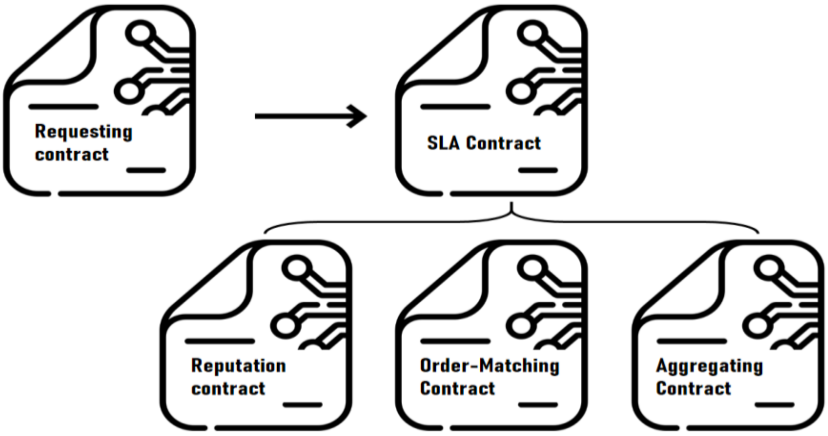


Figure 6. Chainlink smart contracts

The activation of Chainlink smooths the path for Ethereum to exploit various off-chain data. Referring to its systematic essence -here- we will benefit from Blockchain, specifically the Ethereum network, to ban credit card fraud merging this thoroughgoing technology with deep learning as a detecting tool. The next section represents a stage where we overcome all the challenges confronted and discover the clues to reach the intended aims.

3. METHOD

This section is devoted to clarify the way we deploy deep learning in Blockchain for detecting and preventing credit card fraud transactions, making the structure of our suggested ecosystem crystal-clear, as Figure 7 demonstrates. So, after building a model using Autoencoder to detect fraudulent transactions, Blockchain is applied to substitute the quintessential database, on grounds of durability that describes it which -in turn- enhances banning other types of fraud linked to the change and corruption of the recorded data. The whole code is transcribed in the smart contract, and this is the point when the advantage of the deployed DLM is profited. Yet, the smart contract's inability to obtain off-chain data provokes the intervention of Chainlink to get the off-chain data into the chain, permitting the consumption of our model in Blockchain. Our principal goal in this section is to spotlight the second half of the double-key method implemented; in other words, we focalized systematically on Blockchain technology and the mechanisms it involves. Whereas, the DLM part was briefly described since it was already forged in our previous study [6] through a sequence of procedures where a bunch of techniques came into play. After that -in the study in your hands- the DLM was exploited in Blockchain technology to play a role of a detector.

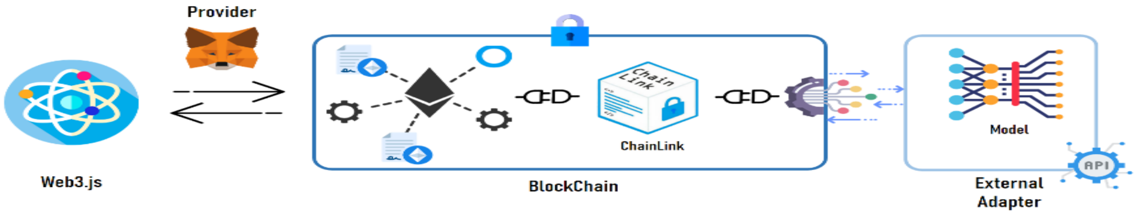


Figure 7. Architecture of the system fusing Blockchain with DLM

3.1. Deep learning model

The reason why we have picked the Autoencoder model for detecting fraudulent transactions stems from the findings of a previous work of ours where we have conducted a comparison study concerned the algorithms: ANN, CNN, and Autoencoder [6], taking into account 'precision', 'recall', and 'accuracy' as metrics of efficiency measurement. This study was conducted on a dataset (attained from Kaggle) of 284,807 transactions, just 492 of which were described as malicious. The matter that made us encounter the first challenge related to the imbalanced data. Autoencoder won over the other algorithms in dealing with the present dataset. It is released that three layers of encoding are the optimal parameters noticed after tuning the hyper-parameters: Tanh as the activation function along the hidden layers and Sigmoid in the output layer.

3.1.1. Dataset description

The dataset exerted in this work is a Europe credit card dataset, representing an imbalanced real-world one. It includes credit card transactions made by European cardholders in September 2013. This dataset introduces all transactions occurring over two days, with 492 instances of fraud identified out of 284,807 transactions. It obviously shows a highly imbalanced data, with fraudulent transactions accounting for nearly 0.172% of all transactions. The dataset contains only numerical input variables which are the result of a PCA transformation due to confidentiality concerns. Consequently, providing the original features or more background information is not feasible. The features are 30 principal components as detailed described in [31].

3.1.2. Selected algorithm

The Autoencoder is a subset of neural networks used to learn data encoding in an unsupervised manner. Its purpose is to learn a lower-dimensional representation (encoding) for higher-dimensional data, specifically for reducing dimensionality, by training the network to select the most crucial components of the input. Its architecture encompasses successively three constituents: Encoder, Bottleneck and Decoder [32]. The option fell on this algorithm, as it does not need a dataset modification allowing us to surpass the imbalanced data issue.

