Interdisciplinary Journal of Computing & AI

IJCAI

Interdisciplinary Journal of Computing & AI

RESEARCH

Creaboost: A Blockchain-Enabled Federated Learning Platform for Privacy-Preserving Ad Preference Insights and Creator Rewards

Ritesh Kumar Shaw[1], Safiya Ahmed[2], Stuti Sinha[3*], Subhangi Chatterjee[4]

[1,2,3,4]*Cybersecurity Centre of Excellence, Institute of Engineering and Management, University of Engineering and Management, Kolkata*

[1]*Email: riteshkumarshaw072@gmail.com*, [2]*Email: safiyaahmed165@gmail.com*, [3]*Email: stutisinha712@gmail.com*, [4]*Email: subhangichatterjee04@gmail.com*

ARTICLE INFO.

Keywords: Blockchain incentives, Federated learning, Low-latency aggregation, Privacy-preserving advertising, Smart contract rewards, XDC Network

*Corresponding author email address: stutisinha712@gmail.com

Manuscript received: 11 March 2026/Accepted 2 April 2026
Published online: 6 April 2026
https://doi.org/10.5281/zenodo.19434964

Cite as: R. K. Shaw, S. Ahmed, S. Sinha and S. Chatterjee, "Creaboost: A Blockchain-Enabled Federated Learning Platform for Privacy-Preserving Ad Preference Insights and Creator Rewards", Interdisciplinary Journal of Computing & AI (IJCAI), vol. 1, no. 1. Aspiration Publishing Trust (DARPAN ID: WB/2025/0887371), p. 43-57, Apr. 2026. doi: 10.5281/zenodo.19434964.

ABSTRACT

Privacy preserving ad targeting is a major challenge in today's digital environment. It is such an environment where the centralized platforms expose user data and provide creators with low lying compensation. Although current federated learning (FL) models help reduce data leakage but do not have on chain reward systems. Blockchain based reward systems often face issues with slow speeds and high costs on public networks like Ethereum. This paper introduces Creaboost, a decentralized application on the XDC Network. It combines FL with smart contract rewards to allow secure, low-lying cost, and fair ad preference collection to its users. Here the users are going to submit their engagement metrics locally. After five unparalleled submissions, we aggregate model parameters off chain using federated learning. The resulting preference (0 or 1) then triggers an on-chain reward (1 or 2 ether) through a user signed transaction. Creaboost extends through five layers: Client, Frontend (HTML/JS), Backend (Flask), FL Server (PyTorch), and Blockchain. This setup guarantees that the raw

	data exposure leaves the Ethereum device. We ensure security with SSL/TLS, reCAPTCHA v2, email verification, and XDC signing. Creaboost exceeds both centralized and XDC alternatives by minimizing data exposure, execution costs, and XDC creating a scalable framework for transaction advertising.

1 Introduction

The rapid rise of digital content platforms within a few decades has changed the advertising industry a lot, generating almost $979 billion (MAGNA) and $1.08 trillion (WPP/GroupM) in annual revenue by using the user's engagement signals like views, likes, shares, and time spent on watching various contents on these platforms. With more than 6 billion active internet users worldwide as of 2025, these behaviors support various complex targeting algorithms that help deliver personalized ads as per viewers interests. However, the value generated with these ads are mainly handed over to centralized ad networks such as Google, Meta, and TikTok. These networks collect, store, and process sensitive user's data on their respective cloud infrastructure. On the other hand, content creators, who produce the entire content, often end up obtaining even less than 1% of the topical ad spend in revenue sharing models. Such uneven distribution of value, with the topical data breaches and India's seen like GDPR, CCPA, and India's Digital Personal Data Protection Act 2023, highlights really dangerous flaws in the revenue sharing topical system.

FL emerged in machine as a local way to create these updates issues in earlier machine learning [1], [2]. Developed by Google, FL can collaboratively model over distinguishable devices without sharing raw determinant data. Instead, each client trains a central model over its own separate data and sends them simply to the model where the updates-like gradients or parameter changes to a young aggregator. The server then combines all of these privacy using algorithms like in [3] to create a spheric model. Rude examples can reach seen like in machine next word prediction and healthcare diagnostics [4] showed that FL can reach almost centralized accuracy while keeping all of data on the model.

