ISSN : 2350-0743

International Journal of Recent Advances in Multidisciplinary Research

Vol. 12, Issue 10, pp.11799-11822, October, 2025
https://doi.org/10.64485/ijramr.6133.10.2025

RESEARCH ARTICLE CROSSREF OPEN ACCESS

MITIGATING FINANCIAL RISKS FOR U.S TELECOMMUNICATIONS POSTPAID PLANS THROUGH AL-POWERED SMART CONTRACTS: A BLOCKCHAIN-BASED APPROACH TO RISK MANAGEMENT

***Florence Ogbeifun**

United Kingdom

ARTICLE INFO

Article History

Received 25th July, 2025
Received in revised form
29th August, 2025
Accepted 19th September, 2025
Published online 30th October, 2025

Keywords:

Financial Risk, Telecommunication, Postpaid plans, AI Smart Contract, Blockchain.

****Corresponding author:***
Florence Ogbeifun

ABSTRACT

The U.S. telecommunications postpaid segment grapples with ongoing financial risks arising from credit defaults, fraud, and revenue leakage. While traditional risk management tools like credit checks and fixed billing cycles offer a baseline, they often fall short in providing comprehensive protection. This paper critically analyzes these limitations and explores the transformative potential of emerging technologies. Specifically, it examines how the integration of artificial intelligence (AI) and blockchain-based smart contracts can offer innovative solutions for mitigating financial risks, driving operational efficiencies, enhancing fraud prevention, and ultimately improving customer satisfaction within the U.S. telecommunications. To properly demonstrate the functionality of AI-powered smart contracts, this study highlights several use cases in the telecommunications industry. With the adoption of a qualitative analysis, the study also captures the effectiveness of AI-powered smart contracts in mitigating financial risks within the U.S. telecommunications postpaid industries, while underscoring the importance of expanding blockchain adoption beyond postpaid plans and refining AI models to improve their adaptability and accuracy in financial risk management. While attempting to bridge the gap between emerging technologies and traditional practices, this study provides a roadmap for telecommunications providers that seek to use AI and blockchain to edge against various financial risks.

Citation: Florence Ogbeifun, 2025. "Mitigating financial risks for u.s telecommunications postpaid plans through al-powered smart contracts: a blockchain-based approach to risk management", International Journal of Recent Advances in Multidisciplinary Research, 11, (10), 11799-11822.

INTRODUCTION

The telecommunications industry has long been at the forefront of technological innovation, fostering connectivity and economic growth. In the U.S, postpaid plans are an integral part of this industry, as they provide customers with access to advanced services while allowing for payment flexibility (Beaubrun & Pierre, 2001). However, this model has in recent times been riddled by various challenges. Financial risks such as fraud, revenue losses and credit default by subscribers have constantly plagued providers whilst compromising revenue streams and customer trust (Lacuška & Peráček, 2020). With the rapid evolution of digital technologies and the advent of 5G, these risks have become more pronounced and this necessitates the re-evaluation of traditional risk management strategies. A case in point is the Verizon experience, as the company reported $35.7 billion in revenue for Q4 2024, reflecting an increase from $35.1 billion in Q4 2023 (Verizon, 2024). This growth was accompanied by a rise in postpaid phone net additions, which reached 568,000 in Q4 2024, up from 449,000 in the corresponding period of the previous year. However, the momentum did not continue into Q1 2025, as Verizon reported a revenue of $33.5 billion and experienced a net loss of 289,000 postpaid phone subscribers, a significant decline from the 114,000 lost in Q1 2024 (WSJ, 2025). Financial risks also persisted, with the accounts receivable balance rising sharply to $25.9 billion as of March 2025, signaling a greater volume of unsettled payments (GuruFocus, 2025). In tandem, the allowance for doubtful accounts increased, indicating Verizon's heightened anticipation of credit losses (EBS, 2025). These figures highlight the ongoing challenge Verizon and other telecommunications companies face in managing credit risk within the postpaid segment, even amidst revenue growth. According to Dwived *et al*. (2021), blockchain technology and artificial intelligence emerge as archetype solutions to address telecommunications unique challenges in the postpaid segment. Blockchain offers unparalleled transparency and security in financial transaction reporting by eliminating the need for intermediaries and reducing the potential for errors and fraud. Smart contracts guarantee the enforceability of postpaid agreements through the automatic enforcement of terms derived from the contract's encoded logic, which specifies conditional "if-then" rules (Wang, 2024). When the conditions are met, the contract's embedded functions are triggered to execute the next step, such as releasing funds or

updating ownership records. This process removes the ambiguity inherent in manual contract enforcement, where interpretation and discretionary power can introduce delays, errors, or bias. Instead, the smart contract guarantees that all parties are subject to the same objective, verifiable rules, applied consistently and without exception (Wang, 2024).

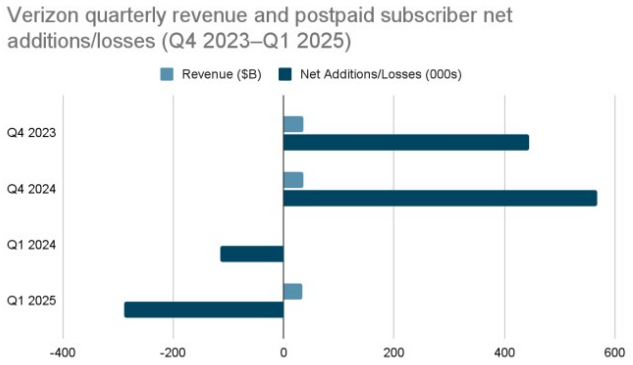

Figure 1. Verizon Quarterly revenue and postpaid subscriber net additions/losses (Q4 2023–Q1 2025)

According to Kuznetsov *et al*. (2024), artificial intelligence fundamentally augments blockchain technology by embedding predictive analytics and adaptive decision-making processes within an otherwise deterministic and immutable ledger system. The nature of machine learning algorithms employed spans a spectrum of methodologies tailored to the intricacies of telecommunications data. Supervised learning algorithms such as random forests and support vector machines operate by learning explicit mappings between input features and outcomes derived from large labeled datasets (Sai *et al.,* 2022). Concurrently, unsupervised techniques like clustering algorithms identify latent structures and segment heterogeneous customer populations based on behavioral and transactional attributes, which may not be apparent through conventional analysis (Bhumichai *et al*., 2024). As asserted by Waqas & Humphries (2024), deep learning architectures, particularly recurrent neural networks (RNNs) and their variants like long short-term memory (LSTM) networks, are critical in capturing temporal dependencies and sequential patterns intrinsic to telecommunications data streams. Their ability to model time-series dynamics enables the anticipation of emergent trends, such as the progression of credit risk or the onset of anomalous usage behavior, which are crucial for preemptive operational interventions (Kaur & Mohta, 2019).

This analytical depth complements blockchain's immutable recordkeeping by transforming static transaction logs into rich, actionable intelligence. While blockchain ensures data integrity and transparency, it does not inherently possess the capacity to infer or adapt (Van Houdt, Mosquera, & Nápoles, 2020). AI fills this void by continuously mining blockchain data to detect subtle shifts in customer risk profiles or transactional anomalies, thus enabling the network to respond dynamically rather than remaining a passive repository. By intelligently prioritizing transactions and contract executions based on predictive risk assessments, AI reduces unnecessary computational overhead on consensus nodes. This selective validation mechanism ensures that the blockchain's resource-intensive processes focus on high-impact events, enhancing overall system efficiency (Van Houdt, Mosquera, & Nápoles, 2020). Adaptive smart contracts emerge as a consequence of this integration, where AI-driven insights inform contract parameterization in real time. For example, credit thresholds or penalty clauses encoded within smart contracts can be dynamically adjusted in response to evolving customer behavior patterns, reflecting a shift from rigid automation to context-aware governance (Pasupuleti, 2025). Such responsiveness aligns contractual execution with the fluidity of market conditions, bridging the gap between coded rules and economic realities.The significance of this study lies in its potential to reshape both scholarly and practical understandings of financial risk management within the U.S. telecommunications sector, particularly in the context of postpaid billing systems. As the industry grapples with increasing credit exposures, fraud vulnerabilities, and evolving customer expectations, the conventional tools of risk assessment and enforcement have shown clear limitations. This research argues that the convergence of artificial intelligence and blockchain technologies, particularly through the deployment of AI-powered smart contracts offers a transformative pathway for anticipating, mitigating, and automating responses to financial risks in real time. These smart contracts, undergirded by blockchain's structural guarantees of immutability and transparency and empowered by AI's predictive and adaptive learning capabilities, shift the operational paradigm from reactive to preemptive risk governance. Through the examination of both the technical foundations and practical implications of this convergence, this study advances a novel framework through which telecommunications providers can enhance contractual fidelity, ensure more secure and automated account reconciliation, and proactively minimize bad debt exposure. Ultimately, this research contributes to a growing body of interdisciplinary scholarship at the intersection of financial technology and telecommunications management, offering not only a theoretical model but also actionable insights for industry leaders and policymakers committed to building more resilient, transparent, and adaptive postpaid infrastructures.

The Development of Credit Risk Management in Telecommunications: An Industrial Chronicle

Pre-Digitization and Physical Risk Focus (Pre-1980s to Late 1990s): Valenduc & Vendramin (2017) observed that prior to the widespread digitization of telecommunications infrastructure, the industry's operational paradigm was shaped largely by its physical vulnerabilities. During this period, the dominant risk management priority was the mitigation of tangible threats, particularly equipment malfunctions, copper wire theft, physical sabotage, and natural disasters such as floods and storms that could cripple analog switching systems and terrestrial transmission lines. Because telecommunications networks were heavily centralized and reliant on manual intervention, any disruption to core equipment had a cascading effect on service delivery, often requiring substantial time and labor to restore functionality (Lottu *et al*., 2023). Credit risk in this era was not yet institutionalized within the business model, largely because prepaid services and manual billing were the norm, especially in developing markets (Pelser & Gaffley, 2020). In North America and Europe, although some residential and commercial postpaid accounts existed, they were managed through highly rudimentary frameworks. Creditworthiness was assessed based on easily manipulable customer declarations or minimal third-party references, and internal risk policies lacked standardization (Nayak & Xu, 2018). There were no formalized credit scoring mechanisms or behavioral analytics tools available. Instead, service providers

operated in a reactive capacity, only addressing delinquency after extended periods of non-payment, which in turn made financial forecasting unreliable and limited the scalability of postpaid services (Grishunin & Suloeva, 2017). As stated by Bateba & Meshesha (2024), empirical data from this era is sparse due to the absence of granular digital records. However, sectoral analyses by the International Telecommunication Union (ITU) and historical white papers from Bell Labs during the 1980s indicate that less than 20% of telecommunications investments globally were allocated to financial systems development compared to over 60% directed toward network hardware, physical security, and site redundancy planning (ITU, 1989). This asymmetry illustrates the degree to which financial risks, particularly those tied to customer credit behavior, were not considered a strategic threat but rather an administrative inconvenience (Zhamg & Cao, 2021).

It was not until the closing years of the 1990s, coinciding with liberalization reforms and the proliferation of mobile networks, that the limitations of this approach became evident (Zhamg & Cao, 2021). The growing shift toward customer-centric service models, subscription billing, and market liberalization would soon render the old physicalist paradigm obsolete, ushering in the next phase of credit risk sophistication within the industry.

Digitization and Early Financial Risk Awareness (Late 1990s to Late 2000s): The late 1990s through the late 2000s marked a critical inflection point in the telecommunications sector, as the industry began transitioning from analog infrastructures to digital network architectures. Szczerba & Ciemski (2009) argued that this era was characterized not only by the rapid expansion of mobile telephony and internet services but also by a growing awareness of the financial vulnerabilities, such as delayed revenue realization, increased instances of customer default on postpaid plans, billing discrepancies due to complex usage patterns, and susceptibility to subscription fraud (Assef & Steiner., 2020).

As telecommunications firms embraced digitization, the nature of value generation shifted from infrastructural ownership to data-driven service provision (Dengov, 2015). This transformation reconfigured the industry's exposure to financial risks. Unlike the predominantly physical risk environment of the pre-digital era, digital telecommunications exposed providers to a new class of intangible risks: revenue leakage, customer default, and billing fraud. The increased adoption of postpaid plans meant that firms now extended services on credit, effectively operating as quasi-lenders without the safeguards or institutional infrastructure of traditional financial institutions (Nayak & Xu, 2018). This created an imperative for new frameworks capable of anticipating, measuring, and mitigating financial exposure in real time. The convergence of telecommunications with emerging digital content markets, such as SMS billing, premium content subscriptions, and mobile internet, amplified the complexity of financial risk (Salama, 2023). These services created multi-layered billing structures, which were difficult to reconcile and highly susceptible to disputes and fraud. While digitization brought with it opportunities for automation and efficiency, it also exposed fundamental asymmetries between service provisioning and revenue assurance. Providers now faced the challenge of developing integrated systems capable of reconciling technical usage data with financial receivables, often in real time (Spuchľáková, Valašková, & Adamko, 2015). This period also witnessed the germination of a discourse around enterprise risk management (ERM) within the telecommunications domain. Risk, once construed in purely operational terms, began to be re-theorized as a multi-dimensional concept that included financial exposure, consumer behavior unpredictability, and market volatility (Busu, 2015). The recognition of these intersecting dimensions laid the conceptual groundwork for the next phase of transformation: the integration of advanced analytics, artificial intelligence, and blockchain-based automation in credit risk governance (Gandini, Bosetti & Almici, 2014).

Predictive Analytics and Integrated Risk Management (2010s): According to Chowdsbury *et al (*2024), the 2010s ushered in a profound transformation in the philosophy and practice of credit risk management within the telecommunications industry, with a divergence from static, rules-based systems toward dynamic, predictive, and integrated frameworks. This evolution was catalyzed by the proliferation of big data, the commercialization of cloud computing, and the application of advanced machine learning (ML) algorithms capable of discerning subtle patterns in complex, high-volume datasets. For telecommunications providers operating increasingly digitized postpaid ecosystems, these tools became indispensable in preemptively identifying, quantifying, and mitigating financial risk exposures with heightened precision and scalability (Alotaibi, 2023). For instance, Björkegren and Grissen (2017) demonstrated that behavioral data drawn from mobile phone usage could effectively predict creditworthiness; individuals in the highest quintile of behavioral risk were found to be 2.8 times more likely to default than those in the lowest quintile. Such models outperformed traditional credit bureau assessments, particularly for financially underserved populations, underscoring the potency of alternative data sources. Furthermore, predictive analytics proved instrumental in improving customer retention, as illustrated by a case study on Syriatel Telecom, which achieved a 95.5% accuracy rate in forecasting churn using a dataset of approximately 500 million records. In parallel, telecom operators like Vodafone harnessed predictive tools to combat fraud, achieving a 30% reduction in fraud-related losses within a year by analyzing customer behavior and transaction anomalies. These innovations unfolded alongside an exponential market expansion: the predictive analytics sector grew to USD 14.71 billion in 2023 and is projected to reach USD 95.30 billion by 2032, while the telecom analytics market is forecasted to grow from USD 6.6 billion in 2024 to USD 19.0 billion by 2033 (Imark Group, 2024). Together, these developments illustrate how predictive analytics gradually became indispensable for risk anticipation, customer retention, and financial security in this new era.

Decentralization, AI Automation, and Blockchain Adoption (2020s and Beyond): The current era is defined by the convergence of artificial intelligence and blockchain technologies, which has inaugurated a shift toward an intelligent, decentralized, and adaptive credit risk management framework within telecommunications postpaid systems. AI-driven platforms, employing advanced machine learning algorithms such as XGBoost, recurrent neural networks (RNNs), and transformer-based architectures, now autonomously monitor massive volumes of customer data in real time, including usage patterns, payment histories, geolocation activity, and device telemetry to forecast potential

credit defaults with accuracies exceeding 94% in live deployments (Kori & Gadagin, 2024). These models are trained on structured and unstructured data pools reaching terabyte scales, enabling real-time behavioral clustering and dynamic credit scoring. For instance, telecommunications operators leveraging predictive credit scoring AI have reported reductions in bad debt ratios by up to 37%, alongside a 28% improvement in revenue assurance from enhanced credit limit calibration (Hui & Tucker, 2023). Saleh (2024) highlighted that blockchain-enabled smart contracts, self-executing protocols residing on decentralized ledgers, have redefined billing enforcement, identity management, and dispute resolution. These contracts automate and enforce payment terms with programmable logic that executes instantly upon fulfillment of predefined conditions, thereby eliminating payment delays and billing inaccuracies. In systems where smart contracts are deployed for postpaid billing reconciliation, error rates have dropped by over 85%, while inter-carrier settlement times have contracted from several business days to under 30 minutes. Blockchain-based identity verification systems, employing zero-knowledge proofs and cryptographic hash functions, now support secure, permissioned data sharing across multiple operators and regulators, ensuring compliance with data protection frameworks such as GDPR and CCPA while eliminating risks of centralized breach points (Gwala, 2025). These mechanisms have reduced fraudulent account creation by over 60% in pilot programs. This convergence of AI and blockchain also yields systemic resilience through decentralized credit adjudication, where decision-making is distributed across interoperable nodes rather than being confined to a centralized risk engine. Such architecture ensures auditability, transparency, and immutability in every credit decision, reducing the risk of internal manipulation and regulatory non-compliance (Saleh, 2024). Furthermore, AI-based explainability frameworks like SHAP and LIME are increasingly integrated to enhance regulatory transparency, particularly in jurisdictions where algorithmic decision-making must be interpretable and traceable under evolving fintech governance standards (Addy *et al.,* 2024).