3.2. Blockchain technology

After the stage of detecting fraudulent transactions using the DLM, comes the stage of storing the transactions in the database. However, we may face another type of fraud represented by the corruption and alteration of data after the storing phase. For this purpose, a decentralized immutable database was adopted, namely Ethereum Blockchain that enables us to use the smart contract.

3.3. Mechanisms for the system deployment

3.3.1. Smart contract and external adapter

The smart contract's ineptitude appears when it cannot bring off-chain data (data out of Blockchain). This is treated as a serious challenge preventing us to consume our model in Blockchain. To overcome this obstacle, Chainlink shows up to provide the chain with data from the external world. The external adapters function as one API to do perplex computations because every transaction is paid on the chain and they serve Chainlink in terms of offering it data directly. Hence, we have used our DLM in the external adapter so that it can be available for the smart contract across Chainlink.

3.3.2. Chainlink

Chainlink here plays the role of an intermediary instrument between the external adapter and the smart contract. It provides off-chain data from external sources to the Blockchain network.

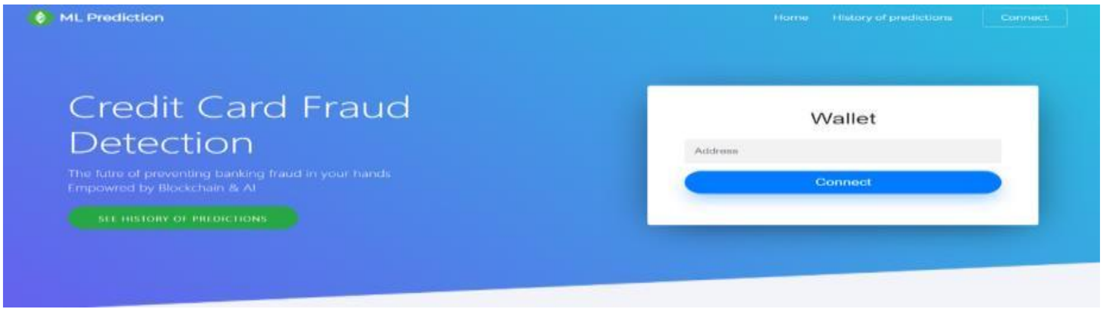
3.3.3. Website and cryptocurrency

Hereupon, the system becomes apt to recover transactions from storage and label them with predictions done by the model. After that, it stores transactions and their corresponding predictions on Blockchain in an inalterable mode. So as to justify the practicality of this merger, a website was developed and connected to Blockchain exploiting web3.js in order to link the Blockchain with the Metamask wallet [33] to effect transactions on the chain. This website will be devoted to a couple of users. The first user, after his wallet detection, all transactions he has executed are exposed to view and he owns access to execute more transactions as well as he can see their predictions by paying with ETH cryptocurrency. In parallel, the second user is the one who owns the smart contract -who has also used it. He can examine the balance the smart contract stored after every prediction and he can withdraw the balance to his wallet, as well.

4. VISUALIZATION

So that we could marry the AI model within Blockchain technology, we designed a web user interface that applies all the previously indicated attributes. This web app contains the following elements:

- A button allowing the user to connect his wallet.
- A section dedicated to the display of previous transactions performed based on the connected wallet.
- A form to enter the attributes of the transaction in order to make a prediction.
- A section dedicated to the owner of the smart contract for withdrawing the contract's balance. The two figures: Figures 8 and 9 show the primary graphical user interface before a wallet is connected.



Credit Card Fraud Detection

The futre of preventing banking fraud in your hands
Empowred by Blockchain & AI

Figure 8. Main user interface before a wallet connection (a)

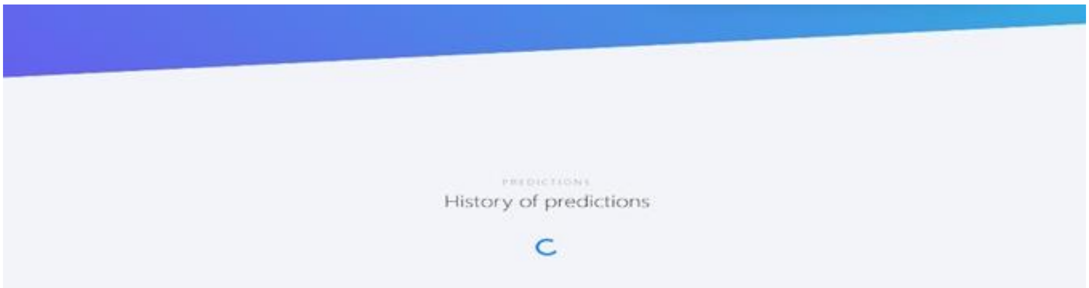
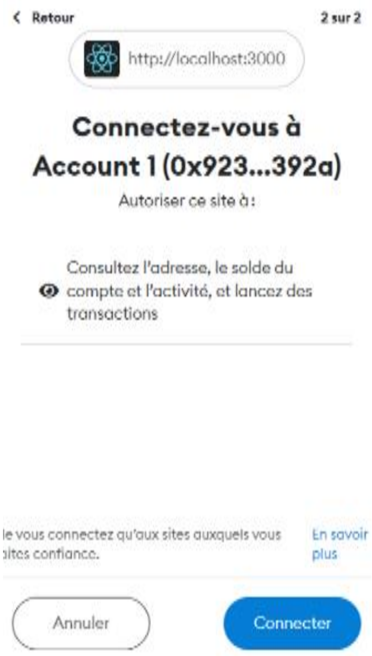