Blockchain technology complements FL in many ways by introducing programmable, secure, and transparent incentives. Since Bitcoin's launch in 2009 and Ethereum's in 2015, blockchain has advanced a lot from just a cryptocurrency register to a versatile state machine that can easily execute smart contracts. Projects like Basic Attention Token (BAT) (2017) and the Brave Browser have pioneered the idea of rewarding their user's attention with tokens, allowing the publishers to earn directly from their audience itself. However, all of these systems run on Ethereum Mainnet, where transaction fees

often exceed $1-$10 during busy times when the load is very high, and confirmation times average around 15 seconds per block approximately. These costs and delays make the real-time micro-rewards an impractical task, especially for frequent actions like updating ad preferences [5], [6], [7].

Alternative layer-1 and layer-2 solutions have really tried to boost the scalability. Solana achieves 65,000 transactions per second using the Proof-of-History, but its validator centralization raises a very high risk of censorship. Polygon cuts Ethereum gas fees by 90% through their sidechain commitment, but it still faces delays while facing a huge load during high network stress. None of these platforms were created with the idea of enterprise-level compliance or hybrid public-private interoperability in mind.

The XDC Network, launched in 2019 by XinFin, addresses these limitations through a hybrid blockchain system designed for orderly digital asset workflows. Built on XDPoS (XinFin Delegated Proof of Stake), it operates with a consortium of 108 master nodes for 2 second block finality, over 2,000 transactions per second, and very low fees around 1/100th of Ethereum's cost. Its built-in support for ISO 20022 financial messaging standards allows easy integration with traditional banking systems, making it ideal for privacy focused, high traffic applications in advertising, trade finance, and supply chains [5]. Despite these benefits, no former work has used XDC as a settlement layer for federated learning-based advertising systems.

In this paper, we present Creaboost, the first production-ready decentralized application, integrating federated learning, threshold-based off-chain aggregation, and XDC native smart contracts for rewards under a single advertising platform. Users can interact through a simple web interface, clientP.html, to send engagement metrics. AdTargetingModel, the local network trains locally, sending encrypted model updates to a Flask backend, which stores them in an SQLite database and combines them all after five unique, verified submissions, avoiding manipulations and minimizing blockchain writes. The final multiple preference, 0 for neutral and 1 for high engagement, is then recorded on the XDC blockchain through a user-signed transaction to the AdPreferences1.sol smart contract, instantly minting a reward of 1 or 2 ether depending on the strength of the preference.

The system is structured across five standard layers:

- Client Layer: Browser based interface with XDC wallet integration (XDCPay or MetaMask).
- Frontend Layer: HTML/JavaScript with client-side validation and local model inference.
- Backend Layer: Flask server managing API endpoints, submission tracking, and aggregation triggers.
- Federated Learning Layer: PyTorch based aggregation server running FedAvg.
- Blockchain Layer: XDC Testnet (Apothem) hosting the clever contract

for minting rewards.

Security is reinforced at every level: SSL/TLS secures all communication, reCAPTCHA v2 stops bot submissions, email and OTP verification links identities, private key signing guarantees non repudiable transactions, and a 10% gas price buffer protects against network fluctuations.

The innovations in this work include:

- The first combination of federated learning with threshold triggered, XDC based smart contract rewards for advertising that preserves privacy.
- A local to global preference inference process that does not expose raw engagement data at any point.
- Gas optimized reward minting based on binary preference outcomes and Sybil resistant aggregation.
- A complete, open-source full stack solution with thorough performance testing under realistic scenarios.
- Proving sub-five-second end-to-end latency and sub-cent transaction costs in a regulated blockchain setting.

The rest of this paper is organized as follows: Section 2 provides the preliminary knowledge of federated learning, blockchain incentives, and decentralized advertising. Section 3 presents the literature survey. Section 4 outlines the proposed design, followed by Section 5 on security analysis. Section 6 assesses performance against focused benchmarks using latency, throughput, cost, and scalability metrics. Section 7 wraps up the paper and suggests future research paths.