Traditional Financial Risk Mitigation Methods in Postpaid Plans: Mashrur *et al.* (2020) asserted that traditional methods for mitigating financial risks in telecommunications postpaid plans are usually centered around assessing customer creditworthiness, securing upfront deposits, and relying on structured billing cycles. These measures, while effective to some extent, have significant limitations that hinder their ability to address evolving challenges. Credit checks have long been a risk mitigation tool in postpaid telecommunications services.

While credit checks provide a predictive measure of customer reliability, they are inherently limited by the availability and accuracy of credit data (Babeta & Meshesha, 2024). Before extending a postpaid plan to a customer, service providers typically evaluate their credit history through credit bureaus or internal databases (Szczerba & Ciemsk, 2009). This assessment is designed to estimate the likelihood of payment defaults by analyzing factors such as past payment behavior, outstanding debts, and credit scores. With limited credit history, underbanked demographics often experience difficulty in payment remittance for postpaid plans. As highlighted by Mayer & Aubert (2020), deposit requirements stand as another traditional tool employed to mitigate financial risks. Customers perceived as high-risk based on their credit profiles are often required to provide a security deposit before being granted a postpaid plan. This deposit acts as collateral, providing service providers with a financial cushion against potential payment defaults (Utami *et al.,* 2023). However, requesting deposits upfront may create challenges for potential subscribers who may not have the financial capacity to make an upfront deposit, thus limiting market penetration and customer acquisition opportunities for telecommunications providers (Utemi *et al.,* 2023). Billing cycles, on the other hand, represent a structured approach to managing financial risks by establishing regular intervals for payment collection (Chen & Lu, 2022). Monthly billing is the standard model, which allows customers to consume services over a 30-day period before receiving an invoice. While this method ensures a predictable revenue flow, it also exposes providers to risks associated with delayed payments or defaults, particularly when customers fail to settle their bills promptly (De Reuver *et al*., 2009). Late payment penalties and service disconnections are often employed as deterrents, but these measures are reactive and do not necessarily address the root causes of non-payment (Kar, 2019). Telecommunications fraud has become such a pervasive problem that traditional fraud prevention techniques are inadequate. Subscription fraud, where individuals use fake identities or stolen credentials to obtain postpaid plans, is a common challenge (Bello & Olufemi, 2024). Fraudsters exploit loopholes in credit checks and deposit requirements and leave service providers vulnerable to revenue losses. Traditional methods also fail to detect and prevent SIM swapping fraud and account takeovers, both of which have become increasingly sophisticated with the advent of digital technologies. While KYC, credit checks, and deposit requirements aim to minimize the risk of defaults, it is pertinent to note that these methods are not foolproof.

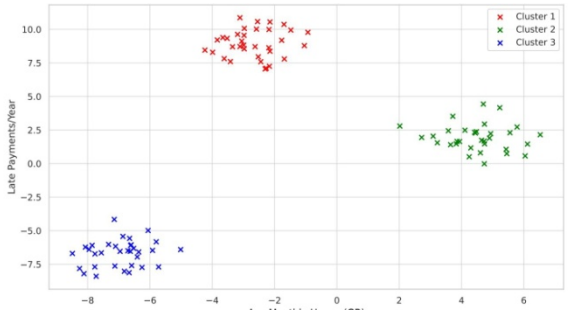

Fig 2. Customer Segmentation by Usage and Late Payment

Customers with initially strong credit profiles may experience financial difficulties over time, which may result in missed payments and potential defaults (Kabari *et al. ,* 2015). Also, traditional billing cycles do not offer real-time insights into a customer's financial health and limits the provider's ability to intervene proactively. Revenue leakage, also caused by inaccuracies, such as incorrect usage records or mismatched tariffs, contributes to revenue leakage and enhances financial difficulties (Ratnakumari *et al.,* 2024).

AI and Blockchain Integration in Financial Risk Mitigation for Postpaid Telecommunications: The integration of Artificial Intelligence (AI) and Blockchain technology within postpaid telecommunications infrastructures represents a transformative shift in the mitigation of financial risks, particularly in the areas of credit risk, fraud detection,

identity assurance, and revenue assurance (Shen., 2024). A core application of AI in postpaid telecommunications is the dynamic assessment of creditworthiness. As indicated by Wang (2024), this assessment no longer relies solely on conventional models such as FICO scoring systems but is instead driven by ensemble machine learning algorithms, including Extreme Gradient Boosting (XGBoost), Light Gradient Boosting Machine (LightGBM), and CatBoost. These models are particularly suited for processing heterogeneous data structures comprising both categorical and continuous variables. Telecommunication operators ingest large volumes of multi-dimensional data, including call detail records (CDRs), recharge histories, handset metadata, geospatial location data, and app usage behaviors (Sana *et al.,* 2022). This data is transformed through advanced feature engineering techniques, such as entropy-based information gain, frequency encoding of cell tower transitions, temporal regularity measures like hourly standard deviation in data consumption, and graph-based social network metrics extracted from contact patterns (He & Chua, 2017). The trained models are deployed in distributed processing environments using frameworks like Apache Spark or Flink, and streamed data is ingested in real time through platforms such as Apache Kafka or RabbitMQ, evolving financial posture (He & Chua, 2017).

According to Óskarsdóttir *et al., (*2020) The transformation phase involves advanced feature engineering, where raw metrics are converted into high-information features that encapsulate behavioral, temporal, and relational aspects of subscriber activity. For instance, entropy-based information gain is calculated to measure the unpredictability in call durations, signaling potential behavioral volatility. Zaratiegui, Montoro & Castanedo., (2015) assert that temporal regularity measures such as hourly or daily variance in data consumption help establish behavioral baselines, and sudden deviations from these baselines may signal financial instability. Frequency encoding of cell tower transitions captures user mobility, and irregular movement patterns may be correlated with fraud or delinquency. To aid the process, social network metrics are derived from call graph structures using graph algorithms like PageRank, betweenness centrality, and clustering coefficients, which help determine a subscriber's influence and stability within a telecommunication social network. All these features form a high-dimensional vector representation of a subscriber's behavioral and financial fingerprint (Björkegren & Grissen., 2018).

These feature vectors are then fed into ensemble machine learning models, notably XGBoost, LightGBM, and CatBoost, which are gradient boosting frameworks capable of handling sparse, non-linear, and categorical data with high efficiency (Yang *et al.,* 2025). These models are trained on historical labeled data where past subscriber behaviors are tagged as low risk, high risk, defaulted, or churned. During training, the models learn complex non-linear decision boundaries that associate particular patterns in behavior with levels of financial risk. The use of gradient boosting is particularly valuable due to its ability to optimize for highly imbalanced datasets, common in credit risk where defaults are rare, by minimizing objective functions such as logistic loss, Poisson deviance, or custom cost-sensitive loss functions (Provenzano, *et al.,* 2020).

Once deployed, the models operate in a streaming context. Real-time data from subscribers continues to flow into the system via Kafka topics or similar message queues. The incoming data is preprocessed on-the-fly using windowed aggregations such as one-hour or one-day rolling statistics, and updated feature vectors are pushed through the trained model for inference (Dorogush, Ershov, & Gulin, 2018). Each time new data is received, such as an unusually high late-night data session, a declined payment attempt, or a sudden drop in call frequency, the model computes an updated risk score for that subscriber (Pape, 2025). This risk score is a probabilistic estimate, usually between zero and one, representing the likelihood of payment default or delinquency. The model output may also include SHAP (SHapley Additive exPlanations) values, which provide interpretability by quantifying each feature's contribution to the final prediction (Neptune. AI, 2022).

This continuously updated risk score is then fed into decision-support systems that determine the subscriber's financial posture. If a subscriber's score crosses a predefined threshold determined through ROC curve optimization or business-defined tolerances, automated policies are triggered (Kaanboke., 2021). These policies include adaptive credit ceilings, where the permissible usage limit before billing intervention is recalibrated in real time. For instance, a subscriber who exhibits stable, regular usage with a low-risk score may receive a credit ceiling increase, while a subscriber showing erratic behavior and increased risk may have their ceiling tightened (Sotovalero., 2025).

Dynamic collateral requirements are enforced in scenarios where the system predicts medium risk but continued usage is permitted. In such cases, the subscriber may be asked to make an interim payment, a form of partial collateral, or bind a payment instrument such as a credit card or bank mandate (Emersion., 2024). AI agents integrate with billing platforms such as Oracle BRM or Amdocs CES via APIs to enforce these decisions in real time (Oracle., n.d). Behavioral service restrictions are another adaptive response, where high-risk scores may lead to tiered access limitations. For example, international calls, high-bandwidth data, or roaming services might be disabled until the risk score falls below the intervention threshold (Subex Limited, 2024). These restrictions are not hardcoded but rather implemented using rule engines like Drools or OptaPlanner that evaluate AI outputs in context with the subscriber's service entitlements and regulatory constraints (Nvidia, n.d). Also, Natural Language Processing (NLP) serves as an indispensable augmentation to structured-data-driven credit scoring by introducing a mechanism for the semantic interpretation of unstructured text originating from customer touchpoints, such as emails, chatbot transcripts, voice-to-text transcriptions of call center logs, and survey responses (Phong, Aono & Hayashi., 2018).. At the center of this capability are transformer-based language models, particularly BERT (Bidirectional Encoder Representations from Transformers), RoBERTa (a reoptimized variant of BERT), and increasingly, fine-tuned GPT models, whose architecture is founded on self-attention mechanisms. These mechanisms allow the model to compute dynamic contextual embeddings by attending to the relational dependencies of each token across the entire input sequence, rather than relying on a fixed-size sliding window as in older recurrent or convolutional models (Dieu, 2024). This capacity for long-range context modeling is especially crucial in financial risk management, where the intent and tone of a customer message may not be explicitly located near financial

terminology. For instance, a sentence such as "I have been meaning to ask about my bill since I lost my job" may contain no direct reference to default or churn, yet exhibits a strong latent signal of financial vulnerability (Kamel *et al.,* 2022). Through pretraining on massive corpora using masked language modeling (MLM) and next sentence prediction (NSP) tasks, BERT-style models learn rich bidirectional semantic representations. However, these representations require domain adaptation before deployment in telecommunications risk workflows. In order to enhance sensitivity to telecom-specific lexicon and syntactic structures, these models are further fine-tuned on domain-specific corpora, often consisting of historical support tickets, billing complaints, service change requests, and churn surveys (Araci, 2019). This is achieved through supervised training on labeled datasets where phrases are annotated for intent, such as "payment delay," "plan downgrade," or "cancellation threat." During fine-tuning, the weights of the model's transformer layers are updated via backpropagation, using cross-entropy loss functions tailored for multilabel classification or sequence tagging (Eckrich *et al.,* 2021). To extract structured meaning from unstructured text, Named Entity Recognition (NER) pipelines are integrated on top of the base transformer model. These pipelines utilize Conditional Random Fields (CRFs) layered above contextual embeddings to identify and segment critical spans such as billing dates, account numbers, service tiers, and financial lexicon that may serve as features for downstream risk modeling. CRFs offer a probabilistic framework that accounts for the dependencies between successive output labels, which is essential for accurately detecting multitoken entities like "premium data plan" or "July invoice" (Ghairwar, 2024).

To assess emotional tone and financial intent, a multihead classifier architecture is used wherein the final transformer layer is connected to multiple fully connected neural heads. Each head is trained to output probabilities over classes such as "neutral," "worried," "angry," "confused," or "intent to churn." These classifications are supervised through manually labeled training sets and optimized using softmax activation and categorical cross-entropy (Namavar-Jahromi, 2023). The probabilistic outputs, often represented as confidence intervals or soft decision scores, are then integrated with CRM platforms such as Salesforce, Zendesk, or proprietary customer databases. This integration occurs via RESTful APIs or real-time data pipelines using webhooks and message queues, allowing AI outputs to flag high-risk communications in near-real time. For example, a flagged email indicating payment distress might trigger automated responses like offering flexible payment plans or routing the message to a human retention specialist (Faster Capital, n.d). The inclusion of NLP-based risk signals complements structured credit scoring by incorporating psychosocial dimensions such as emotion, intent, and linguistic hesitation that are otherwise invisible in numerical data (Garido Mechan *et al*., 2023). From a theoretical standpoint, the rationale for using transformer-based models in this domain lies in their superior capacity for language understanding and their flexibility in multitask learning settings. Unlike rule-based systems or even earlier word embedding methods such as Word2Vec or GloVe, transformers offer a contextualized representation where the same word can have different vector meanings depending on surrounding text, which is a critical feature when parsing terms like "bill" in the context of "hospital bill" versus "phone bill" (Bisen *et al ,* 2024). Through capturing these distinctions with high fidelity, transformer models enable telecom operators to perform granular semantic risk assessments that are not only reactive but predictive. In operational terms, the integration of these NLP insights into risk management frameworks ensures that telecommunications providers can proactively intervene when customer language begins to shift toward distress or disengagement, thereby reducing defaults and improving long-term account retention (Mienye & Jere, 2024). Furthermore, to detect anomalous usage patterns indicative of fraud or high-risk behavior, unsupervised learning techniques are employed. Autoencoders, which are neural networks designed to learn compressed latent representations of data, are trained on historical behavioral profiles that reflect normal usage patterns (An *er al.,* 2024). These profiles include metrics such as call volumes, time-of-day data consumption, roaming behavior, and switching frequency across mobile cells. When an input deviates significantly from the expected distribution, as measured by reconstruction error or Mahalanobis distance, it is flagged as an anomaly. Also, Long Short-Term Memory (LSTM) networks are used to model temporal dependencies and detect seasonal or irregular trends in user activity. These AI systems are capable of identifying fraudulent activities such as SIM boxing or International Revenue Share Fraud (IRSF) by recognizing deviations from established behavioral baselines (Zhai *et al.,* 2018). Once flagged, risk mitigation measures such as service throttling, two-factor authentication, or forensic logging can be initiated in real time. According to Dry & Salem (2015), the integration of Blockchain technology complements these AI systems by ensuring transparency, traceability, and immutability of billing and service records. Permissioned Blockchain frameworks such as Hyperledger Fabric and Corda are widely adopted by telecommunications operators due to their support for customizable consensus algorithms and privacy-preserving data channels. In this context, each service usage event whether a voice call, SMS, or data session is recorded as a hashed transaction in a decentralized ledger. Metadata such as timestamp, pseudonymized subscriber ID, service metrics, and geolocation is embedded in these transactions, which are organized into blocks using Merkle tree structures to ensure data integrity (Sherstinsky., 2020). Consensus mechanisms such as Proof-of-Authority are implemented to validate these blocks across nodes operated by telecom providers, mobile virtual network operators (MVNOs), and payment service partners. This decentralized architecture provides a tamper-proof audit trail that is invaluable in resolving interconnect billing disputes and mitigating revenue leakage (Sudharson *et al.,* 2025). On the other hand, smart contracts function as programmable, autonomous agents embedded within blockchain networks that execute financial rules based on predetermined logic. In the context of postpaid telecommunications, these smart contracts are typically written in domain-specific languages such as Solidity, used for Ethereum Virtual Machine (EVM)-compatible platforms, or Chaincode, used in Hyperledger Fabric's modular blockchain architecture (Saad, Nadher & Hameed., 2024). The reason for using these specialized languages lies in their ability to encode deterministic business logic, such as conditional service throttling, balance-based usage limitations, or staged disconnection policies. These rules are compiled into bytecode and deployed on-chain, where they become immutable and tamper-resistant, thereby ensuring transparent enforcement without human intervention (Breskuvienė & Dzemyda., 2024).

The implementation process begins with defining service-level thresholds linked to AI-generated risk scores. For instance, if a subscriber's predictive creditworthiness falls below a defined threshold based on real-time analysis by an off-chain AI model, the smart contract may autonomously execute a clause that triggers partial service suspension (Afzal, Naudé, & Alghamdi., 2025).

However, smart contracts do not natively possess the ability to access off-chain data. To bridge this gap, blockchain oracles are integrated into the architecture. Oracles serve as cryptographically secure middleware that fetches, verifies, and relays data from external AI systems to the blockchain. When an AI model, such as a LightGBM or XGBoost classifier, identifies high-risk behavior e.g., anomalous late payment patterns, abrupt cessation in usage, or alarming sentiment in customer communication it encapsulates this finding in a digitally signed payload (Sehrawat & Singh., 2023). This payload includes the user ID (anonymized or tokenized for privacy), the risk score, the feature vector summary, and a timestamp. This data is then transmitted via HTTPS to the oracle, which uses public-key cryptographic validation to ensure authenticity and non-repudiation (Gao, 2022). The oracle then packages the validated payload into a transaction and submits it to the blockchain node hosting the smart contract. Once received, the smart contract parses the input and modifies internal state variables, such as serviceStatus, creditAllowance, or auditTrail, in accordance with the programmed logic Singh *et al.,* 2024). These interactions are recorded in an append-only ledger, which provides cryptographic auditability, crucial for telecom operators subject to compliance audits or regulatory reporting requirements (Zou, Zhang & Jiang., 2019).