Figure 9. Main user interface before a wallet connection (b)

4.1. Regular user

A regular user (a normal user) could log in by clicking on the "Connect" button as shown in Figures 10 and 11 and the application will automatically detect the connected wallet and the wallet address will be displayed along with the records of the previous transactions made by the current account as shown in Figure 12.



< Retour 2 sur 2

http://localhost:3000

Connectez-vous à
Account 1 (0x923...392a)

Autoriser ce site à :

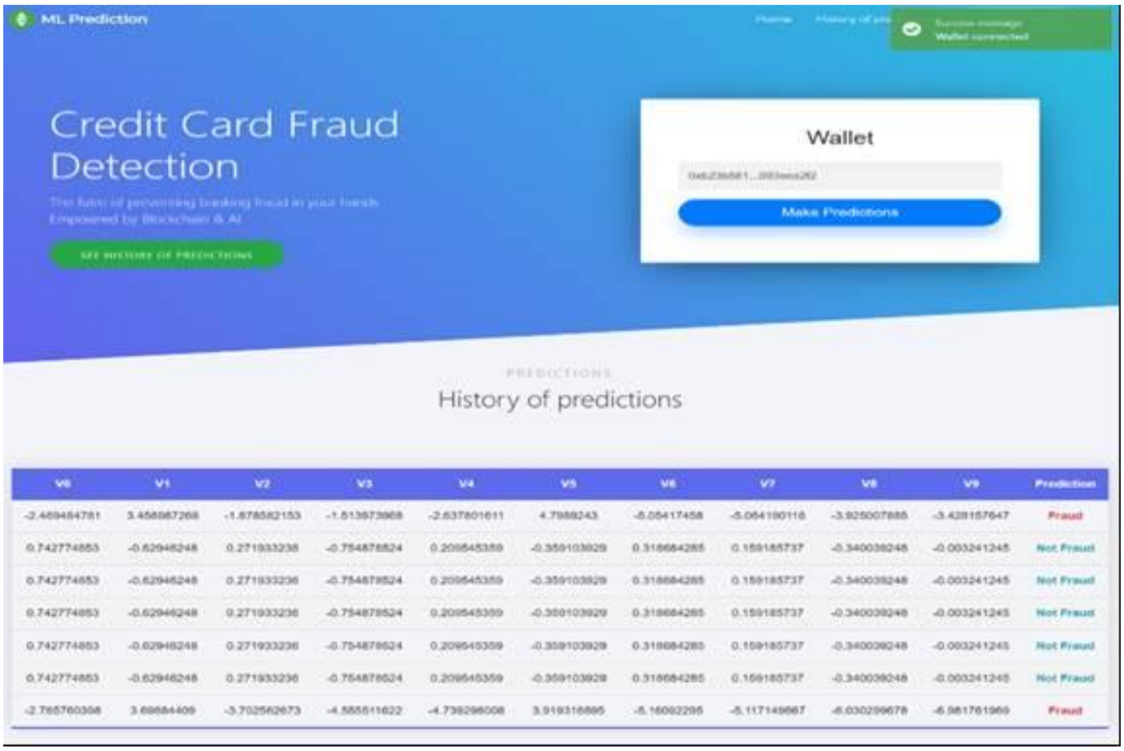
Consultez l'adresse, le solde du compte et l'activité, et lancez des transactions

le vous connectez qu'aux sites auxquels vous
oites confiance.

En savoir plus

Annuler Connecter

Figure 10. Wallet connection



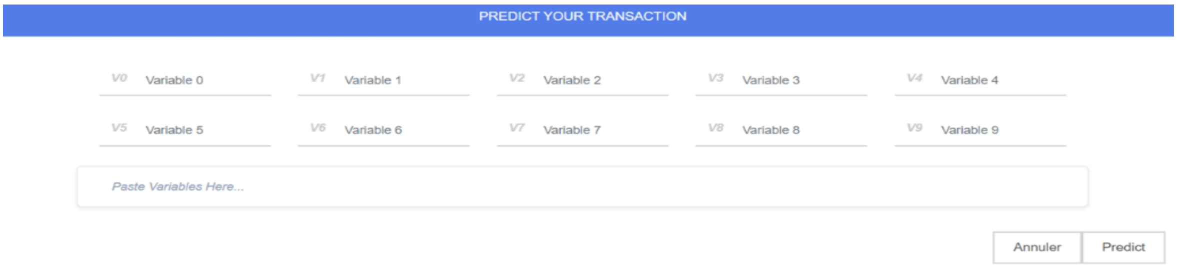
Credit Card Fraud Detection

Wallet

History of predictions

V0	V1	V2	V3	V4	V5	V6	V7	V8	V9	Prediction
-2.469484781	3.458087268	-1.878582153	-1.813673868	-2.637801611	4.7988243	-6.05417458	-6.064190116	-3.925007885	-3.428157647	Fraud
0.742774853	-0.62946248	0.271933236	-0.754878524	0.209645359	-0.359103929	0.318684285	0.159185737	-0.340039248	-0.003241245	Not Fraud
0.742774853	-0.62946248	0.271933236	-0.754878524	0.209645359	-0.359103929	0.318684285	0.159185737	-0.340039248	-0.003241245	Not Fraud
0.742774853	-0.62946248	0.271933236	-0.754878524	0.209645359	-0.359103929	0.318684285	0.159185737	-0.340039248	-0.003241245	Not Fraud
0.742774853	-0.62946248	0.271933236	-0.754878524	0.209645359	-0.359103929	0.318684285	0.159185737	-0.340039248	-0.003241245	Not Fraud
0.742774853	-0.62946248	0.271933236	-0.754878524	0.209645359	-0.359103929	0.318684285	0.159185737	-0.340039248	-0.003241245	Not Fraud
-2.765760308	3.69884409	-3.702562673	-4.585511622	-4.739298008	3.919316885	-6.16002296	-6.117149867	-6.030299678	-6.981761969	Fraud

Figure 11. Main user interface after a client wallet connection



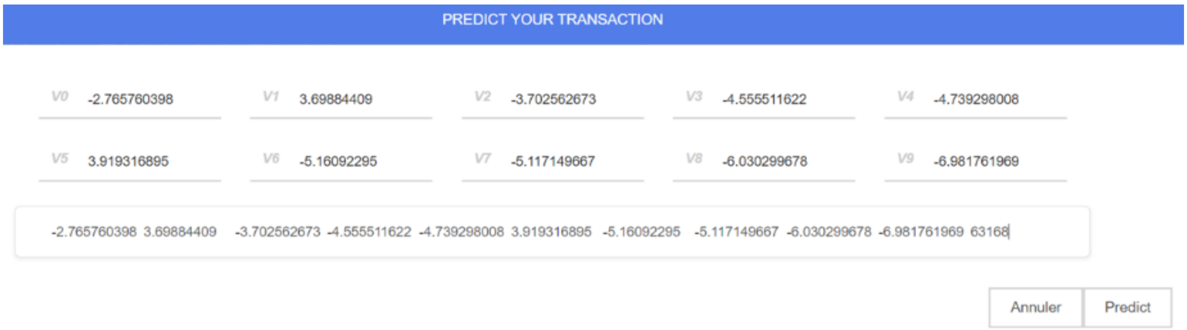
PREDICT YOUR TRANSACTION

V0 Variable 0
V1 Variable 1
V2 Variable 2
V3 Variable 3
V4 Variable 4
V5 Variable 5
V6 Variable 6
V7 Variable 7
V8 Variable 8
V9 Variable 9

Paste Variables Here...

Figure 12. Transaction attributes form

Hereafter, by clicking on the "make a prediction" button, the user can make a prediction as shown in Figure 11. Then, a form is displayed requesting the input of the transaction attributes (Figures 13 and 14). Ultimately, the demand is proceeded and the transaction's prediction is generated and displayed as shown in Figure 15.

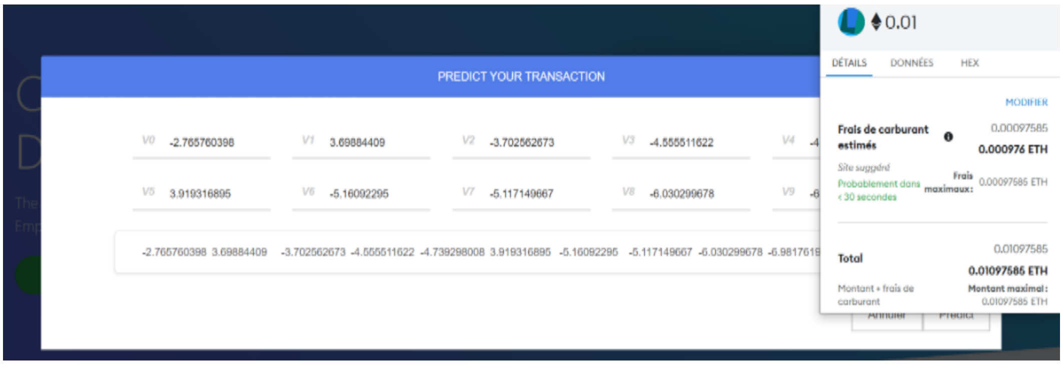


PREDICT YOUR TRANSACTION

V0 -2.765760398
V1 3.69884409
V2 -3.702562673
V3 -4.555511622
V4 -4.739298008
V5 3.919316895
V6 -5.16092295
V7 -5.117149667
V8 -6.030299678
V9 -6.981761969