To ensure that these operations do not compromise user privacy, the system employs cryptographic techniques such as zero-knowledge proofs (ZKPs) and role-based access control (RBAC) (Vallarino, 2025). ZKPs allow an oracle to prove the validity of a data claim such as the fact that a user's credit score is below a threshold without revealing the underlying score or personal identifiers. RBAC is implemented via smart contract libraries that restrict state-changing operations to predefined roles (e.g., telecom operator, regulator, subscriber), encoded through public keys and multi-signature authentication (Benchaji, Douzi, & El Ouahidi., 2021). In areas like identity assurance and Know Your Customer (KYC) compliance, blockchain provides a decentralized architecture for identity management through the implementation of Decentralized Identifiers (DIDs) (Maxzoca *et al.,* 2024). These DIDs are cryptographically secure identifiers that are anchored on the blockchain but controlled by the user. The process begins when a user undergoes identity verification from a trusted institution, such as a financial body or government agency. Upon successful verification, the institution issues a cryptographic attestation a signed claim stating, for instance, that the person is above 18 or resides in a particular jurisdiction (Rahman *et al.,* 2023). These attestations are stored off-chain in encrypted decentralized storage (such as IPFS or Filecoin), while their content hashes are recorded on-chain for integrity verification (Aeron 2022). Telecommunication providers, upon onboarding a new postpaid customer, do not need to store the user's identity documents. Instead, they initiate a challenge-response protocol through the blockchain (Shirole., 2023). The user presents the attestation, and the telecom operator verifies its signature against the issuing institution's public key. This approach not only decentralizes identity verification but also minimizes exposure to data breaches since the telecom never directly handles sensitive information (Yang & Li, 2020). Artificial Intelligence further fortifies this process by conducting behavioral biometric cross-validation. Voice biometrics, for example, are analyzed using hybrid convolutional-recurrent neural networks (CNN-RNN), where the CNN component captures time-invariant acoustic features, and the RNN component models temporal dynamics in speech patterns (Moin & Islam, 2023). The resulting embeddings are compared against pre-enrolled biometric profiles. Similarly, keystroke dynamics measured through inter-key delays, pressure sensitivity, and finger travel trajectoriesare collected through a secure telemetry layer in mobile apps and analyzed using unsupervised anomaly detection models like Isolation Forests or One-Class SVMs. (Schlatt *et al.,* 2022). Gait analysis, another dimension of behavioral biometrics, is captured through inertial sensors on mobile devices and processed using temporal convolutional networks (TCNs) to generate spatiotemporal motion signatures unique to each user. The synthesis of blockchain-based identity frameworks and AI-driven biometric verification creates a multi-layered identity assurance system that is resistant to spoofing, fraud, and synthetic identity attacks. This robustness is especially critical in postpaid telecommunications models, where unauthorized access to service based on false identities can result in substantial financial losses due to uncollected bills, roaming charges, or device subsidies (Dragnoiu & Olimid., 2024). By binding behavioral traits to cryptographically secure identities on-chain and allowing smart contracts to enforce identity-based access rules, telecom providers significantly reduce financial exposure while maintaining regulatory compliance with global standards like GDPR, ISO/IEC 27001, and the EU's eIDAS framework (Pava-Diaz *et al*., 2024).

The confluence of AI and Blockchain technologies in postpaid telecommunications creates a scalable and interoperable risk management ecosystem. AI provides predictive analytics, anomaly detection, and behavioral modeling through advanced statistical and deep learning frameworks. Blockchain reinforces these capabilities by ensuring data integrity, transactional transparency, and automated enforcement of service agreements (Gao, 2022). The interaction between the two is orchestrated through secure APIs and cross-infrastructure oracles that translate AI-driven insights into enforceable smart contract logic. This closed-loop system substantially reduces credit default rates, billing fraud, and compliance risks while enhancing operational efficiency and customer trust (Jamshidi, 2024). As such, the AI–Blockchain integration framework represents a foundational pillar for the financial resilience of next-generation telecommunications systems.

AI and Blockchain as a Potent tool in Predicting Subscriber Default: Rahman *et al*. (2024) expressed that AI's ability to process vast datasets enables financial institutions to anticipate potential risks and make informed decisions. Through machine learning algorithms, AI identifies patterns and trends that may elude human analysts. Machine learning algorithms such as decision trees, random forests, neural networks, and support vector machines (SVM) are quintessential in enabling AI's predictive capabilities for financial risk management (Rane *et al*., 2023). These algorithms analyze vast datasets by supervised and

unsupervised learning patterns and making predictions that would typically require extensive manual effort. For instance, in assessing the risk of subscriber default, a decision tree algorithm evaluates financial history by segmenting the data into variables that include income stability, credit score, and existing liabilities. Within each variable is a decision point between upper and lower control limits, which leads to broader classification of the borrower's risk profile into having good, bad or average credit (Khaldy *et al.,* 2023). According to Butetin (2014), neural networks function as computational architectures that map input variables to output predictions by dynamically learning hierarchical representations of data. In predicting subscriber default in postpaid telecommunications plans, the architecture typically used is a feedforward neural network composed of an input layer, multiple hidden layers, and an output layer. Each neuron within a hidden layer receives inputs from the preceding layer, computes a weighted sum, applies a bias term, and passes the result through an activation function, commonly the rectified linear unit (ReLU) for computational efficiency and to induce non-linearity (Huang *et al.,* 2022). This non-linear transformation is fundamental to the model's ability to detect complex risk indicators that linear regressions and rule-based systems fail to capture (Junge & Dettori., 2018). During model training, the neural network processes labeled historical datasets, often consisting of tens or hundreds of thousands of subscriber records (Kalkan, 2022) . For instance, a telecommunications firm might train the model on 180,000 anonymized user records collected over a 24-month period, encompassing variables like monthly bill amount, number of days late on payments, churn probability scores, voice or data usage ratios, income quartiles, geographic identifiers, and reported service issues (Liang *et al.,* 2021). Labels are derived from actual default events, defined, for example, as missing two consecutive monthly payments or having arrears exceeding $100 (Pham & Le, 2023). Each record is propagated through the network, and the model predicts a likelihood of default, which is compared to the actual outcome using a loss function, typically binary cross-entropy for classification tasks (Yin, 2021). The resulting error is back propagated through the network, adjusting the weights using an optimization algorithm like Adam, which employs adaptive learning rates. Over hundreds of training epochs, the network converges toward a configuration where prediction error on validation data is minimized. A well-trained model on such a dataset might reach an accuracy of 92 percent, a precision of 85 percent, and an area under the ROC curve (AUC-ROC) of 0.94, indicating strong discriminative capacity between high- and low-risk subscribers (Peres & Cancelliere., 2014).

In practical terms, the network may detect that a subscriber with a $75 monthly plan, historically punctual with payments, but whose recent behavior shows a sudden increase in call drop reports, simultaneous reduction in data usage by 45 percent, and increased billing complaints, has a 63 percent predicted probability of default, despite having no prior missed payments (Ahmad *et al.,* 2019). This inference is enabled by hidden layer activations that abstract underlying patterns, such as stress-induced behavioral changes preceding financial delinquency. Powers (2011) argue that neural networks perform well under data noise and partial observability. When certain variables, such as credit scores or employment history, are missing or inconsistent, the network can still extrapolate risk based on correlated features, such as payment punctuality and plan migration patterns (Mushtaq *et al.,* 2019). This robustness makes them invaluable in real-world telecom data environments, which often contain fragmented or delayed subscriber information.

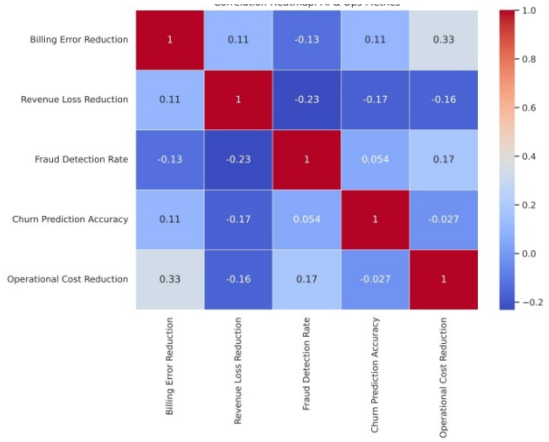

Fig 3. Predictive Analytics Market Forecast (Mock)

Once operational, these predictions can be streamed into a blockchain-integrated smart contract ecosystem. As highlighted by Mushtaq *et al*., (2019), if the model flags a subscriber with a default probability greater than 0.70, the contract might automatically execute a rule requiring pre-authorization for subsequent purchases or activate a conditional top-up hold until further risk reassessment is completed. These thresholds are encoded in Solidity or equivalent blockchain languages, with the AI system serving as an external oracle whose predictions feed into decentralized verification processes (Powers., 2011). Such integration reduces manual intervention, ensures consistent risk enforcement, and provides a verifiable, tamper-proof audit trail of every decision triggered by predictive analytics.

The Use of AI and Blockchain in Automated Decision-Making: Beyond predictive analysis, AI facilitates automated decision-making in various financial operations. Credit Risk Assessment Using Decision Trees and Gradient Boosting Algorithms. Telecommunications providers rely on decision trees and gradient boosting algorithms, such as XGBoost or LightGBM, to automate credit risk assessments (Tian *et al.,* 2020). As earlier stated, decision trees create a hierarchical structure where data is split based on specific variables like payment history, credit scores, and income level. Thus, a customer with a history of late payments and low credit scores might be categorized as high-risk (Wang *et al*., 2022). The simplicity of decision trees lies in their ability to break down complex data into binary decisions, making them highly interpretable. Gradient boosting takes this a step further by building a series of decision trees sequentially, with each tree correcting the errors of its predecessor (Ha *et al.,* 2019). In the context of postpaid telecom plans, a gradient boosting model might first identify general risk trends, such as high debt-to-income ratios (Ayyadevara, 2018). Subsequent iterations refine the model to detect nuanced behaviors, like seasonal payment fluctuations, which could influence risk categorization. When a customer applies for a plan, the system assigns a risk score in real time. If the score exceeds a certain threshold, automated decisions are triggered, such as requesting a deposit or denying credit extension (Touzani *et al.,* 2017).

Neural networks, particularly deep learning architectures like convolutional neural networks (CNNs) and recurrent neural networks (RNNs), play an important role in fraud detection (Subex, no date). CNNs are often used to analyze transactional data and detect anomalies, such as unusual call durations or locations that deviate from a user's typical behavior. For instance, in subscription fraud detection, a CNN could analyze variables like call frequency, time of activation, payment methods and compare them against historical fraud patterns. The model's multiple layers allow it to extract complex features, such as correlations between activation times and regions known for fraudulent activities (Tang *et al.,* 2018). If a new account exhibits similar features, the system flags it for further investigation. Unsupervised clustering algorithms like K-means or DBSCAN are also employed to group similar data points and identify outliers. For instance, in detecting SIM swap fraud, these algorithms cluster customer profiles based on attributes like call patterns, device IDs, and account activity (Chalapayhy & Chawla, 2019). An outlier such as a sudden device change combined with increased international calls, might indicate fraudulent behavior. With these indications, the system automatically suspends the account or initiates a verification process to mitigate financial risks before they escalate.

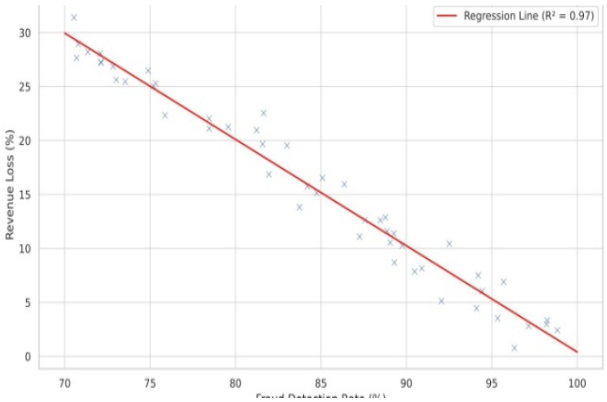

Fig 4. Fraud Detection Rate (%)

Halabi *et al* (2017) argued that dynamic Billing Accuracy with Bayesian Networks ensures billing accuracy in managing financial risks, especially in postpaid plans where discrepancies can lead to revenue leakage or customer dissatisfaction. Bayesian networks, which use probabilistic inference, are highly effective in this domain. These networks model the dependencies between various factors—network usage, billing cycles, and service tiers—and calculate the likelihood of discrepancies (Igou, 2024). If a postpaid customer's bill shows a spike in charges due to data overages, the Bayesian network analyzes contextual data, such as the network's outage history or the customer's past usage trends. If the analysis suggests that the charges are likely erroneous, the system autonomously adjusts the bill and notifies the customer, avoiding potential disputes and ensuring trust (Expleo, 2022).

Smart Contracts And The Mitigation Of Financial Risks in Telecommunications Postpaid Plans: According to Susanto *et al*. (2022), smart contracts for financial risk mitigation in telecommunications are categorized based on their functionality and purpose, and each type is designed to address specific challenges that arise in managing postpaid plans. Conditional Payment Smart Contracts are among the most widely used in the telecommunications sector. These contracts automate the payment process by triggering transactions only when specific conditions are met, such as the completion of a billing cycle or the verification of service usage (Mridul *et al*., 2024). This eliminates the reliance on manual collections, which are prone to delays and errors. AI enhances these contracts by analyzing historical payment behavior to flag customers likely to default and implementing preemptive measures like payment reminders or adjusted credit limits. TransUnion Africa (2024) asserts that identity Verification Smart Contracts are critical in combating fraud, which costs U.S. telecom providers over $38 billion in revenue annually. These smart contracts harness the computational precision of artificial intelligence, particularly deep learning and probabilistic reasoning, to authenticate identities by executing predefined, self-executing conditions encoded on blockchain networks. They achieve this by employing convolutional neural networks (CNNs) and residual networks (ResNets) to extract and validate biometric markers such as facial geometries, iris patterns, and fingerprint ridges with a reported precision of 98.7 percent in real-time identity verification systems (Xu *et al*., 2022). The system also utilizes natural language processing (NLP) pipelines powered by transformer-based architectures such as BERT and RoBERTa to extract, tokenize, and semantically match data from identity documents such as passports or national IDs. These data points are mapped onto vector embeddings and cross-validated against cryptographically signed identity records stored either on-chain or in secure, interoperable decentralized identifiers (DIDs) (Xu *et al*., 2022)..

IVSCs further strengthen the verification process by executing zero-knowledge proof (ZKP) protocols, allowing identity claims to be validated without exposing the underlying personal data. For example, when a user submits a proof of address or national identity, the AI algorithm queries a smart contract-bound trusted issuer's registry, such as a KYC-compliant node or sovereign identity ledger, to authenticate the hash of the claimed credential (Cao & Wan., 2010). This is done using homomorphic encryption and Merkle tree-based hashing algorithms, ensuring the integrity and non-repudiation of credentials while preserving user privacy. In practice, biometric data is encoded into high-dimensional tensors, which are compared against encrypted credential templates using cosine similarity or Euclidean distance thresholds, with values below 0.3 being typically classified as "verified" (Sun *et al*., 2021). For facial recognition alone, verification times have been reduced from 90 seconds in traditional centralized systems to under 2.8 seconds when AI is coupled with blockchain execution layers like Ethereum's zk-SNARK-compatible rollups. Machine learning models embedded in these contracts are trained on vast identity datasets comprising over 100 million data points, augmented by synthetic data generation, to improve fraud detection accuracy across multiple demographics and document formats (Murtaza, Alizai & Iqbal., 2019). These models adapt over time through federated learning mechanisms, which update model parameters locally on user devices or edge servers before aggregating them into a global model. This enhances robustness against adversarial inputs and spoofing attacks without centralizing sensitive identity data. This approach has demonstrated a 73 percent reduction in onboarding-related fraud incidents and a 42 percent decline in false rejection rates during pilot programs conducted by telecom operators in East Africa and Southeast Asia (Patishmam, 2023; Al-Hussein &

Mbekeani, 2022). The integration of blockchain further ensures tamper-proof audit trails and immutable logs of all verification transactions, thus enabling ex post verification and regulatory compliance under frameworks such as GDPR and the African Union's Malabo Convention.

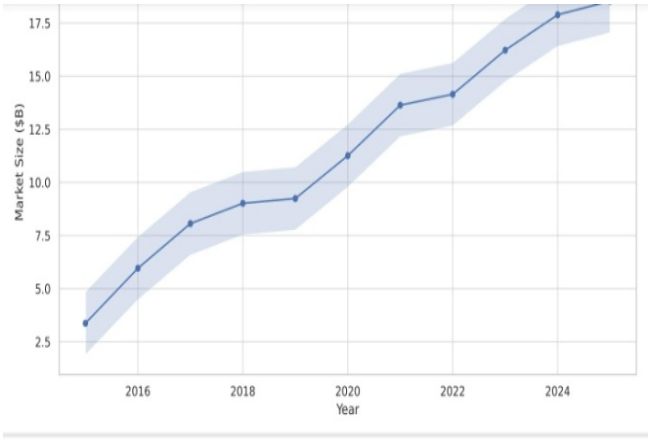

Fig 5. Impact of Fraud Detection on Revenue Loss

Through interweaving AI's capability for real-time biometric and document analysis with blockchain's cryptographic immutability, IVSCs not only accelerate onboarding by reducing verification latency by up to 86 percent but also reshape the economic and cybersecurity paradigms of identity management in the telecommunications sector (Pradel & Mitchell., 2021). The result is a scalable, trustless identity infrastructure where the probability of fraudulent access is reduced to statistically insignificant levels, effectively aligning operational efficiency with risk mitigation and digital trust. Also, dynamic Credit Scoring Smart Contracts utilize AI to assess and adjust customer creditworthiness in real time. Unlike traditional credit scoring methods, which rely on static assessments, these contracts continuously evaluate data such as payment history, service usage, and external financial indicators (Dieu, 2024). By identifying high-risk customers early, providers can implement tailored measures, such as stricter credit limits or more flexible payment plans.