-2.765760398 3.69884409 -3.702562673 -4.555511622 -4.739298008 3.919316895 -5.16092295 -5.117149667 -6.030299678 -6.981761969 63168

Figure 13. Predicting transactions



PREDICT YOUR TRANSACTION

V0 -2.765760398
V1 3.69884409
V2 -3.702562673
V3 -4.555511622
V5 3.919316895
V6 -5.16092295
V7 -5.117149667
V8 -6.030299678

-2.765760398 3.69884409 -3.702562673 -4.555511622 -4.739298008 3.919316895 -5.16092295 -5.117149667 -6.030299678 -6.9817619

0.01

DÉTAILS DONNÉES HEX

MODIFIER

Frais de carburant estimés: 0.00097585 0.000976 ETH

Site suggéré

Probablement dans < 30 secondes

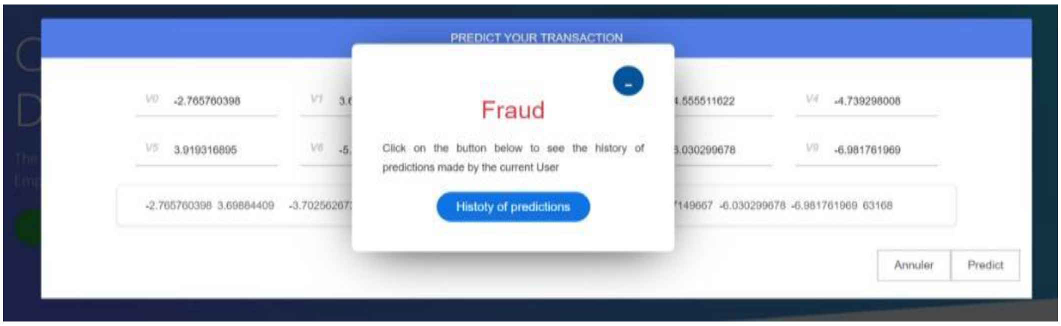
Frais maximaux: 0.00097585 ETH

Total: 0.01097585 0.01097585 ETH

Montant + frais de carburant

Montant maximal: 0.01097585 ETH

Figure 14. Prediction payment



PREDICT YOUR TRANSACTION

V0 -2.765760398
V4 -4.739298008
V5 3.919316895
V9 -6.981761969

-2.765760398 3.69884409 -3.70256267 ... 149667 -6.030299678 -6.981761969 63168

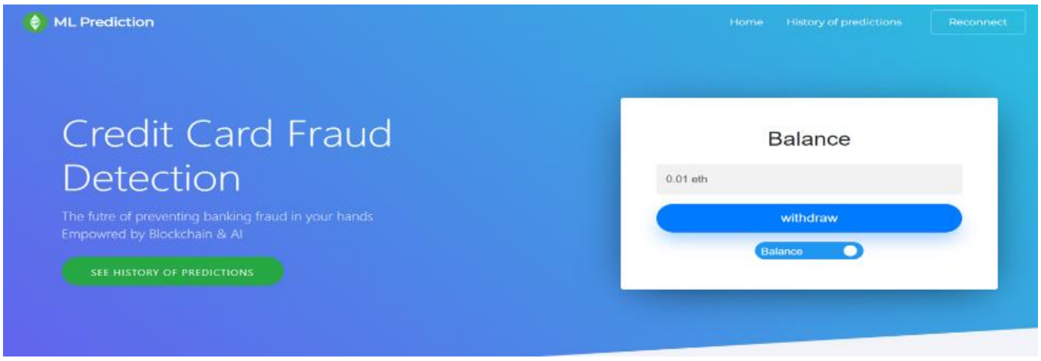
Fraud

Click on the button below to see the history of predictions made by the current User

Figure 15. Prediction result

4.2. Owner of the smart contract

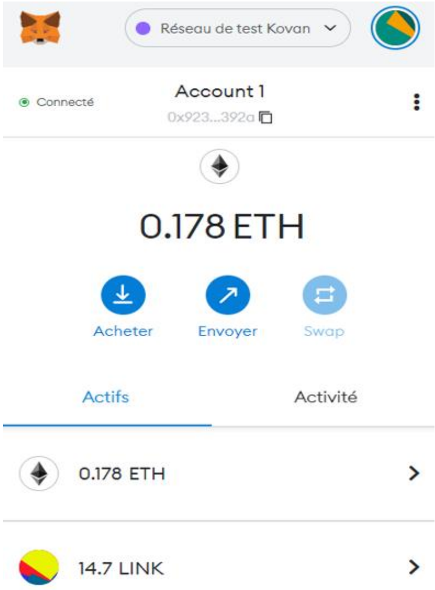
This user is also considered a normal user but with the added feature that after connecting his wallet, he is able to withdraw the contract's balance got by the predictions which other users made as it is respectively demonstrated in the Figures 16-19.


Credit Card Fraud Detection

The futre of preventing banking fraud in your hands
Empowered by Blockchain & AI

Balance: 0.01 eth

Figure 16. The contract balance before withdrawing it


Réseau de test Kovan

Connecté

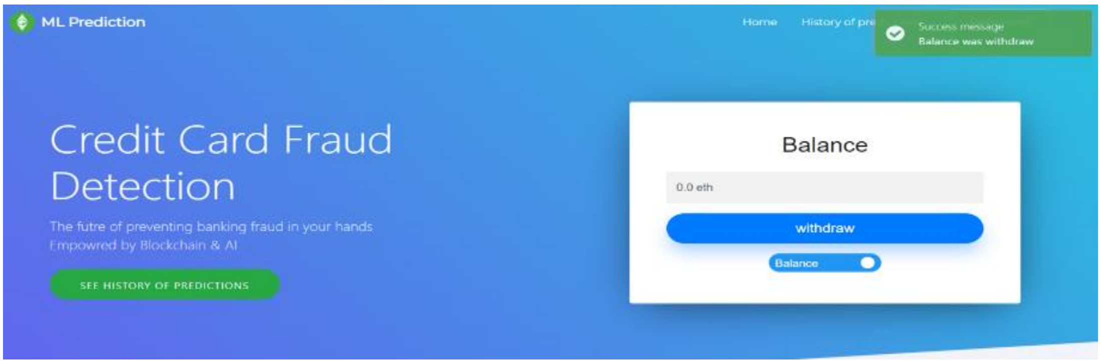
Account 1
0x923...392a

0.178 ETH

0.178 ETH

14.7 LINK

Figure 17. Account balance before withdrawing contract balance

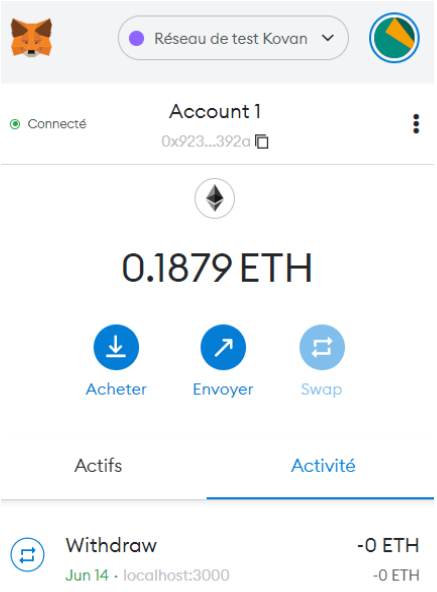

Success message
Balance was withdraw

Credit Card Fraud Detection

The futre of preventing banking fraud in your hands
Empowered by Blockchain & AI

Balance: 0.0 eth

Figure 18. The contract balance after withdrawing it



Account 1
0x923...392a

0.1879 ETH

Withdraw -0 ETH
Jun 14 · localhost:3000 -0 ETH

Figure 19. Account balance after withdrawing contract balance

In the light of the findings produced, which evinces an unprecedented efficiency of our prototype in banning fraudulent transactions. So, based on an in-depth evaluation of -firstly- the results generated previously by the DLM, we deduced that the latter has shown optimal scores in terms of accuracy, precision and f1-score. Secondly, the assessment of Blockchain structure justifies its workability because of the multiple mechanisms brought automatically into service as soon as this technology is activated.

Our proposed system is of a paramount significance to confront credit card fraud. Not only can it detect fraudulent transactions (DLM) but also prevent them (Blockchain). This is a remarkable improvement, because to date, the best achievable results by the majority of works conducted earlier -relied on AI algorithms- did not lead to radical solutions. In comparison to our model, they employed numerous balancing techniques to surpass imbalanced dataset issue. Still, most of the experimental outcomes were not pertinent. On the contrary, our model has demonstrated promising results (e.g., 93% as f1-score in the classification case). This is owing to the essence that our model does not require any techniques to adjust the dataset. Similarly, when the Blockchain comes into play, most studies relied on the basic Blockchain structure. It remains locked, and does not permit to call any type of data. Thus, it is hard to operate in a flexible way since they -even in their best cases- were obliged to convert the targeted model into an adequate format to be consumed on the Blockchain. In contrast, the outcomes of the present study reveal that Blockchain is used in its advanced version, involving the intervention of 'Chainlink' component that let the system unlocked and accessible to get external data. The matter proves a successful combination, especially to swell security, integrity and transparency.

Eventually, after an insightful meditation at the series of figures we have come out with in this study, it is evident that our system is practical for it can be smoothly re-used as an ecosystem by the financial institutions. The system allows them to bring their own database into effect, simply thanks to the role of Chainlink. For bye, the designed website mentioned above, implies that our concept is translated from a scientific experiment into a real-world system can be profited concretely by banks to detect and prevent fraudulent transactions.

5. CONCLUSION

This paper is intended to give a comprehensive image of our proposed model. Merging deep learning with Blockchain has been an efficient method to tackle credit card fraud. Thanks to deep learning characteristics sketched with its ability to handle huge and complex datasets and has been proved to reach state-of-the-art performance on a wide range of problems -as embedded in our topic matter- and its adaptability and scalability. In addition, owing to the Blockchain strengths determined by its functionality, its possession of high security, and its immutability and traceability. We have built a solid prototype, manages to make transitional solutions via neural networks and creates an unchangeable storage of transactions with end-to-end encryption to ban fraud and illegitimate activities.