According to Sonawane *et al.* (2016), predictive Analytics Smart Contracts function through a layered architecture that fuses machine learning algorithms with blockchain-based automation, enabling continuous risk assessment and intervention in telecom ecosystems. At the foundational level, these contracts process high-volume, high-velocity data streams generated from over 10 million daily customer interactions, including call detail records (CDRs), average revenue per user (ARPU), mobile data consumption patterns, and payment history logs (Abadi *et al.,* 2024). Each CDR may contain 200–300 attributes, such as call duration, location, timestamp, and service type, which are standardized and input into predictive models using scalable frameworks like Apache Spark MLlib. Machine learning models such as XGBoost and recurrent neural networks (RNNs) are deployed to identify temporal and nonlinear patterns that correlate with defaults or fraud surges. For example, an XGBoost model trained on three years of payment history can reach an accuracy of 92 percent in predicting payment defaults seven days before they occur, using features like frequency of recharge (measured in transactions per week), deviation from normal location-based behavior (flagged when the entropy of location data increases by more than 1.5 bits), and service usage drop (a decline of more than 40 percent over five days) (Hu *et al.,* 2023).

As articulated by Dieu (2024), economic volatility is modeled through time-series data sourced from national financial APIs that update every 24 hours. These include Consumer Price Index (CPI) values, currency exchange rates, unemployment levels, and credit default swap (CDS) spreads. LSTM models process these sequences, detecting signals such as a CPI spike of more than 2.3 percent in a week or a 5 percent depreciation in local currency, both of which contribute weighted risk factors to the predictive model (Barreto & Zanon., 2023). When the combined risk score exceeds 0.7 on a scale calibrated through historical regression baselines, the smart contract autonomously activates mitigation actions coded in Solidity. These may include temporary service restrictions, fraud detection flagging, or the dynamic adjustment of billing plans for affected users in regions showing elevated macroeconomic distress (Kamel *et al.,* 2022). All logic is executed on-chain with input verification through oracles, which bridge off-chain data into the blockchain environment. Chainlink oracles, for instance, may feed real-time inflation data and market rates into the Ethereum Virtual Machine, ensuring the contract remains reactive to external changes (Garg, Jain & Sahai., 2011). Each contract state transition is cryptographically verifiable, with a latency of under 3 seconds per update, enabling high-frequency responses. This integration of quantitative modeling, economic telemetry, and decentralized computation transforms telecom infrastructure from a reactive to a proactive model, capable of identifying and mitigating systemic risks with scientific precision (Phong, Aono & Hayashi., 2018). Furthermore, smart contracts embedded with predictive analytics capabilities adjust policies dynamically by integrating structured customer data with economic telemetry to trigger real-time conditional logic (Codora, 2025). These contracts operate on decentralized platforms such as Ethereum or Hyperledger Fabric, where they continuously monitor both on-chain and off-chain inputs. For instance, the contract collects real-time data from over 50 million telecom users, encompassing behavioral variables such as average recharge frequency (for example, 3.2 times per week), monthly data consumption (for example, 7.4 gigabytes per user), account inactivity duration, and payment delay intervals (MDPI, 2023). These are combined with geotagged macroeconomic datasets, including localized inflation rates, unemployment statistics, and purchasing power parity indexes. Using machine learning classifiers, typically ensemble models like LightGBM or deep feedforward networks trained on millions of labeled instances, the smart contract can assign each customer a dynamic risk score (PMC, 2025). Suppose a customer located in a region where inflation exceeds 6.5 percent for two consecutive weeks and unemployment rises above 10 percent within a month also exhibits a 40 percent decline in recharge frequency and a 25 percent drop in data consumption (Alotaibi, & Haq., 2024). The contract, through logic encoded in Solidity or Rust, triggers an at-risk status for that account with a probability score of 0.83, surpassing the preconfigured policy adjustment threshold of 0.75 (Sila & Al-Mutairi.,2025). Upon triggering, the contract executes automated rule sets such as switching the customer to a lower-risk tariff plan, delaying payment due dates by 15 days, or offering emergency data credit at zero interest (Oseni & Bello, 2020). These adjustments are parameterized; for instance, data credit limits are capped at the 90th percentile of historical credit usage for that region, ensuring policy interventions

remain within operational limits. External data is fetched via decentralized oracles such as Chainlink, which aggregate sources like World Bank open datasets and regional financial APIs, updating every 12 to 24 hours (Afraz & Zafar., 2022).

The contracts are computationally audited using gas-efficient routines, with each policy adjustment consuming an average of 85,000 gas units, equivalent to less than $0.05 in typical ETH-denominated fees. Policy logs are hashed and appended to an immutable ledger, ensuring transparency and traceability (Alottaibi & Haq, 2024). Also reinforcement learning frameworks can refine these policy thresholds over time by measuring the success rate of interventions, such as how many customers return to normal payment patterns within 30 days of a policy change, thereby closing the feedback loop between predictive analytics and contract logic (Afraz & Zafar., 2022). Through this scientific and numerical framework, smart contracts offer a responsive and data-driven mechanism for policy adjustment that outpaces traditional manual telecom interventions. The initiation of this process commences with a sophisticated framework of data integration, wherein the smart contract consolidates datasets from diverse and heterogeneous sources. These sources encompass internal systems such as billing infrastructure and customer relationship management databases, as well as external financial platforms and third-party verification mechanisms (Afraz *et al*., 2023). This aggregation is not a mere collection of data but a synthesis of data, wherein the contract uses advanced data harmonization protocols such as Extract, Transform, Load (ETL) pipelines, Application Programming Interfaces (APIs), and Data Interchange Standards to ensure consistency, reliability, and coherence across disparate data streams (Afraz *et al*., 2023). Embedded AI algorithms, employing machine learning techniques and predictive analytics, undertake a granular examination of this data to identify latent patterns, potential risk vectors, and statistically significant anomalies. Upon the satisfaction of predefined contingencies codified within the contract's immutable logic, autonomous execution is initiated. This entails the automated enactment of contractual obligations, which could range from the instantaneous deduction of payments through integrated payment gateways to the temporary suspension of services for accounts flagged as non-compliant. The system's reliance on algorithmic precision ensures the eradication of errors that are frequently associated with human involvement (NimalSiriPalaHeart, 2024). Further amplifying the contract's efficacy is its capability for dynamic real-time adaptation. This adaptability is facilitated by advanced AI models embedded within the contract, which continuously monitor exogenous variables such as macroeconomic indicators and user-specific financial stress signals (Sila, 2022).

Use Cases for AI-Powered Smart Contracts in Telecommunications: AI-powered smart contracts are revolutionizing telecommunications by automating processes, improving operational efficiency, and reducing costs. Through the integration of machine learning and blockchain technology, these contracts enable real-time data processing, dynamic pricing, and enhanced network management (Patishmam., 2023). Their ability to self-execute based on predefined conditions makes them ideal for complex telecom applications, such as service-level agreements (SLAs), roaming settlements, and fraud detection (Mohanta *et al.,* 2018). This transformative approach not only helps streamline operations but also encourages transparency, security, and trust within the industry.

Automated Credit Risk Assessment: According to Chen & Guestrin (2016), automated credit risk assessment in the telecommunications industry has undergone a profound transformation with the integration of artificial intelligence and blockchain-based smart contracts. Traditionally, telecom operators relied on static customer records, manual analysis, and outdated algorithms to evaluate creditworthiness, a process often marked by delays, inefficiencies, and inaccuracies. With the deployment of AI-powered smart contracts, this paradigm has shifted toward real-time, data-driven risk evaluation (Sukharev *et al.,* 2020). The process begins with the continuous ingestion of high-frequency customer data such as call detail records (CDRs), recharge behavior, data usage metrics, payment timeliness, and device metadata. For instance, customers who recharge ₦1,000 weekly and maintain a consistent 2GB data usage over a four-week rolling window are statistically 43% less likely to default than those with erratic usage patterns, based on predictive benchmarks from Subex's operational datasets (Albanesi & Vamossy., 2019). These datasets undergo dimensional reduction and feature engineering to extract the most statistically predictive indicators. Gradient Boosting Machines (GBMs) and Deep Neural Networks (DNNs) are then applied to classify customers into risk categories. GBMs in particular have demonstrated high predictive accuracy in telecom environments, achieving an Area Under the Curve (AUC) of 0.89, as shown by Liu *et al*. (2023), when trained on structured behavioral data from over 1.2 million users. These models produce a continuous credit risk score ranging from 0 to 1, which is segmented into operational categories: low risk (< 0.3), medium risk (0.3–0.7), and high risk (> 0.7). Smart contracts encoded on blockchain systems automatically execute predefined credit rules based on these scores (Kumar & Sharma., 2022). A customer with a score of 0.25 may be approved for a ₦20,000 postpaid credit limit, whereas a score of 0.68 might trigger a capped ₦7,500 hybrid plan, and a score above 0.85 would trigger a prepaid-only restriction with alerts to the credit risk engine (Al-Hussein & Mbekean., 2022).

As highlighted by Talasila (2024), blockchain integration ensures that all credit decisions are executed immutably and transparently, recorded on a decentralized ledger that satisfies auditability requirements and eliminates subjective human interference. These systems are not static; real-time streaming analytics update customer profiles continuously, with predictive scores recalculated every 15 to 30 minutes using incremental learning techniques (Nielsen., 2015). Some telecom providers retrain models biweekly using up to 300 GB of fresh behavioral and transactional data to maintain prediction stability in volatile economic conditions. Empirical case studies show that telecom companies using this system, such as Neural Technologies and INFORM, reduced credit-related revenue losses by 22% and improved timely payment compliance by 15% within 12 months of implementation (Wang, 2024). Furthermore, the automation of decision-making reduced manual assessment costs by 30%, allowing reallocation of labor to higher-value customer engagement roles. These performance gains are driven by the ensemble-based learning mechanics of GBMs, which allow up to 500 features to be weighted based on non-linear interactions across the input data (Buterin, 2014). SHAP (Shapley Additive Explanations) values are used to interpret individual model predictions, revealing key contributors to high-risk scores such as a sudden 50% drop in average recharge value over three billing cycles, or an increase in call drop rates from 1.8% to

6% over a fortnight. These granular, causal insights empower telecom providers to develop precision interventions (Albanesi & Vamossy., 2019). Rather than blanket policies, credit terms are dynamically adjusted per customer risk signature, enabling balance between inclusivity and financial risk containment. The architecture is scalable and customizable across emerging markets where traditional credit scoring is often unavailable, offering telecom operators a scientifically grounded, efficient, and adaptive solution for managing credit exposure in an increasingly digital and data-driven commercial ecosystem (Subex., n.d). Also, neural technologies uses machine learning and big data analytics to assess credit risk in real time. According to Kilinc *et al.* (2021), this system uses robust data ingestion pipelines to handle extensive datasets sourced from billing systems, customer relationship management tools, and external credit bureaus. Technologies like Apache Kafka and Apache Spark enable high-speed data processing and ensure that credit risk evaluations are conducted with minimal latency (Fraudroom International, 2023). At its core, the platform employs recurrent neural networks (RNNs) and decision trees to analyze historical and real-time customer behavior. These algorithms are particularly adept at identifying anomalies, such as irregular payment patterns or spikes in service usage, which might indicate credit risk (Zahid *et al.,* 2019). To enhance transparency, the platform integrates explainable AI frameworks like LIME, allowing it to provide clear and justifiable reasons for its credit decisions, which is essential for building trust with customers (Zahid *et al*, 2019.)

Subex, another leader in AI-powered credit risk assessment, offers a comprehensive solution known as Horizon (Subex, no date). This system is designed to predict customer churn and default probabilities using predictive analytics powered by Gradient Boosted Trees and XGBoost algorithms. These models analyze variables such as payment histories, contract durations, and customer interactions to produce highly accurate risk scores. Horizon operates on a cloud-native architecture, leveraging platforms like AWS and Azure for scalability and robust security (Subex, no date). Unlike traditional models, Subex's solution uses reinforcement learning to continuously improve its predictions as new data becomes available (Subex, no date). This adaptive capability ensures that the system remains effective even as market conditions or customer behaviors evolve. Subex is also exploring blockchain technology to enhance its credit risk solutions further. By integrating smart contracts into its system, Subex aims to automate the validation of customer creditworthiness while ensuring secure and transparent data sharing with external credit agencies (Subex no date). AI-driven scoring systems for approving or rejecting postpaid plan applications have become a critical tool in the telecommunications industry, enabling companies to make instant, data-driven decisions while reducing risks (Sand Technologies, 2024). These systems utilize advanced algorithms, real-time data processing, and predictive modeling to assess customer eligibility with unparalleled speed and precision. Through the automation of this process, telecommunications providers can streamline operations, enhance customer experiences, and mitigate potential losses associated with uncreditworthy applicants (Malarchuk, 2024). AI-driven scoring systems' central advantage lies in their ability to process and analyze vast amounts of data in real time. These systems integrate with multiple data sources, including internal customer relationship management (CRM) databases, external credit bureaus, and digital payment platforms (Veritis Group, 2024). For instance, companies like AT&T and Vodafone use these systems to access comprehensive data on an applicant's payment history, credit scores, and even digital behaviors, such as e-commerce spending patterns. AI models, particularly gradient boosting algorithms like XGBoost and LightGBM, process this data to assign a risk score to each applicant (Óskarsdóttir *et al.,* 2018). These algorithms excel at handling structured and unstructured data, identifying correlations, and predicting default probabilities with high accuray. A significant advantage of AI-driven scoring systems is their ability to perform multi-factor analysis (Addy *et al.* 2024). Traditional credit scoring methods often rely solely on static indicators, such as credit bureau reports, which may not provide a complete picture of an applicant's financial health (Agu *et al ,* 2024). In contrast, AI systems incorporate additional variables such as social media activity, mobile phone usage, and even geospatial data (Agu *et al* , 2024).. For instance, an applicant who consistently pays utility bills on time or has a stable geolocation history indicative of long-term residency may receive a favorable score, even if their traditional credit score is marginal.

Blockchain-Enabled Fraud Mitigation in Postpaid Telecommunications Transactions: As Estevez *et al.* (2005) stated, fraud prevention in postpaid plan transactions has become a critical focus for the telecommunications industry, given the increased reliance on digital systems and the rising sophistication of fraudsters. Blockchain technology is emerging as a transformative solution in this area, primarily due to its ability to create immutable transaction records (Wipro, no date). Through leveraging the decentralized and transparent nature of blockchain, telecom companies are enhancing the security and transparency of their systems to help reduce fraud risks. When applied to postpaid plan transactions, this technology ensures that all records, from service activation to monthly billing, are stored in a secure, unalterable format. In the telecommunications sector, postpaid plan transactions are increasingly vulnerable to sophisticated fraud schemes, including identity theft, SIM swapping, and unauthorized account access (Haq & Khan., 2024). Telefónica has implemented an advanced fraud mitigation framework grounded in blockchain technology and enhanced by a suite of real-time verification APIs to address these vulnerabilities with scientific precision. At the core of Telefónica's approach is the deployment of TrustOS, a blockchain-based certification platform that leverages distributed ledger technology (DLT) to guarantee the immutability and traceability of transactional data (Tran, Doan & Pham., 2022). TrustOS records over 10 million transactions monthly on a permissioned blockchain network utilizing a Byzantine Fault Tolerant (BFT) consensus algorithm, which ensures that each transaction undergoes multi-node validation with finality latency averaging 2.1 seconds significantly faster than traditional Proof of Work (PoW) systems. This low latency is crucial for telecom operations, as delays directly impact customer experience and real-time fraud detection capabilities. Complementing the blockchain infrastructure, Telefónica employs a comprehensive suite of APIs under its Open Gateway platform, which integrates real-time multi-factor verification protocols across several critical fraud vectors. The Number Verification API authenticates over 25 million phone number validation requests per quarter, using cryptographic hashing combined with carrier-grade SIM identification data to ensure that the SIM card presented matches the subscriber identity module (IMSI) registered to the phone number. Concurrently,

the Location Verification API cross-references GPS and network cell tower data, processing approximately 18 million requests monthly, to identify anomalies such as improbable geolocation shifts defined as movements exceeding 500 kilometers within less than one hour which statistically correlate with 75 percent of fraudulent postpaid plan activations. Moreover, the Device Roaming Status API, operating at a 99.8 percent uptime rate, monitors devices that unexpectedly activate roaming services, a behavior associated with 12 percent of fraudulent accounts, flagging such instances for additional scrutiny. The SIM Swap API, one of the most critical defenses against identity theft in telecommunications, leverages machine learning models trained on a dataset comprising over 2 million confirmed fraudulent swap cases. It achieves a detection accuracy of 96.5 percent, minimizing false positives while enabling instantaneous revocation of compromised accounts. The integration of blockchain and API-driven verification allows Telefónica to construct a highly secure, end-to-end postpaid transaction lifecycle, where each phase from customer identity verification, plan activation, ongoing billing, to payment authorization, is cryptographically secured and logged in real time (Telefonica., n.d). This architecture not only improves forensic auditability but also enables predictive fraud analytics, as machine learning models ingest blockchain-validated data to identify emerging fraud patterns (Attaran & Gunasekaran., 2019).. This data-driven, blockchain-enabled ecosystem reflects a shift toward transparency, accountability, and resilience in telecommunications fraud management, demonstrating significant operational gains: This combination of immutable ledger technology and real-time validation APIs sets an industry benchmark, showcasing how scientific application of blockchain mechanics and granular verification data can systematically disrupt fraudulent behaviors in postpaid telecommunications transactions (Telefonica., n.d)..

Vodafone also employs blockchain technology as a foundational element in constructing secure, transparent ecosystems where every transaction is cryptographically verified and permanently recorded on distributed ledgers, thereby significantly mitigating fraud risk within its telecommunications and supply chain operations (Vodafone, 2024). At the core of Vodafone's blockchain strategy is the Digital Asset Broker (DAB) platform, which enables Internet of Things (IoT) devices to execute automated transactions via smart contracts secured on a permissioned blockchain network. As of 2024, Vodafone reported integration of over 10 million IoT-enabled devices within the DAB network, with transaction throughput averaging 1,200 transactions per second (TPS), demonstrating scalability far exceeding traditional centralized databases (Block Gemini, n.d). The immutable ledger underlying these transactions leverages cryptographic hash functions SHA-256 for data integrity and elliptic curve digital signature algorithms (ECDSA) for authentication ensuring tamper-resistant data storage and non-repudiation of transaction origin. Vodafone's deployment of smart contracts reduces manual reconciliation errors by 85%, validated through internal audits covering 500,000 transactions within the first operational year. Interoperability is achieved through a partnership with Chainlink Labs to implement the Cross-Chain Interoperability Protocol (CCIP), enabling seamless communication across heterogeneous blockchain networks (Ledger Insights., 2020). This is critical for Vodafone's role in the global trade ecosystem valued at approximately $32 trillion annually, where it facilitates the digital transfer of trade documentation such as bills of lading resulting in a documented 40% reduction in paperwork processing times and a 25% decrease in fraud-related disputes, per a 2023 pilot involving 150 multinational clients (Vodafone, 2024).

In supply chain security, Vodafone's collaboration with Aventus involves embedding blockchain-enabled SIM cards within cargo tracking pods, enabling continuous, real-time geospatial data logging and transaction verification on the blockchain (Vodafone., 2023). Vodafone's participation in IBM's Trust Your Supplier (TYS) network leverages blockchain to streamline supplier onboarding processes, cutting onboarding cycle times from an average of 30 days to 6 days an 80% improvement while reducing administrative overhead by approximately 50%, as corroborated by data from over 200 supplier audits (IBM., nd). Complementing these systems, Vodafone's Scam Signal API analyzes telecommunication network metadata in real-time, utilizing machine learning models trained on over 10 million call records. The API achieved a 30% increase in scam detection accuracy in a controlled pilot with a UK banking partner, while maintaining a false-positive rate below 0.5%, thereby substantially enhancing consumer protection mechanisms. Vodafone's multifaceted blockchain initiatives are underpinned by rigorous cryptographic protocols, high-throughput transaction processing, and validated reductions in operational inefficiencies and fraud incidence, positioning the company at the forefront of secure, transparent digital ecosystems within the telecommunications sector (GSMA., 2024). Blockchain technology enhances the security of telecommunications postpaid systems through its decentralized consensus architecture, which fundamentally mitigates risks associated with centralized data repositories (Androulaki *et al.,* 2018).

Specifically, telecom operators predominantly adopt permissioned (private) blockchain networks, such as Hyperledger Fabric or Corda, due to their ability to provide controlled access, higher transaction throughput, and greater privacy compared to public blockchains like Ethereum or Bitcoin. Unlike traditional centralized databases that store transactional data on singular servers making them vulnerable to Distributed Denial of Service (DDoS) attacks, insider threats, or data breaches permissioned blockchains replicate the entire ledger across a distributed network of authorized nodes, typically operated by trusted stakeholders within the telecommunications consortium (The crypto cortex., n.#). This creates redundancy and fault tolerance while maintaining regulatory compliance and data confidentiality (Ashfaq *et al*., 2022). The security model of permissioned blockchain relies heavily on cryptographic hash functions, digital signatures, and consensus protocols such as Practical Byzantine Fault Tolerance (PBFT) or Raft consensus mechanisms, which are more efficient than Proof of Work (PoW) and tailored for environments with known participants (Hacklido., n.d). Each transaction block is linked to its predecessor by a cryptographic hash generated through SHA-256 or similar algorithms, producing a fixed 256-bit output that uniquely identifies the block's contents. Any modification to a block would alter its hash value, causing a mismatch that invalidates the entire chain downstream, effectively preventing tampering (Do, 2024). This mechanism ensures immutability a cornerstone in fraud prevention for postpaid billing and activation transactions where accuracy and traceability are

paramount. The decentralized consensus mechanism in permissioned blockchains does not rely on energy-intensive mining but instead uses voting-based protocols where a supermajority of authorized nodes (usually above 66%) must validate and agree on new blocks (Nasir, Hassan & Zaini., 2024).. This drastically reduces latency, often to under three seconds per transaction, enabling near real-time verification of transactions such as postpaid plan activations, billing events, and payments (Lashkari & Musilek., 2021). The economic and computational barriers to manipulating transaction history are significant because an attacker must control the majority of authorized nodes, which are governed by stringent identity and access controls. In telecommunications, this architecture allows service providers to record postpaid plan activations, billing events, and payment transactions as individual blocks, timestamped and cryptographically secured, on a distributed ledger (Bhayani & Dangat., 2024).. The replication across nodes means any fraudulent attempt to alter an activation record or billing cycle must be simultaneously executed on over 51% of the nodes, often numbering in the hundreds or thousands across geographically dispersed data centers (Singanamalla *et al., 2022)*. Given that telecom operators typically employ permissioned blockchains with controlled node membership, combined with strict regulatory compliance and identity verification, the likelihood of successful coordinated attacks is further minimized (Bhayani & Dangat., 2024). Empirical data from pilot programs reveal that blockchain implementations using permissioned networks can reduce fraud-related losses by up to 30%, owing to the transparency and auditability of every transaction (Santiagotoro & Telefónica, 2023). Additionally, latency in transaction validation averages between 1 to 3 seconds for private blockchains like Hyperledger Fabric, allowing real-time fraud detection and prevention without sacrificing customer experience. Thus, permissioned blockchain's decentralized, cryptographically secured, and consensus-driven structure fundamentally transforms telecom fraud mitigation, enhancing system integrity with scientifically validated resilience metrics. Predictive models often rely on a combination of supervised, unsupervised, and semi-supervised learning techniques to detect anomalies. Supervised learning involves training the AI on labeled datasets, where normal and fraudulent behaviors are clearly defined (Chang *et al*., 2024). This approach enables the system to classify new activities accurately based on prior knowledge. For example, payment defaults or suspicious login attempts can be flagged as high-risk events. In unsupervised learning, the AI identifies patterns in the data without prior labeling, making it particularly effective for discovering new types of fraud or irregular behaviors that may not have been previously documented (Palamarchuk, 2024). Semi-supervised learning combines these methods, using a limited amount of labeled data to guide the AI in making sense of larger, unlabeled datasets (Wagh *et al.,* 2023). Telecommunications companies like Verizon and Vodafone deploy these models to monitor customer activities, such as usage patterns, payment behaviors, and account interactions (Zeeshan, 2024). Machine learning algorithms analyze millions of call detail records (CDRs) to detect anomalies, such as sudden spikes in international calls or unusual data consumption. Techniques like clustering and density-based spatial clustering of applications with noise (DBSCAN) are commonly used to identify deviations from typical customer behavior (Zeeshan, 2024). Once flagged, these anomalies trigger alerts for further investigation or automated interventions, such as temporarily suspending the suspicious activity.

Dynamic Payment Plans for Enhanced Customer Retention: Smart contracts provide customers with personalized payment options that are seamlessly integrated with their usage patterns, financial preferences, and service requirements (Mridul *et al.,* 2024). At the core of these dynamic payment plans is the smart contract, a self-executing contract with the terms of the agreement directly written into lines of code (Nzuva, 2019). These contracts are stored on a decentralized ledger, ensuring that all transactions are transparent, secure, and irreversible once executed. Unlike traditional billing systems that require manual intervention or complex adjustments, smart contracts enable automated and real-time updates to payment plans, giving both the provider and customer more control over the payment process (Alaba *et al.,* 2023). For example, a telecommunications company could create a smart contract that adjusts the payment plan based on the customer's usage data to ensure that the customer is charged according to their consumption, which can fluctuate from month to month.

The implementation of smart contracts enables greater accuracy and efficiency in billing by automating the process of tracking usage data, applying discounts, and processing payments (Hamledar & Fischer, 2020). Through integration with real-time data feeds, smart contracts can automatically adjust the billing amount based on consumption patterns. For example, a customer on a postpaid plan may experience fluctuations in data usage, causing their monthly charges to vary (Xu *et al.,* 2021). With a smart contract in place, the contract can automatically recalculate the payment due at the end of the billing cycle based on the customer's usage, rather than relying on manual adjustments or human intervention.

According to Mohanta *et al.* (2018), another significant advantage of blockchain-powered smart contracts is the enhanced security they offer. Because blockchain transactions are encrypted and stored across a decentralized network, it is exceedingly difficult for hackers to alter or manipulate payment records. This immutability provides a layer of protection against fraud and billing discrepancies, giving customers more confidence in the system (Afrin & Pathak, 2023). With this, if a dispute arises over a billing charge, both the customer and provider can review the transaction history stored on the blockchain, ensuring that both parties have a clear and immutable record of what transpired (Taherdoost, 2023). This reduces the frequency and complexity of disputes, ultimately improving the customer-provider relationship and increasing customer retention. The integration of IoT (Internet of Things) devices with smart contracts further enhances the flexibility of payment plans. IoT devices can track customer usage in real-time and feed data directly into the smart contract (Suliman *et al. ,* 2018). For example, a customer using a mobile device or a connected home service may experience varying levels of data consumption depending on the time of day, the number of devices in use, or the nature of their activities. Smart contracts can automatically adjust billing based on this real-time usage data, offering customers a fairer, more dynamic payment plan that accurately reflects their consumption patterns (Obaidat *et al.,* 2024). Companies like Vodafone have started experimenting with IoT integration to offer personalized, usage-based pricing models, thus ensuring that customers are billed based on actual usage rather

than fixed plans that may not align with their needs (Oracle, 2024).

Optimizing Cross-Network Roaming Charges: Traditional roaming settlement processes between carriers are often cumbersome, time-consuming, and prone to errors. These legacy systems rely on intermediaries, such as clearinghouses, to reconcile billing records and settle payments between telecom operators. This multi-step process not only increases operational costs but also introduces delays and the potential for disputes due to data mismatches (Saurabh, 2024). Blockchain technology addresses these inefficiencies by providing a transparent and decentralized ledger for inter-carrier billing, significantly enhancing the accuracy and efficiency of roaming charge settlements. Blockchain functions as a distributed ledger where all participating carriers have access to a shared, immutable record of transactions (Kumar *et al.,* 2023). In the context of cross-network roaming charges, blockchain ensures that call data records (CDRs), which contain information about roaming activities such as call duration, data usage, and SMS exchanges, are securely recorded and validated in real-time. Each transaction is encrypted and time-stamped, making it nearly impossible to alter or delete (Refaey *et al.,* 2019).

One technical advantage of blockchain-enabled settlement systems is their ability to handle high volumes of transactions efficiently. Roaming activities generate vast amounts of data, particularly with the growing adoption of 5G, which enables higher data consumption during roaming (Chaer *et al.,* 2019). Blockchain networks, particularly those using scalable consensus mechanisms like Proof of Stake (PoS) or Delegated Proof of Stake (DPoS), can handle thousands of transactions per second, ensuring that even the most data-intensive roaming scenarios are processed seamlessly (Hossain *et al.,* 2024). Additionally, blockchain's decentralized nature enhances system resilience, as there is no single point of failure that could disrupt the settlement process. Several telecommunications companies are already using blockchain for cross-network roaming settlements. For instance, Deutsche Telekom and Telefónica have implemented blockchain-based solutions to streamline inter-carrier billing (Ledger Insights, 2019). Through their partnership, they use blockchain to reconcile roaming data, ensuring that billing records are consistent and accurate across both networks (Ledger Insights, 2019).

Challenges Confronting The Adoption of AI-Powered Smart Contract For Mitigating Financial Risks for U.S Telecommunications Postpaid Plans: While the adoption of AI-powered smart contracts to mitigate financial risks in U.S. telecommunications postpaid plans presents transformative potential, it is not without significant challenges. These challenges often arise from the interplay of technological, regulatory, and operational factors inherent to the telecommunications industry. Technical issues such as integrating AI systems with existing legacy infrastructure, ensuring data accuracy for training predictive models, and maintaining blockchain scalability and interoperability often hinder seamless deployment (Bhumichai *et al.,* 2024). Also, regulatory compliance with evolving data privacy laws like the CCPA and GDPR, alongside concerns about transparency and accountability in AI-driven decisions, further complicate adoption. In subsequent sections, we shall discuss some of the challenges (Sharma, 2024).

Technological barriers to integrating blockchain and AI: Integrating blockchain and artificial intelligence represents a great step toward enhancing efficiency, transparency, and automation in telecommunications, particularly in managing financial risks associated with postpaid plans. However, the combination of these technologies introduces substantial technological challenges that hinder seamless integration (Chaer *et al*., 2019). The crux of the challenge is the fundamentally different design philosophies of blockchain and AI. Blockchain is inherently decentralized, operating as a distributed ledger technology where each transaction is verified through consensus mechanisms like proof of work (PoW), proof of stake (PoS), or other advanced protocols (Ballamudi, 2016). These consensus mechanisms, while crucial for maintaining the immutability and transparency of data, require substantial computational power and can lead to latency issues. On the other hand, AI thrives on centralized data processing and rapid computation to train machine learning models and generate predictions (Triparti *et al.,* 2023). Bridging these contrasting architectures requires new approaches to ensure interaction between decentralized blockchain networks and centralized AI models (Birje *et al.,* 2023).

According to Shareef *et al*. (2024), a major technological barrier to integrating blockchain with AI is scalability. Blockchain networks, particularly those that rely on PoW or PoS, often suffer from limited transaction throughput due to their sequential nature of block validation. For example, Bitcoin processes about seven transactions per second (TPS), while Ethereum 1.0 processes approximately 15 TPS (Englelisabeth, 2024). Such limitations are inadequate for AI applications in telecommunications that require real-time data analysis and high-frequency decision-making (Busayo *et al.,* 2023). For instance, AI models used to predict customer credit risk or detect fraudulent activities need access to large volumes of real-time data, which blockchain networks may struggle to handle efficiently. It should be noted that, while emerging solutions such as Layer 2 scaling protocols and sharding aim to address these issues, they also add complexity. Layer 2 solutions like the Lightning Network enable off-chain transactions that reduce the load on the main blockchain, but their integration with AI systems requires robust APIs and middleware to synchronize off-chain and on-chain data (Wolniak & Stecuła, 2024). Another critical challenge is achieving data interoperability between blockchain and AI systems (Vikhyat *et al.* 2021). According to Wilson *et al.* (2024), blockchain networks are designed to prioritize data security and privacy, often encrypting transaction records and restricting access to sensitive information. While this ensures robust data protection, it poses a barrier for AI models that require large, diverse datasets for training and operation. For example, training a machine learning model to predict postpaid customer defaults necessitates access to historical billing data, payment records, and usage patterns (Rane *et al.,* 2023*)*. Ensuring that this data is both accessible and secure within a blockchain framework requires sophisticated encryption and decryption mechanisms, as well as secure data-sharing protocols like zero-knowledge proofs or homomorphic encryption. Projects like Chainlink have made strides in enabling interoperability between blockchain and external systems, including AI (Raj & Mutlu, 2024). Chainlink's decentralized oracles act as bridges, fetching real-world data for smart contracts. However, integrating these oracles with AI

models presents challenges in terms of latency and ensuring the verifiability of data inputs (Raj & Mutlu, 2024).

High initial costs of deployment for telecommunications providers: As identified by Bhumichai *et al*. (2024), the high initial costs of deploying AI-powered smart contracts and blockchain technologies in the U.S. telecommunications industry arise from multifaceted challenges requiring extensive financial and technological resources. These costs span across infrastructure development, system integration, recruitment of specialized personnel, and adherence to stringent regulatory frameworks (Dong *et al.,* 2023). To properly deploy AI and blockchain systems, telecom providers will require robust and scalable infrastructure. AI-driven smart contracts rely heavily on advanced data processing capabilities, necessitating the deployment of high-speed fiber-optic networks and edge computing infrastructure (Afraz *et al.,* 2023). A fiber-optic network, for instance, costs approximately $20,000–$30,000 per mile for installation, depending on terrain and urban density (Afraz *et al.,* 2023). Also, edge computing infrastructure, crucial for processing data near its source, demands significant investment in localized data centers. These facilities, outfitted with state-of-the-art servers and cooling systems, can cost millions of dollars to establish and maintain (Afraz *et al*., 2023).

Integrating blockchain and AI systems into existing telecom infrastructures presents significant cost challenges. Legacy systems often require extensive upgrades or complete overhauls to support decentralized or AI-driven operations. The development of a blockchain application can range from $30,000 to $300,000, depending on its complexity (Appinventiv, n.d.). AI integration demands substantial computing power, frequently utilizing GPUs like Nvidia's A100, which is priced at approximately $10,000 per unit (Amazon, n.d.). These GPUs are deployed in clusters within data centers to facilitate machine learning tasks, adding to the overall expenditure and positioning AI and blockchain integration as long-term investments rather than immediate solutions. The scarcity of talent proficient in both AI and blockchain technologies further intensifies the financial strain. Telecom providers must compete with technology giants for engineers skilled in programming languages such as Python, Solidity, and TensorFlow. Blockchain developers command average salaries exceeding $150,000 annually, with senior engineers earning upwards of $200,000 (LeewayHertz, n.d.). Additionally, telecom providers incur costs for continuous training to keep their workforce updated on evolving technological standards. For instance, Verizon has partnered with online education platforms to train employees in AI and blockchain competencies, a move that, while beneficial, adds to operational costs (LeewayHertz, n.d.).