The present study is an expansion of a preliminary project where we stressed only deep learning-based systems to cope with the same issue. According to our experience, there were no instant recipes. It was imperative to sift through many variables and possibilities that come to bear on our problematic. Still, however appealing a particular approach might be to us, however smart and practical it might seem, the best method remains non-stop researching and trying other techniques; simply because the evolution of defrauding is on an ongoing vertical growth.

This work has triggered our interest for further experiments to be undertaken, which might concern fusing more sophisticated algorithms beyond traditional deep learning so that we can reinforce privacy, ameliorate robust testing environments and sustain the security of Blockchain system.

REFERENCES

[1] Y. Sahin and E. Duman, "Detecting credit card fraud by ANN and logistic regression," in *2011 international symposium on innovations in intelligent systems and applications*, 2011, pp. 315–319, doi: 10.1109/INISTA.2011.5946108.

[2] M. A. Ali, M. A. Azad, M. Parreno Centeno, F. Hao, and A. van Moorsel, "Consumer-facing technology fraud: Economics, attack methods and potential solutions," *Future Generation Computer Systems*, vol. 100, pp. 408–427, Nov. 2019, doi: 10.1016/j.future.2019.03.041.

[3] B. B. Sagar, P. Singh, and S. Mallika, "Online transaction fraud detection techniques: A review of data mining approaches," in *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, 2016, pp. 3756–3761.

[4] A. Roy, J. Sun, R. Mahoney, L. Alonzi, S. Adams, and P. (2018 Beling, "April). Deep learning detecting fraud in credit card transactions," *InSystems and Information Engineering Design Symposium (SIEDS)*, pp. 129–134, 2018, doi: 10.1109/SIEDS.2018.8374722.

[5] J. K. Afriyie *et al.*, "A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions," *Decision Analytics Journal*, vol. 6, p. 100163, 2023, doi: 10.1016/j.dajour.2023.100163.

[6] I. Karkaba, E. M. Adnani, and M. Erritali, "Deep learning detecting fraud in credit card transactions," *Journal of Theoretical and Applied Information Technology*, vol. 101, no. 9, pp. 3557–3565, 2023.

[7] P. K. Chan, W. Fan, A. L. Prodromidis, and S. J. Stolfo, "Distributed data mining in credit card fraud detection," *IEEE Intelligent Systems and Their Applications*, vol. 14, no. 6, pp. 67–74, 1999, doi: 10.1109/5254.809570.

[8] A. C. Bahnsen, A. Stojanovic, D. Aouada, and B. Ottersten, "Improving credit card fraud detection with calibrated probabilities," in *Proceedings of the 2014 SIAM international conference on data mining*, 2014, pp. 677–685, doi: 10.1137/1.9781611973440.78.

[9] A. Dal Pozzolo, "Adaptive machine learning for credit card fraud detection," p. 199, 2015.

[10] J. Wang, W. Liu, Y. Kou, D. Xiao, X. Wang, and X. Tang, "Approx-SMOTE Federated learning credit card fraud detection system," in *Proceedings - International Computer Software and Applications Conference*, 2023, vol. 2023-June, pp. 1370–1375, doi: 10.1109/COMPSAC57700.2023.00208.

[11] D. Cahill, D. G. Baur, Z. F. Liu, and J. W. Yang, "I am a blockchain too: How does the market respond to companies' interest in blockchain?," *Journal of Banking and Finance*, vol. 113, p. 105740, 2020, doi: 10.1016/j.jbankfin.2020.105740.

[12] E. Tijan, S. Aksentijević, K. Ivanić, and M. Jardas, "Blockchain technology implementation in logistics," *Sustainability*, vol. 11, no. 4, p. 1185, 2019, doi: 10.3390/su11041185.

[13] M. Pilkington, "Blockchain technology: principles and applications," in *Research Handbook on Digital Transformations*, Edward Elgar Publishing, 2016.

[14] N. Z. Benisi, M. Aminian, and B. Javadi, "Blockchain-based decentralized storage networks: A survey," *Journal of Network and Computer Applications*, vol. 162, p. 102656, 2020, doi: 10.1016/j.jnca.2020.102656.

[15] D. Vujičić, D. Jagodić, and S. Randić, "Blockchain technology, bitcoin, and Ethereum: A brief overview," *2018 17th International Symposium on Infoteh-Jahorina, Infoteh 2018 - Proceedings*, vol. 2018-Janua, pp. 1–6, Apr. 2018, doi: 10.1109/INFOTEH.2018.8345547.

[16] S. I. M. Ali, H. Farouk, and H. Sharaf, "A blockchain-based models for student information systems," *Egyptian Informatics Journal*, vol. 23, no. 2, pp. 187–196, 2022, doi: 10.1016/j.eij.2021.12.002.

[17] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract]," *ACM SIGMETRICS Performance Evaluation Review*, vol. 42, no. 3, pp. 34–37, 2014, doi: 10.1145/2695533.2695545.

[18] A. Baliga, "Understanding blockchain consensus models," *Persistent*, vol. 4, no. 1, p. 14, 2017.