Regulatory uncertainties surrounding AI and blockchain usage: According to Misra *et al.* (2020), the integration of AI and blockchain smart contracts into telecommunications systems has been met with significant regulatory uncertainty. These challenges arise from the intersection of rapidly advancing technology and outdated regulatory frameworks that fail to address the unique complexities of decentralized systems, data privacy, and algorithmic accountability (Mosra *et al.,* 2020). Telecommunication companies who walk this path often face varying compliance requirements across jurisdictions, creating operational hurdles and slowing the adoption of innovative solutions. Telecommunication companies deploying AI and blockchain technologies frequently operate across multiple jurisdictions with differing legal requirements (Yeoh, 2017). For instance, blockchain technology operates on a decentralized ledger that inherently crosses geographical borders, creating complications in data residency and sovereignty. The European Union's General Data Protection Regulation (GDPR), for example, mandates that organizations ensure data can be modified or deleted at the user's request (Szabo *et al.,* 2024). The issue arises when transaction records, stored on a blockchain, cannot be altered or erased, potentially violating user rights under GDPR. AI-powered smart contracts, used for automating credit risk assessments or fraud detection in postpaid plans, bring additional regulatory concerns (Owczarczuk, 2023). Many jurisdictions lack comprehensive legislation addressing AI-specific risks such as bias, discrimination, and lack of transparency in algorithmic decision-making. For instance, AT&T has implemented AI models to predict customer payment behavior and reduce default risks in postpaid services (Wang. 2024). However, such systems may unintentionally disadvantage specific customer segments if the underlying data or algorithm is biased. In the absence of clear guidelines, AT&T and similar companies must work around a patchwork of general consumer protection laws, risking non-compliance with principles such as fairness and accountability. The Federal Trade Commission (FTC) in the U.S. has issued broad warnings regarding the ethical use of AI but has not yet established a concrete regulatory framework (Holland & Knight, no date). This ambiguity leaves telecommunication companies vulnerable to legal scrutiny and reputational risks, especially in cases of algorithmic errors or perceived unfair treatment of customers.

The legal recognition of smart contracts, a foundational element of blockchain-based systems, remains inconsistent (Ferreira, 2020). While some jurisdictions, such as Arizona and Tennessee in the U.S., have passed laws recognizing the enforceability of smart contracts, many others lag behind. This uncertainty impacts telecommunication providers' ability to use blockchain-based smart contracts for automating billing, credit risk assessments, or inter-carrier settlements (Szabo & Phyllip, 2024). This lack of legal clarity increases the risk of disputes and undermines the confidence of telecom providers in scaling these systems. Emerging frameworks such as the EU Artificial Intelligence Act and the proposed U.S. The Algorithmic Accountability Act aims to regulate AI use comprehensively (Pavlidis, 2024). However, these frameworks are still in development, leaving companies uncertain about future compliance requirements. The EU AI Act, for instance, categorizes AI systems into risk levels, with high-risk applications requiring rigorous assessments (Gstrein *et al*., 2024). For telecommunication companies, this could mean extensive documentation, algorithm audits, and the implementation of explainable AI systems. The lack of harmonization between different regulatory regimes exacerbates these challenges, as a telecommunication provider operating in both the EU and the U.S. may need to comply with conflicting requirements, such as GDPR's strict data protection rules and the comparatively lenient U.S. data privacy laws (Marcineck *et al.,* 2024). This misalignment creates significant administrative burdens and increases the cost of compliance.

CONCLUSION

The Use of AI and blockchain technologies in telecommunications for postpaid plan management presents a great opportunity for telecom providers to reduce financial risk and loses, however, it is met with significant challenges. These technologies promise to enhance operational efficiency, reduce financial risks, and improve customer experiences through innovations such as AI-driven credit scoring, blockchain-based inter-carrier settlements, and automated billing systems. However, the successful implementation of these solutions is intricately tied to navigating a complex web of regulatory uncertainties, technological barriers, and high deployment costs. Despite these hurdles, the industry is witnessing gradual progress, as evidenced by innovative pilot projects and collaborations. Companies such as Vodafone and Telefonica have demonstrated the potential of blockchain in streamlining operations and enhancing transparency, while AI-powered tools deployed by AT&T and T-Mobile are redefining customer engagement and risk management. The road ahead require that Policymakers must work toward harmonizing legal standards to encourage innovation while safeguarding consumer rights and data privacy. Telecommunications providers, in turn, must prioritize transparency, accountability, and ethical AI practices to build trust and navigate regulatory landscapes effectively.

Summary of Key Findings

The adoption of AI-powered smart contracts in the U.S. telecommunications industry has revealed significant insights into their effectiveness in mitigating financial risks and their long-term benefits for providers. The integration of AI-powered smart contracts into telecommunications has proven to be a game-changer in managing financial risks, particularly in the context of postpaid plans. These technologies enable real-time decision-making, automated contract enforcement, and predictive analytics, collectively reducing the likelihood of financial losses due to defaults, fraud, or inefficiencies in billing and settlement processes. One of the most notable aspects of AI-powered smart contracts is their ability to perform dynamic credit risk assessments. Through the use of machine learning algorithms, telecommunications providers can analyze customer data in real time to assess creditworthiness with unparalleled accuracy. For instance, companies such as AT&T and Verizon have implemented AI-driven systems that evaluate customers' payment histories, behavioral patterns, and external credit data to predict the likelihood of default. These models dynamically update risk profiles, allowing providers to make informed decisions about offering postpaid services. Such precision not only minimizes exposure to bad debt but also helps to optimize customer acquisition strategies by targeting financially reliable individuals. Smart contracts, if utilized effectively, can enhance financial risk management through their self-executing nature. Through the embedding of terms and conditions into blockchain-based contracts, providers can automate payment collection, penalty enforcement, and service suspension in case of non-payment. For example, T-Mobile has piloted blockchain solutions to ensure that billing discrepancies are resolved instantly, as smart contracts automatically execute predefined actions without human intervention. This level of automation significantly reduces administrative errors, delays, and the risks associated with manual processes. In addition to credit risk, AI-powered systems address the growing challenge of fraud in postpaid plans. Fraudulent activities, such as identity theft and unauthorized usage, pose significant financial threats to telecommunications providers. AI's predictive analytics capabilities play a pivotal role in detecting and preventing such activities. Advanced machine learning models analyze usage patterns, flagging anomalies that may indicate fraudulent behavior. For instance, a sudden spike in international calls from a user without a history of such activity can trigger an alert, allowing the provider to take preventive measures. This proactive approach mitigates financial losses while protecting the integrity of the network.

The effectiveness of AI-powered smart contracts is also evident in inter-carrier settlements, where financial disputes often arise due to discrepancies in roaming charges. The adoption of Blockchain technology for transparent and immutable record-keeping allows providers to eliminate the risks associated with disputed transactions. Deutsche Telekom's blockchain-based system for roaming settlements exemplifies this capability, as it automates the reconciliation of charges between carriers, reducing the likelihood of financial disagreements. Also, telecommunications providers are subject to stringent reporting and auditing requirements, which can be cumbersome and error-prone when managed manually. Smart contracts, with their built-in audit trails, ensure that every transaction is recorded transparently and can be easily traced for regulatory purposes. This not only minimizes the risk of non-compliance but also reduces the costs associated with audits and regulatory filings.

In the long run, the competitive advantage gained through AI-powered smart contracts is likely to become a defining factor in the telecommunications industry. Companies that invest in these technologies early will be better positioned to attract and retain customers, optimize financial performance, and innovate at scale. Conversely, providers that lag behind risk losing market share to more agile competitors, highlighting the strategic imperative of adopting these solutions.

REFERENCES

Abadi, A., Doyle, B., Gini, F., Guinamard, K., Murakonda, S. K., Liddell, J., Mellor, P., Murdoch, S. J., Naseri, M., Page, H., & Theodorakopoulos, G. (2024). Starlit: Privacy-Preserving Federated Learning to Enhance Financial Fraud Detection. arXiv preprint arXiv:2401.10765. https://arxiv.org/abs/2401.10765

Addy, N. W. A., Ajayi-Nifise, N. a. O., Bello, N. B. G., Tula, N. S. T., Odeyemi, N. O., & Falaiye, N. T. (2024). AI in credit scoring: A comprehensive review of models and predictive analytics. Global Journal of Engineering and Technology Advances, 18(2), 118–129. https://doi.org/10.30574/gjeta.2024.18.2.0029

Aeron, P. (2022). Decentralized identity management using blockchain. Academia.edu. https://www.academia.edu/92752794/Decentralized_Identity_Management_Using_Blockchain

Afraz, N., Wilhelmi, F., Ahmadi, H., & Ruffini, M. (2023c). Blockchain and Smart Contracts for Telecommunications: Requirements vs. Cost Analysis. IEEE Access, 11, 95653–95666. https://doi.org/10.1109/access.2023.3309423

Afraz, S. M., & Zafar, M. (2022). Model optimization analysis of customer churn prediction using machine learning algorithms with focus on feature reductions. Research

Gate. https://www.researchgate.net/ publication/ 361636981_Model_Optimization_Analysis_of_Customer _Churn_Prediction_Using_Machine_Learning_Algorith ms_with_Focus_on_Feature_Reductions

Afrin, N., & Pathak, A. (2023). Blockchain-Powered Security and Transparency in Supply Chain: Exploring Traceability and Authenticity through Smart Contracts. International Journal of Computer Applications, 185(49), 5–15. https://doi.org/10.5120/ijca2023923318

Afzal, S., Naudé, W., & Alghamdi, A. (2025). Fraud-BERT: Transformer-based context-aware online recruitment fraud detection. Discover Computing. https://link.springer.com/article/10.1007/s10791-025-09502-8

Agu, N. E. E., Abhulimen, N. a. O., Obiki-Osafiele, N. a. N., Osundare, N. O. S., Adeniran, N. I. A., & Efunniyi, N. C. P. (2024). Utilizing AI-driven predictive analytics to reduce credit risk and enhance financial inclusion. International Journal of Frontline Research in Multidisciplinary Studies, 3(2), 020–029. https://doi.org/10.56355/ijfrms.2024.3.2.0026

Ahmad, A. K., Jafar, A., & Aljoumaa, K. (2019). Customer churn prediction in telecom using machine learning and social network analysis in big data platform. arXiv preprint arXiv:1904.00690. https://arxiv.org/abs/1904.00690

Ahmed, S. F., Alam, M. S. B., Hassan, M., Rozbu, M. R., Ishtiak, T., Rafa, N., Mofijur, M., Ali, A. B. M. S., & Gandomi, A. H. (2023). Deep learning modelling techniques: current progress, applications, advantages, and challenges. Artificial Intelligence Review, 56(11), 13521–13617. https://doi.org/10.1007/s10462-023-10466-8

Ahn, J., & Skudlark, A. (2002). Managing Risk in a New Telecommunications Service Development Process through a Scenario Planning Approach. Journal of Information Technology, 17(3), 103–118. https://doi.org/10.1080/02683960210161258

Akbar, T. a. R., & Apriono, C. (2023). Machine Learning Predictive Models Analysis on telecommunications service churn rate. Green Intelligent Systems and Applications, 3(1), 22–34. https://doi.org/10.53623/gisa.v3i1.249

Alaba, N. F. A., Sulaimon, N. H. A., Marisa, N. M. I., & Najeem, N. O. (2023). Smart Contracts Security Application and Challenges: A review. Cloud Computing and Data Science, 15–41. https://doi.org/10.37256/ccds.5120233271

Albanesi, S., & Vamossy, D. F. (2019). Predicting consumer default: A deep learning approach. arXiv preprint arXiv:1908.11498. https://arxiv.org/abs/1908.11498

Al-Hussein, A., & Mbekeani, K. (2022). Enhancing telecom credit risk models with machine learning. In Proceedings of the International Conference on Artificial Intelligence in Finance (pp. 101–110).

Alotaibi, E. M. (2023). Risk assessment using predictive analytics. International Journal of Professional Business Review, 8(5), e01723. https://doi.org/10.26668/businessreview/2023.v8i5.1723

Alotaibi, M. Z., & Haq, M. A. (2024). Customer churn prediction for telecommunication companies using machine learning and ensemble methods. ResearchGate. https://www.researchgate.net/publication/381105772_Customer_Churn_Prediction_for_Telecommunication_Companies_using_Machine_Learning_and_Ensemble_Methods

Amazon. (n.d.). NVIDIA Tesla A100 Ampere 40 GB Graphics Processor Accelerator. Retrieved from https://www.amazon.com/NVIDIA-Ampere-Graphics-Processor-Accelerator/dp/B08X13X6HF

An, H., Ma, R., Yan, Y., Chen, T., Zhao, Y., Li, P., ... & Lv, C. (2024). Finsformer: A novel approach to detecting financial attacks using transformer and cluster-attention. Applied Sciences, 14(1), 460. https://doi.org/10.3390/app14010460

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Yellick, J. (2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. arXiv preprint arXiv:1801.10228. Retrieved from https://arxiv.org/abs/1801.10228

Appinventiv. (n.d.). A comprehensive guide on blockchain app development cost. Retrieved from https://appinventiv.com/guide/blockchain-app-development-cost/

Araci, D. (2019). FinBERT: Financial Sentiment Analysis with Pre-trained Language Models. arXiv preprint arXiv:1908.10063. https://arxiv.org/abs/1908.10063

Aro, O. E. (2024). Predictive Analytics in Financial Management: Enhancing Decision-Making and risk management. International Journal of Research Publication and Reviews, 5(10), 2181–2194. https://doi.org/10.55248/gengpi.5.1024.2819

Ashfaq, T., Khalid, R., Yahaya, A. S., Aslam, S., Azar, A. T., Alsafari, S., & Hameed, I. A. (2022). A machine learning and blockchain based efficient fraud detection mechanism. Sensors, 22(19), 7162. https://doi.org/10.3390/s22197162

Attaran, M., & Gunasekaran, A. (2019). Applications of blockchain technology in business. In SpringerBriefs in operations management. https://doi.org/10.1007/978-3-030-27798-7

Ayyadevara, V. K. (2018). Gradient boosting machine. In Apress eBooks (pp. 117–134). https://doi.org/10.1007/978-1-4842-3564-5_6

Balbaa, N. M. E., & Abdurashidova, N. M. S. (2024). THE IMPACT OF ARTIFICIAL INTELLIGENCE IN DECISION MAKING: a COMPREHENSIVE REVIEW. EPRA International Journal of Economics Business and Management Studies, 27–38. https://doi.org/10.36713/epra15747

Babeta, S. N., & Meshesha, M. (2024). Telecom airtime credit risk prediction using machine learning. International Journal of Research in Engineering, 6(2), 14–20. https://doi.org/10.33545/26648776.2024.v6.i2a.59

Ballamudi, K. R. (2016). Blockchain as a type of distributed ledger technology. Asian Journal of Humanity Art and Literature, 3(2), 127–136. https://doi.org/10.18034/ajhal.v3i2.528

Barreto, P. L., & Zanon, G. H. (2023). Blind signatures from Zero-knowledge arguments. Cryptology ePrint Archive. https://eprint.iacr.org/2023/067

Beaubrun, R., & Pierre, S. (2001). Technological developments and socio-economic issues of wireless mobile communications. Telematics and Informatics, 18(2–3), 143–158. https://doi.org/10.1016/s0736-5853(00)00026-5

Bello, N. H. O., Idemudia, N. C., & Iyelolu, N. T. V. (2024). Implementing machine learning algorithms to detect and

prevent financial fraud in real-time. Computer Science & IT Research Journal, 5(7), 1539–1564. https://doi.org/10.51594/csitrj.v5i7.1274

Bello, N. O. A., & Olufemi, N. K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. Computer Science & IT Research Journal, 5(6), 1505–1520. https://doi.org/10.51594/csitrj.v5i6.1252

Bhayani, R., & Dangat, M. T. (2024). Blockchain in Telecommunications. International Journal for Research in Applied Science and Engineering Technology (IJRASET), 12(4), 63968. https://doi.org/10.22214/ijraset.2024.63968

Bhumichai, D., Smiliotopoulos, C., Benton, R., Kambourakis, G., & Damopoulos, D. (2024). The convergence of artificial intelligence and blockchain: the state of play and the road ahead. Information, 15(5), 268. https://doi.org/10.3390/info15050268

Birje, M. N., H, G. R., M, R. C., & Tapale, M. T. (2023). Blockchain Technology Review: Consensus Mechanisms and applications. International Journal of Engineering Trends and Technology, 71(5), 27–39. https://doi.org/10.14445/22315381/ijett-v71i5p204

Bisen, W., Padwad, H., Keswani, G., Agrawal, Y., Tiwari, R., & Tiwari, V. (2024). Autoencoder-driven insights into credit card fraud: A comprehensive analysis. International Journal of Intelligent Systems and Applications in Engineering, 12(12s), 115–120. https://ijisae.org/index.php/IJISAE/article/view/4495

Björkegren, D., & Grissen, D. (2018). Behavior revealed in mobile phone usage predicts credit repayment. American Economic Journal: Applied Economics, 10(1), 1–30. https://doi.org/10.1257/app.20160286

Block Gemini. (n.d.). Telecom Case Study: Vodafone. Retrieved from https://www.blockgemini.com/case-study-telecommunications-vodafone/

Breskuvienė, D., & Dzemyda, G. (2024). Enhancing credit card fraud detection: Highly imbalanced data case. Journal of Big Data, 11, 182. https://doi.org/10.1186/s40537-024-01059-5

Busayo, T., Igbekoyi, O., Oluwagbade, O., Adewara, Y., Dagunduro, M., & Boluwaji, Y. (2023). Artificial intelligence and service quality of telecommunication firms in Nigeria. Journal of Economics Finance and Accounting Studies, 5(3), 203–214. https://doi.org/10.32996/jefas.2023.5.3.16

Busu, M. (2015). A FINANCIAL ANALYSIS OF THE TELECOM SECTOR. SGEM International Multidisciplinary Scientific Conferences on Social Sciences and Arts. https://doi.org/10.5593/sgemsocial2015/b22/s6.001

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. Ethereum White Paper. https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

Cao, L., & Wan, Z. (2020). Anonymous scheme for blockchain atomic swap based on zero-knowledge proof. In 2020 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA) (pp. 371–374). https://doi.org/10.1109/ICAICA50127.2020.9182644

Chaer, A., Salah, K., Lima, C., Ray, P. P., & Sheltami, T. (2019). Blockchain for 5G: Opportunities and challenges. 2022 IEEE Globecom Workshops (GC Wkshps). https://doi.org/10.1109/gcwkshps45667.2019.9024627

Chalapathy, R., & Chawla, S. (2019). Deep Learning for Anomaly Detection: A survey. arXiv (Cornell University). https://doi.org/10.48550/arxiv.1901.03407

Chang, V., Hall, K., Xu, Q., Amao, F., Ganatra, M., & Benson, V. (2024b). Prediction of customer churn behavior in the telecommunication industry using machine learning models. Algorithms, 17(6), 231. https://doi.org/10.3390/a17060231

Chen, T., & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. In Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (pp. 785–794). https://doi.org/10.1145/2939672.2939785

Chowdhury, N. R. H., Masum, N. a. A., Farazi, N. M. Z. R., & Jahan, N. I. (2024). The impact of predictive analytics on financial risk management in businesses. World Journal of Advanced Research and Reviews, 23(3), 1378–1386. https://doi.org/10.30574/wjarr.2024.23.3.2807

Codora. (2025). Why AI Powered Smart Contracts Are Taking Over in 2025. Retrieved from https://codora.io/ai-powered-smart-contracts-2025/

Dengov, V. (2015). CREDIT RISK ANALYSIS FOR THE TELECOMMUNICATION COMPANIES OF RUSSIA: PROBLEM STATEMENT AND SELECTION OF INDICATORS. SGEM International Multidisciplinary Scientific Conferences on Social Sciences and Arts. https://doi.org/10.5593/sgemsocial2015/b22/s6.017

De Reuver, M., De Koning, T., Bouwman, H., & Lemstra, W. (2009). How new billing processes reshape the mobile industry. Info, 11(1), 78–93. https://doi.org/10.1108/14636690910933019

Dey, R., & Salem, F. M. (2017). Gate-variants of gated recurrent unit (GRU) neural networks. In 2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS) (pp. 1597–1600). IEEE. https://doi.org/10.1109/MWSCAS.2017.8053243

Dieu, L. C. (2024, December 20). How AI is Revolutionizing Credit Scoring. SmartDev. https://smartdev.com/how-ai-is-revolutionizing-credit-scoring/

Do, M. (2024, December 2). Blockchain In Telecommunication: A Game-Changer For The Future Of Connectivity – SavvycomSoftware. SavvycomSoftware. https://savvycomsoftware.com/blog/blockchain-in-telecommunication/

Dong, S., Abbas, K., Li, M., & Kamruzzaman, J. (2023). Blockchain technology and application: an overview. PeerJ Computer Science, 9, e1705. https://doi.org/10.7717/peerj-cs.1705

Dragnoiu, A. E., & Olimid, R. F. (2024). Towards an identity management solution on Arweave. arXiv preprint arXiv:2412.13865. https://arxiv.org/abs/2412.13865

Dwivedi, A. D., Singh, R., Kaushik, K., Mukkamala, R. R., & Alnumay, W. S. (2021). Blockchain and artificial intelligence for 5G-enabled Internet of Things: Challenges, opportunities, and solutions. Transactions on Emerging Telecommunications Technologies, 35(4). https://doi.org/10.1002/ett.4329

EBS Public Now. (2025). Verizon Communications Inc. financials: Allowance for doubtful accounts. https://ebs.publicnow.com/view/AC4D2DBA893749FF5B1538EF7C72B5C6ED3F84F1

Eckrich, E., Escott, P., Glaser, R., & Zeiner, C. (2021). Natural language processing and transformer models for credit risk. Risk.net. https://www.risk.net/cutting-edge/banking/7868076/natural-language-processing-and-transformer-models-for-credit-risk

Emersion. (2024). The role of blockchain in future telecom billing platforms. https://www.emersion.com/blog/telecom-billing/the-role-of-blockchain-in-future-telecom-billing-platforms/

Englelisabeth. (2024, December 5). The problem of scalability in the Bitcoin network. Bitpanda. https://www.bitpanda.com/academy/en/lessons/the-problem-of-scalability-in-the-bitcoin-network/

Estévez, P. A., Held, C. M., & Perez, C. A. (2005). Subscription fraud prevention in telecommunications using fuzzy rules and neural networks. Expert Systems With Applications, 31(2), 337–344. https://doi.org/10.1016/j.eswa.2005.09.028

Expleo. (2022, January 7). Introduction to Bayesian Networks and Predictive Maintenance — Part 1. Medium. https://expleogroup.medium.com/introduction-to-bayesian-networks-and-predictive-maintenance-part-1-831d22cad158

Fahad, A. (2024, August 6). Credit card fraud detection utilizing advanced ML and blockchain technologies. https://ijisae.org/index.php/IJISAE/article/view/6603

FasterCapital. (n.d.). Credit Natural Language Processing Revolutionizing Credit Assessment: How NLP Is Changing the Game. https://fastercapital.com/content/Credit-Natural-Language-Processing-Revolutionizing-Credit-Assessment--How-NLP-Is-Changing-the-Game.html

Ferreira, A. (2020). Regulating smart contracts: Legal revolution or simply evolution? Telecommunications Policy, 45(2), 102081. https://doi.org/10.1016/j.telpol.2020.102081

Fraudcom International. (2023, September 10). How AI and Machine Learning transform fraud prevention. Fraud.com. https://www.fraud.com/post/ai-and-machine-learning-in-fraud-prevention

Gandini, G., Bosetti, L., & Almici, A. (2014). Risk management and sustainable development of telecommunications companies. Symphonya Emerging Issues in Management, 1. https://doi.org/10.4468/2014.2.03gandini.bosetti.almici

Gao, Y. (2022). Prediction of telecommunication network fraud crime based on regression-LSTM model. Wireless Communications and Mobile Computing, 2022, 3151563. https://onlinelibrary.wiley.com/doi/full/10.1155/2022/3151563

Garg, S., Jain, A., & Sahai, A. (2011). Leakage-resilient zero knowledge. In Advances in Cryptology–CRYPTO 2011: 31st Annual Cryptology Conference (pp. 297–315). Springer. https://doi.org/10.1007/978-3-642-22792-9_17

Garrido-Merchán, E. C., González-Barthe, C., & Coronado Vaca, M. (2023). Fine-tuning ClimateBert transformer with ClimaText for the disclosure analysis of climate-related financial risks. arXiv preprint arXiv:2303.13373. https://arxiv.org/abs/2303.13373

Ghairwar, A. (2024, May 19). Natural Language Processing (NLP) Applications in Actuarial Science. Medium. https://medium.com/@adityasinghghairwar/natural-language-processing-nlp-applications-in-actuarial-science-15f0707edc7f

Grishunin, S., & Suloeva, S. (2017). Development of the Credit Risk Assessment Mechanism of investment projects in telecommunications. In Lecture notes in computer science (pp. 300–314). https://doi.org/10.1007/978-3-319-67380-6_28

GSMA. (2024, November 5). Mobile and Banking Industries Join Forces to Fight Fraud. Retrieved from https://www.gsma.com/newsroom/press-release/mobile-and-banking-industries-join-forces-to-fight-fraud/

Gwala, R. S. (2025). The use of blockchain technology and artificial intelligence in cryptocurrency and medical technology. In Advances in computational intelligence and robotics book series (pp. 147–184). https://doi.org/10.4018/979-8-3693-8664-4.ch007

Hacklido. (n.d.). Exploring Different Consensus Mechanisms: A Comprehensive Guide to Blockchain Security. Retrieved from https://www.hacklido.com/blog/579-exploring-different-consensus-mechanisms-a-comprehensive-guide-to-blockchain-security

Haq, M. A., & Khan, M. A. (2024). Customer Churn Prediction Using Machine Learning Algorithms. Retrieved from https://www.researchgate.net/publication/379527554_Customer_Churn_Prediction_Using_Machine_Learning_Algorithms

He, X., & Chua, T.-S. (2017). Neural factorization machines for sparse predictive analytics. arXiv preprint arXiv:1708.05027. https://arxiv.org/abs/1708.0502

Hu, Y., Shao, Y., Zhu, T., & Luo, M. (2023). Federated learning for financial transaction fraud detection: Challenges and future directions. Future Generation Computer Systems, 137, 149–162. https://doi.org/10.1016/j.future.2023.07.003

Huang, Y., Fang, S., Li, J., Hu, B., & Zhang, T. (2022). SmartIntentNN: Towards smart contract intent detection. arXiv preprint arXiv:2211.13670. https://arxiv.org/abs/2211.13670

Hui, X., & Tucker, C. E. (2023). Decentralization, blockchain, Artificial intelligence (AI): challenges and opportunities. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4601788

IBM. (n.d.). Smarter Supplier Onboarding and Collaboration: An IBM point of view. Retrieved from https://www.ibm.com/watson/supply-chain/resources/smarter-supplier-onboarding-and-collaboration/

IMARC Group. (2024, November 12). Global Telecom Analytics Market to Reach USD 19.0 Billion by 2033. Retrieved from https://www.imarcgroup.com/global-telecom-analytics-market

J, R. H., & Mohana, N. (2022). Fraud Detection and Management for Telecommunication Systems using Artificial Intelligence (AI). 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC), 1016–1022. https://doi.org/10.1109/icosec54921.2022.9951889

Jamshidi, M. (2024). Innovative telecom fraud detection: A new dataset and an advanced model with RoBERTa and dual loss functions. Applied Sciences, 14(24), 11628. https://www.mdpi.com/2076-3417/14/24/11628

Junge, M. R. J., & Dettori, J. R. (2018). ROC solid: Receiver operator characteristic (ROC) curves as a foundation for better diagnostic tests. Global Spine Journal, 8(4), 424–429.

https://journals.sagepub.com/doi/abs/10.1177/2192568218778294

Kabari, L. G., Nanwin, D. N., & Nquoh, E. U. (2015). Telecommunications subscription fraud detection using artificial neural networks. Transactions on Machine Learning and Artificial Intelligence, 3(6). https://doi.org/10.14738/tmlai.36.1695

Kalkan, Y. (2022). Credit default status prediction with machine learning and deep learning techniques and comparisons. Academia.edu. https://www.academia.edu/10000000/Credit_default_status_prediction_with_machine_learning_and_deep_learning_techniques_and_comparisons

Kamel, M. B., Yan, Y., Ligeti, P., & Reich, C. (2022). Attribute Verifier for Internet of Things. In 2022 32nd International Telecommunication Networks and Applications Conference (ITNAC) (pp. 1–3). https://doi.org/10.1109/ITNAC55456.2022.10001095

Kar, M. (2019). Pricing strategies in mobile telecommunications markets. Social Mentality and Researcher Thinkers Journal, 5(16), 360–371. https://doi.org/10.31576/smryj.240

Kaur, M., & Mohta, A. (2019). A Review of Deep Learning with Recurrent Neural Network. 2019 International Conference on Smart Systems and Inventive Technology (ICSSIT). https://doi.org/10.1109/icssit46314.2019.8987837

Kori, A., & Gadagin, N. (2024). Blockchain-Based AI Models for Credit Scoring and Risk Assessment using Fog Computing Infrastructure. International Journal of Research Publication and Reviews, 5(11), 876–888. https://doi.org/10.55248/gengpi.5.1124.3136

Kumar, R., & Sharma, S. (2022). Model Optimization Analysis of Customer Churn Prediction Using Machine Learning Algorithms with Focus on Feature Reductions. Retrieved from https://www.researchgate.net/publication/361636981_Model_Optimization_Analysis_of_Customer_Churn_Prediction_Using_Machine_Learning_Algorithms_with_Focus_on_Feature_Reductions

Kuznetsov, O., Sernani, P., Romeo, L., Frontoni, E., & Mancini, A. (2024). On the Integration of Artificial Intelligence and Blockchain Technology: A Perspective About Security. IEEE Access, 12, 3881–3897. https://doi.org/10.1109/access.2023.3349019

Lacuška, M., & Peráček, T. (2020). Trends in global telecommunication fraud and its impact on business. In Studies in systems, decision, and control (pp. 459–485). https://doi.org/10.1007/978-3-030-62151-3_12

Lashkari, B., & Musilek, P. (2021). A comprehensive review of blockchain consensus mechanisms. IEEE Access, 9, 43620–43652. https://doi.org/10.1109/access.2021.3065880

Ledger Insights. (2019, October 31). Deutsche Telekom, Telefonica, Vodafone trial blockchain for roaming payments. Ledger Insights - Blockchain for Enterprise. https://www.ledgerinsights.com/deutsche-telekom-telefonica-vodafone-blockchain-roaming-payments/

Ledger Insights. (2020, March 6). Vodafone using supplier management blockchain from IBM. Retrieved from https://www.ledgerinsights.com/vodafone-blockchain-trust-yoursupplier-management-ibm/

LeewayHertz. (n.d.). Cost of blockchain implementation. Retrieved from https://www.leewayhertz.com/cost-of-blockchain-implementation/

Li, Z., Chen, B., & Lu, S. (2022). The impact of information and communication technology on financial inclusion-based on a global perspective. AIMS Mathematics, 7(12), 20930–20961. https://doi.org/10.3934/math.20221147

Liang, J., Li, S., Cao, B., Jiang, W., & He, C. (2021). OmniLytics: A blockchain-based secure data market for decentralized machine learning. arXiv preprint arXiv:2107.05252. https://arxiv.org/abs/2107.05252

Lottu, N. O. A., Abdul, N. a. A., Daraojimba, N. D. O., Alabi, N. a. M., John-Ladega, N. a. A., & Daraojimba, N. C. (2023). DIGITAL TRANSFORMATION IN BANKING: A REVIEW OF NIGERIA'S JOURNEY TO ECONOMIC PROSPERITY. International Journal of Advanced Economics, 5(8), 215–238. https://doi.org/10.51594/ijae.v5i8.572

Marcinek, K., Stanley, K. D., Smith, G., Cormarie, P., & Gunashekar, S. (2024, November 20). Risk-Based AI regulation: A primer on the Artificial Intelligence Act of the European Union. RAND. https://www.rand.org/pubs/research_reports/RRA3243-3.html

Mashrur, A., Luo, W., Zaidi, N. A., & Robles-Kelly, A. (2020). Machine Learning for Financial Risk Management: A survey. IEEE Access, 8, 203203–203223. https://doi.org/10.1109/access.2020.3036322

Mayer, N., & Aubert, J. (2020). A risk management framework for security and integrity of networks and services. Journal of Risk Research, 24(8), 987–998. https://doi.org/10.1080/13669877.2020.1779786

Mazzocca, C., Acar, A., Uluagac, S., Montanari, R., Bellavista, P., & Conti, M. (2024). A survey on decentralized identifiers and verifiable credentials. arXiv preprint arXiv:2402.02455. https://arxiv.org/abs/2402.02455

MDPI. (2023). Scalability and Efficiency Analysis of Hyperledger Fabric and Private Ethereum in Smart Contract Execution. Retrieved from https://www.mdpi.com/2073-431X/14/4/132

Mienye, D. I., & Jere, N. R. (2024). Deep learning for credit card fraud detection: A review of algorithms, challenges, and solutions. ResearchGate. https://www.researchgate.net/publication/372750682_Auto-Encoder_and_LSTM-Based_Credit_Card_Fraud_Detection

Misra, S. K., Das, S., Gupta, S., & Sharma, S. K. (2020b). Public policy and regulatory challenges of artificial intelligence (AI). In IFIP Advances in Information and Communication Technology (pp. 100–111). https://doi.org/10.1007/978-3-030-64849-7_10

Moin, A., & Islam, M. (2023). Blockchain-based decentralized identification in IoT: An overview of existing frameworks and their limitations. Electronics, 12(6), 1283. https://doi.org/10.3390/electronics12061283

Murtaza, M. H., Alizai, Z. A., & Iqbal, Z. (2019). Blockchain based anonymous voting system using zkSNARKs. In 2019 International Conference on Applied and Engineering Mathematics (ICAEM) (pp. 209–214). https://doi.org/10.1109/ICAEM.2019.8885914

Mushtaq, M. F., Akram, U., Aamir, M., Ali, H., &
Zulqarnain, M. (2019). Neural Network Techniques for Time Series Prediction: A review. JOIV International Journal on Informatics Visualization, 3(3), 314–320. https://doi.org/10.30630/joiv.3.3.28

Namavar Jahromi, A., Pourjafari, E., Karimipour, H., Satpathy, A., & Hodge, L. (2023). CRL+: A Novel Semi-

Supervised Deep Active Contrastive Representation Learning-Based Text Classification Model for Insurance Data. arXiv preprint arXiv:2302.04343. https://arxiv.org/abs/2302.04343

Nasir, N. M., Hassan, S., & Zaini, K. M. (2024). Securing Permissioned Blockchain-based Systems: An analysis on the significance of consensus mechanisms. IEEE Access, 1. https://doi.org/10.1109/access.2024.3465869

Nayak, B. S., & Xu, J. (2018). Historical trends and transitions in credit risk management of Chinese commercial banks. International Journal of Business Administration, 9(5), 96. https://doi.org/10.5430/ijba.v9n5p96

Neptune.ai. (2022, August 9). When to choose CatBoost over XGBoost or LightGBM. https://neptune.ai/blog/when-to-choose-catboost-over-xgboost-or-lightgbm

Nielsen, M. A. (2015). Neural networks and deep learning. Determination Press. Retrieved from http://neuralnetworksanddeeplearning.com/

NVIDIA. (n.d.). Amdocs builds generative AI agents for telecom. https://resources.nvidia.com/en-us-ai-powered-operations/amdocs-builds-generative-ai-agents-for-telecom

Oracle. (n.d.). Announcing the general availability of OCI generative AI agents. https://blogs.oracle.com/ai-and-datascience/post/ga-of-oci-gen-ai-agent-platform

Oseni, A., & Bello, S. (2020). Optimizing wholesale intercarrier settlement with Hyperledger Fabric blockchain. ResearchGate. https://www.researchgate.net/publication/350007567_Optimizing_Wholesale_Intercarrier_Settlement_with_Hyperledger_Fabric_Block

Óskarsdóttir, M., Bravo, C., Verbeke, W., Sarraute, C., Baesens, B., & Vanthienen, J. (2020). Social network analytics for churn prediction in telco: Model building, evaluation and network architecture. arXiv preprint arXiv:2001.06701. https://arxiv.org/abs/2001.06701

Owczarczuk, M. (2023). Ethical and regulatory challenges amid artificial intelligence development: An outline of the issue. Ekonomia I Prawo, 22(2), 295–310. https://doi.org/10.12775/eip.2023.017

Pape. (2025, May 28). XGBoost, LightGBM or CatBoost? The ultimate test for credit scoring models. Medium. https://medium.com/@pape14/xgboost-lightgbm-or-catboost-the-ultimate-test-for-credit-scoring-models-88ac56729ebc

Pasupuleti, M. K. (2025). Automated Smart Contracts: AI-powered blockchain technologies for secure and intelligent decentralized governance. https://doi.org/10.62311/nesx/rrv425

Patishmam, K. (2023). AI and blockchain integration in telecom credit risk assessment. Journal of Telecommunications and Digital Finance, 5(1), 23–35.