[19] W. Li, S. Andreina, J.-M. Bohli, and G. Karame, "Securing proof-of-stake blockchain protocols," in *Data privacy management, cryptocurrencies and blockchain technology*, Springer, 2017, pp. 297–315.

[20] A. Wright and P. De Filippi, "Decentralized blockchain technology and the rise of lex cryptographia," *SSRN Electronic Journal*, 2015, doi: 10.2139/ssrn.2580664.

[21] N. Hackius and M. Petersen, "Blockchain in logistics and supply chain: trick or treat?," in *Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment. Proceedings of the Hamburg International Conference of Logistics (HICL), Vol. 23*, 2017, pp. 3–18, doi: 10.15480/882.1444.

[22] U. Tariq, A. Ibrahim, T. Ahmad, Y. Bouteraa, and A. Elmogy, "Blockchain in internet-of-things: a necessity framework for security, reliability, transparency, immutability and liability," *IET Communications*, vol. 13, no. 19, pp. 3187–3192, 2019, doi: 10.1049/iet-com.2019.0194.

[23] N. M. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in IoT," *Procedia Computer Science*, vol. 132, pp. 1815–1823, 2018, doi: 10.1016/J.PROCS.2018.05.140.

[24] V. Babich and G. Hilary, "OM Forum—Distributed ledgers and operations: What operations management researchers should know about blockchain technology," *Manufacturing and Service Operations Management*, vol. 22, no. 2, pp. 223–240, 2020, doi: 10.1287/msom.2018.0752.

[25] A. Beniiche, "A study of blockchain oracles," *arXiv preprint arXiv:2004.07140*, 2020, doi: 10.48550/arXiv.2004.07140.

[26] X. Liu, R. Chen, Y.-W. Chen, and S.-M. Yuan, "Off-chain data fetching architecture for ethereum smart contract," in *2018 International Conference on Cloud Computing, Big Data and Blockchain (ICCBB)*, 2018, pp. 1–4, doi: 10.1109/ICCBB.2018.8756348.

[27] S. K. Lo, X. Xu, M. Staples, and L. Yao, "Reliability analysis for blockchain oracles," *Computers and Electrical Engineering*, vol. 83, p. 106582, 2020, doi: 10.1016/j.compeleceng.2020.106582.

[28] G. Lobo, "Oracle networks: a deep dive into data bridging solutions," *The Tie Research*, 2022.

[29] R. Mühlberger *et al.*, "Foundational oracle patterns: Connecting blockchain to the off-chain world," in *International Conference on Business Process Management*, 2020, pp. 35–51, doi: 10.1007/978-3-030-58779-6_3.
[30] L. Breidenbach *et al.*, "Chainlink 2.0: Next steps in the evolution of decentralized oracle networks," *Chain. Labs*, 2021.
[31] "Credit Card Fraud Detection." https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud (accessed Aug. 14, 2024).
[32] H. Bandyopadhyay, "Autoencoders in deep learning: tutorial and use cases [2024]," Jun. 04, 2021. https://www.v7labs.com/blog/autoencoders-guide (accessed Aug. 14, 2024).
[33] A. Goyal, "Blockchain wallet for secure transactions," *SSRN Electron. Journal*, vol. 100, p. 6, 2024, doi: 10.2139/ssrn.4487894.

BIOGRAPHIES OF AUTHORS

Imane Karkaba is a Ph.D. student in Faculty of Sciences and Techniques, Sultan Moulay Slimane University, Beni Mellal, Morocco. She received two B.Sc degrees: The first in Development of Information and Communication Systems from the University Moulay Ismail, Meknes, and the second in Qualification for Teaching Professions specialized in Computer Science from the University Cadi Ayyad, Marrakech. She got the M.Sc degree in Big Data and Internet of Things from ENSAM, University Hassan II, Casablanca. She is currently a high school ICT teacher. Her research areas include AI, machine learning, deep learning, anomaly detection, fraud prevention, blockchain, and intelligent systems. She is an active contributor in different scientific journals and conferences as an invited board member or guest reviewer. She can be contacted at email: imane.karkaba@usms.ma.

El Mehdi Adnani is a Ph.D. student in Faculty of Sciences and Techniques, Sultan Moulay Slimane University, Beni Mellal, Morocco. He obtained his B.Sc degree in Computer Science from the University Sultan Moulay Slimane, Beni Mellal. He graduated with a M.Sc degree in Business Intelligence form the same university. He is actually a software engineer. His research interests include AI, machine learning, deep learning, and fraud detection systems. He is also an Oracle Certified Professional Java developer and a Blockchain enthusiast. He can be contacted at email: mehdi.adnani2@gmail.com.

Mohammed Erritali is a Ph.D. researcher and professor in Faculty of Sciences and Techniques, Sultan Moulay Slimane University, Beni Mellal, Morocco. He is a Data4Earth Lab member in the same university. He has supervised and co-supervised more than 30 masters and 20 Ph.D. students. He has authored or co-authored more than 100 publications, with 16 H-index and more than 1000 citations. His research interests include AI, IoT, machine learning, deep learning, anomaly detection, sentiment analysis, and computer network security. He can be contacted at email: m.erritali@usms.ma.