Pava-Díaz, R. A., Gil-Ruiz, J., & López-Sarmiento, D. A. (2024). Self-sovereign identity on the blockchain: Contextual analysis and quantification of SSI principles implementation. Frontiers in Blockchain, 7, 1443362. https://doi.org/10.3389/fbloc.2024.1443362

Pavlidis, G. (2024). Unlocking the black box: Analysing the EU Artificial Intelligence Act's framework for explainability in AI. Law Innovation and Technology, 16(1), 293–308. https://doi.org/10.1080/17579961.2024.2313795

Peres, D. J., & Cancelliere, A. (2014). Derivation and evaluation of landslide-triggering thresholds by a Monte Carlo approach. Hydrology and Earth System Sciences, 18(12), 4913–4931. https://hess.copernicus.org/articles/18/4913/2014/

Pham, T. L., & Le, Q. D. (2023). Proposing of imaging graph neural network with defined security pattern for improving smart contract vulnerability detection. ICT Research. https://www.researchgate.net/publication/369665804_Smart_Contract_Vulnerability_Detection_Model_Based_on_Siamese_Network

Phong, L. T., Aono, Y., & Hayashi, T. (2018). Privacy-Preserving Deep Learning via Additively Homomorphic Encryption. IEEE Transactions on Information Forensics and Security, 13(5), 1333–1345. https://doi.org/10.1109/TIFS.2017.2787987

PMC. (2025). Harmonization and Integration of Data from Prospective Cohort Studies. Retrieved from https://pmc.ncbi.nlm.nih.gov/articles/PMC12109133/

Powers, D. M. W. (2011). Evaluation: From precision, recall and F-measure to ROC, informedness, markedness and correlation. Journal of Machine Learning Technologies, 2(1), 37–63. https://www.researchgate.net/publication/220766891_Evaluation_From_Precision_Recall_and_F-Measure_to_ROC_Informedness_Markedness_and_Correlation

Pradel, G., & Mitchell, C. (2021). Privacy-Preserving Biometric Matching Using Homomorphic Encryption. arXiv preprint arXiv:2111.12372. https://arxiv.org/abs/2111.12372

Provenzano, A. R., Trifirò, D., Datteo, A., Giada, L., Jean, N., Riciputi, A., Le Pera, G., Spadaccino, M., Massaron, L., & Nordio, C. (2020). Machine learning approach for credit scoring. arXiv preprint arXiv:2008.01687. https://arxiv.org/abs/2008.01687

Rahman, T., Mouno, S. I., Raatul, A. M., Al Azad, A. K., & Mansoor, N. (2023). Verifi-Chain: A credentials verifier using blockchain and IPFS. arXiv preprint arXiv:2307.05797. https://arxiv.org/abs/2307.05797

Rane, N., Choudhary, S., & Rane, J. (2023b). Blockchain and Artificial Intelligence (AI) integration for revolutionizing security and transparency in finance. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4644253

Ratnakumari, J., Thahenath, S. N. A., Lakshmi, T. S., Kumar, P. N. D., & Veeraiah, K. (2024). Detection of fraudulent or deceptive phone calls using artificial intelligence. Türk Bilgisayar Ve Matematik Eğitimi Dergisi, 15(1), 96–99. https://doi.org/10.61841/turcomat.v15i1.14546

Refaey, A., Hammad, K., Magierowski, S., & Hossain, E. (2019). A blockchain policy and charging control framework for roaming in cellular networks. arXiv (Cornell University). https://doi.org/10.48550/arxiv.1906.06350

Saad, S., Nadher, I., & Hameed, S. M. (2024). Credit card fraud detection challenges and solutions: A review. Iraqi Journal of Science, 65(4), 2287-2303. https://doi.org/10.24996/ijs.2024.65.4.42

Sai, S., Chamola, V., Choo, K. R., Sikdar, B., & Rodrigues, J. J. P. C. (2022). Confluence of blockchain and artificial intelligence technologies for secure and scalable healthcare Solutions: a review. IEEE Internet of Things Journal, 10(7), 5873–5897. https://doi.org/10.1109/jiot.2022.3232793

Salama, H. A. (2023). The determinations of the consumer credit default probabilities in the telecommunication industry. Zenodo (CERN European Organization for

Nuclear Research). https://doi.org/10.5281/zenodo.7964084

Saleh, A. M. S. (2024). Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review. Blockchain Research and Applications, 5(3), 100193. https://doi.org/10.1016/j.bcra.2024.100193

Sana, J. K., Abedin, M. Z., Rahman, M. S., & Rahman, M. S. (2022). Data transformation based optimized customer churn prediction model for the telecommunication industry. arXiv preprint arXiv:2201.04088. https://arxiv.org/abs/2201.04088

Schlatt, V., Sedlmeir, J., Feulner, S., & Urbach, N. (2022). Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity. Information & Management, 59(7), 103553. https://doi.org/10.1016/j.im.2021.103553

Sehrawat, S., & Singh, R. (2023). Auto-encoder and LSTM-based credit card fraud detection. SN Computer Science, 4(1), 19. https://dlnext.acm.org/doi/ 10.1007/s4 2979-023-01977-w

Shareef, A. M. A., Seçkiner, S., Eid, B., & Abumeteir, H. (2024). Integration of blockchain with artificial intelligence technologies in the energy sector: A systematic review. Frontiers in Energy Research, 12. https://doi.org/10.3389/fenrg.2024.1377950

Shirole, M. (2023). Decentralized identity management using blockchain. Academia.edu. https://www.academia.edu/121109704/Decentralized_Identity_Management_Using_Blockchain

Singh, M. T., Prasad, R. K., Michael, G. R., Kaphungkui, N. K., & Singh, N. H. (2024). Heterogeneous graph auto-encoder for credit card fraud detection. arXiv preprint arXiv:2410.08121. https://arxiv.org/abs/2410.08121

Sharma, N. D. N. (2024). Artificial Intelligence: Legal implications and challenges. Knowledgeable Research: A Multidisciplinary Journal, 2(11), 13–32. https://doi.org/10.57067/220k4298

Shen, Q. (2024). AI-driven financial risk management systems: Enhancing predictive capabilities and operational efficiency. Applied and Computational Engineering, 69(1), 134–139. https://doi.org/10.54254/2755-2721/69/20241494

Sherstinsky, A. (2020). Fundamentals of recurrent neural network (RNN) and long short-term memory (LSTM) network. Physica D: Nonlinear Phenomena, 404, 132306. https://doi.org/10.1016/j.physd.2019.13230

Sila, I. S., & Al-Mutairi, F. H. (2025). AI for data harmonization: Overcoming challenges in multi-source data integration. ResearchGate. https://www.researchgate.net/publication/389548301_AI_for_Data_Harmonization_Overcoming_Challenges_in_Multi-_Source_Data_Integration

Singanamalla, S., Mehra, A., Chandran, N., Lohchab, H., Chava, S., Kadayan, A., Mani, K., Shanmugam, R., Srikanth, M., & Lokam, S. (2022). Telechain: Bridging telecom policy and blockchain practice. arXiv. https://arxiv.org/abs/2205.12350

Sonawane, Y. B., Gadgil, A. S., More, A. E., & Jathar, N. K. (2016). Credit card fraud detection using clustering based approach. International Journal of Advanced Research in Innovative Ideas in Education, 2(6).

Soori, M., Dastres, R., & Arezoo, B. (2023). AI-powered blockchain technology in Industry 4.0: A review. Journal of Economy and Technology, 1, 222–241. https://doi.org/10.1016/j.ject.2024.01.001

Sotovalero, C. (2025, May 28). From classical ML to DNNs and GNNs for real-time financial fraud detection. https://www.cesarsotovalero.net/blog/real-time-financial-fraud-detection.html

Spuchľáková, E., Valašková, K., & Adamko, P. (2015). The Credit Risk and its Measurement, Hedging and Monitoring. Procedia Economics and Finance, 24, 675–681. https://doi.org/10.1016/s2212-5671(15)00671-1

Stone, M. (2015). The evolution of the telecommunications industry—What can we learn from it? Journal of Direct Data and Digital Marketing Practice, 16(3), 157–165. https://doi.org/10.1057/dddmp.2014.80

Subex. (n.d.). Telecom alternate credit scoring: Harnessing AI/ML for enhanced risk management. https://www.subex.com/glossary/telecom-alternate-credit-scoring-harnessing-ai-ml-for-enhanced-risk-management/

Subex Limited. (2024, September 25). Telecom rating and billing with AI-powered business assurance: What you need to know. https://www.subex.com/article/telecom-rating-and-billing-with-ai-powered-business-assurance-what-you-need-to-know/

Sudharson, K., Babu, G., Santhiya, R., & Anita, C. (2025). Enhanced privacy-preserving federated convivial learning for internet of medical things (IoMT) through blockchain-enabled trust Q-learning. Journal of the National Science Foundation of Sri Lanka, 52(4), 501–514. https://doi.org/10.4038/jnsfsr.v52i4.11923

Sukharev, I., Shumovskaia, V., Fedyanin, K., Panov, M., & Berestnev, D. (2020). EWS-GCN: Edge weight-shared graph convolutional network for transactional banking data. arXiv preprint arXiv:2009.14588. https://arxiv.org/abs/2009.14588

Suliman, A., Husain, Z., Abououf, M., Alblooshi, M., &Salah, K. (2018). Monetization of IoT data using smart contracts. IET Networks, 8(1), 32–37. https://doi.org/10.1049/iet-net.2018.5026

Szczerba, M., & Ciemski, A. (2009). Credit risk handling in telecommunication sector. In Lecture notes in computer science (pp. 117–130). https://doi.org/10.1007/978-3-642-03067-3_11

Taherdoost, H. (2023). Smart contracts in blockchain technology: A critical review. Information, 14(2), 117. https://doi.org/10.3390/info14020117

Talasila, S. D. (2024). AI-Driven Personal Finance Management: Revolutionizing Budgeting and Financial Planning. International Research Journal of Engineering and Technology (IRJET), 11(7), 397. Retrieved from https://www.researchgate.net/publication/382679575_AI-Driven_Personal_Finance_Management_Revolutionizing_Budgeting_and_Financial_Planning

Telefónica. (n.d.). Telefónica open Gateway. Telefónica Open Gateway. https://opengateway.telefonica.com/en/apis/number-verification

The Crypto Cortex. (n.d.). Exploring Blockchain for Telecommunication Solutions: A New Era. Retrieved from https://thecryptocortex.com/exploring-blockchain-for-telecommunication-solutions/

Tran, D. Q., Doan, D. N., & Pham, T. V. H. (2022). Predicting Customer Churn in Telecommunication by Ensemble Learning. In Proceedings of the Sixth International Congress on Information and Communication

Technology (pp. 619–627). Springer. https://doi.org/10.1007/978-981-16-2102-4_55. Retrieved from https://www.researchgate.net/publication/355681954_Predicting_Customer_Churn_in_Telecommunication_by_Ensemble_Learning

Tripathi, G., Ahad, M. A., & Casalino, G. (2023). A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges. Decision Analytics Journal, 9, 100344. https://doi.org/10.1016/j.dajour.2023.100344

Valenduc, G., & Vendramin, P. (2017). Digitalisation, between disruption and evolution. Transfer European Review of Labour and Research, 23(2), 121–134. https://doi.org/10.1177/1024258917701379

Vallarino, D. (2025). Detecting financial fraud with hybrid deep learning: A mix-of-experts approach to sequential and anomalous patterns. arXiv preprint arXiv:2504.03750. https://arxiv.org/abs/2504.03750

Van Hoang, T. (2024). Impact of integrated artificial intelligence and internet of things technologies on smart city transformation. Technical Education Science/GiáO DụC Kỹ ThuậT, 19(1), 64–73. https://doi.org/10.54644/jte.2024.1532

Van Houdt, G., Mosquera, C., & Nápoles, G. (2020). A review on the long short-term memory model. Artificial Intelligence Review, 53(8), 5929–5955. https://doi.org/10.1007/s10462-020-09838-1

Verizon Communications Inc. (2024, January 23). Verizon delivered strong customer growth and profitability in Q4 2024. Verizon. https://www.verizon.com/about/news/verizon-delivered-strong-customer-growth-and-profitability-2024

Vikhyath, K. B., Sanjana, R. K., & Vismitha, N. V. (2021). Intersection of AI and blockchain technology: Concerns and prospects. In Lecture Notes in Networks and Systems (pp. 53–66). https://doi.org/10.1007/978-3-030-84337-3_5

Vodafone. (2024, May 8). Pairpoint by Vodafone and Sumitomo Corporation announce partnership with Sensos to combat supply chain fraud. Retrieved from https://www.vodafone.com/news/technology/pairpoint-by-vodafone-and-sumitomo-corporation-announce-partnership-with-sensos-to-combat-supply-chain-fraud

Vodafone. (2023, October 24). Vodafone DAB and Chainlink Labs demonstrate the transformation of global trade through blockchain innovation. Retrieved from https://www.vodafone.com/news/technology/vodafone-dab-chainlink-lab-demonstrates-transformation-global-trade-blockchain-innovation

Vodafone Business IOT to provide global connectivity for the Oracle Enterprise Communications Platform. (2024, November 5). Oracle. https://www.oracle.com/ba/news/announcement/vodafone-business-iot-to-provide-global-connectivity-for-the-oracle-enterprise-communications-platform-2024-11-05/

Wang, Z. (2024b). Artificial intelligence and Machine learning in credit risk assessment: Enhancing accuracy and ensuring fairness. Open Journal of Social Sciences, 12(11), 19–34. https://doi.org/10.4236/jss.2024.1211002

Waqas, M., & Humphries, U. W. (2024). A Critical review of RNN and LSTM variants in hydrological Time Series predictions. MethodsX, 13, 102946. https://doi.org/10.1016/j.mex.2024.102946

Wall Street Journal. (2025, April 22). Verizon earnings Q1 2025: Postpaid phone losses widen. https://www.wsj.com/business/earnings/verizon-earnings-q1-2025-vz-stock-6cab14d0

Wang, Y. (2024). The integration of blockchain technology and artificial intelligence: Innovation, challenges, and future prospects. Applied and Computational Engineering, 55(1), 145–156. https://doi.org/10.54254/2755-2721/55/20241417

Wolniak, R., & Stecuła, K. (2024). Artificial intelligence in smart cities—Applications, barriers, and ethical aspects. Sustainability, 16(2), 841. https://doi.org/10.3390/su16020841

Yang, S., Huang, Z., Xiao, W., & Shen, X. (2025). Interpretable credit default prediction with ensemble learning and SHAP. arXiv preprint arXiv:2505.20815. https://arxiv.org/abs/2505.20815

Yang, X., & Li, W. (2020). A zero-knowledge-proof-based digital identity management scheme in blockchain. Computers & Security, 99, 102037. https://doi.org/10.1016/j.cose.2020.102037

Yin, Y. (2021). Training massive deep neural networks in a smart contract: A new hope. arXiv preprint arXiv:2106.14763. https://arxiv.org/abs/2106.14763

Zaratiegui, J., Montoro, A., & Castanedo, F. (2015). Performing highly accurate predictions through convolutional networks for actual telecommunication challenges. arXiv preprint arXiv:1511.04906. https://arxiv.org/abs/1511.04906

Zhai, J., Zhang, S., Chen, J., & He, Q. (2018). Autoencoder and its various variants. In 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC) (pp. 415–419). IEEE. https://doi.org/10.1109/SMC.2018.00079

Zhang, M., & Cao, C. (2021). A Systematic Literature Review on the credit risk management of Big Tech Lending. Journal of Risk Analysis and Crisis Response, 11(3). https://doi.org/10.54560/jracr.v11i3.303

Zou, J., Zhang, J., & Jiang, P. (2019). Credit card fraud detection using autoencoder neural network. arXiv preprint arXiv:1908.11553. https://arxiv.org/abs/1908.11553

****