2 Preliminary Knowledge

2.1 Federated Learning (FL)

Federated Learning (FL) is a distributed machine learning approach that allows multiple devices to collaboratively train a common model while keeping all training data localized [2], [5]. Each client device performs local training on its snobbish dataset such as user engagement metrics and sends only model updates (typically gradients or weights) to a central aggregation server. The server combines these updates using algorithms like FedAvg, which computes a weighted modal to form a better global model. This mechanism ensures that bare raw data never leaves the user's device, importantly reducing privacy risks compared to centralized training. FL has been successfully applied in mobile keyboards, healthcare diagnostics, and recommendation systems, achieving near centralized accuracy with strong data protection.

2.2 XDC Network

The XDC Network is a hybrid and enterprise-focused blockchain platform developed in 2019 by XinFin, aiming for high performance and regulatory compliant digital transactions [7]. It is based on XDPoS technology with 108 validator master nodes for achieving block finality within 2 seconds, facilitating more than 2,000 transactions per second, and charging transaction fees 1/100th of Ethereum. XDC is EVM compatible, supporting solidity smart contracts and ISO 20022 messaging standards for seamless integration with traditional finance systems. XDC Network can be used for both public and consortium blockchains, facilitating the development of decentralized applications in advertising, trade finance, and supply chains in a secure and ascendable manner.

2.3 Smart Contracts and Solidity

A smart contract is a self-executing software stored on a blockchain, which executes a set of pre-defined rules upon occurrence of a valid transaction [5]. These contracts, coded in solidity, a low-level programming language for EVM compatible blockchains like XDC, manage changes in states, token creation, and access control in an immutable and transparent manner. A smart contract, once deployed, is immutable and can be executed by any participant on a decentralized system. In a decentralized system, contracts remove intermediaries and ensure that outcomes like rewards are determined based on code alone.

2.4 Web3 and Wallet Interaction

On the other hand, the term Web3 represents decentralized applications (dApps) that allow the direct interaction of users with the blockchain network without the presence of a specific intermediary. Using a JavaScript library like Web3.js or Ethers.js, the frontend interface interacts with the user's wallet, like XDCPay or MetaMask, which controls the private keys of the users and allows them to perform actions like digital identity and asset completion while allowing non-repudiable actions like preference submission and reward claiming on the blockchain in a privacy-preserving manner.

3 Literature Survey

Scientists have been aware of the concept of FL for quite a while, and they have also taken cognizance of its drawbacks, risks and potential in the same amount of time. The landmark work on federated learning is the primary source of information. By distinguishing FL into cross-device and cross-silo categories, inventing core algorithms such as FedAvg, and identifying the major problems:

network bottlenecks, heterogeneous data, personalization, and privacy, it essentially created the field [2], [5]. More importantly, it had questions concerning incentives, fairness, and evaluation—these being the core of Creaboost's architecture—that it didn't answer but rather left open.

Immature decentralized advertising protocols centered on impression tracking and token systems without machine learning. AdChain [8] introduced an Ethereum based registry for ad metadata, aiming to reduce fraud through on chain verification. However, it viewed impressions as isolated events without considering user preferences. Verasity [9] planned Proof of View (PoV) to confirm video watch time with cryptographic signatures, but relied on centralized oracles for validation.

The convergence of FL and blockchain gained momentum after 2021. FedCoin [10] developed a blockchain-based payment method for federated learning based on Shapley Value-based consensus, also known as PoSap, to fairly reward data owners with incentives

A separate line of research looked at incentive design. Ocean Protocol [11] created data marketplaces with compute to data, allowing models to run in secure environments without data leaving. While important for B2B applications, Ocean focused on enterprise datasets instead of consumer ad signals.

It was discovered that sharing gradients in FL was risky, but Niu et al. [12] proved that using pairwise masking with a re-signature approach was privacy-preserving while maintaining accuracy at 98.47%, 87.12%, and 65.24% for MNIST, FashionMNIST, and CIFAR-10 datasets, respectively. In contrast, Ali et al. [13] proved that FL-based incentive schemes face challenges in terms of reward sharing due to invisible hyperparameters and unverifiable data quality, making them more likely to be manipulated for malicious purposes.

In 2024, Tang et al. [14] found privacy and payment imbalance issues in FL and developed a continuous zero-determinant strategy to stabilize social welfare. Simulation results verified the incentive mechanism based on the CZD method could always attract high-accuracy data contributions with robust and stable results.

By themselves, these sources can only form a decentralized base for dealing substantial amounts of Creaboost. They do not simply provide the architecture or any way for dealing with the data heterogeneity, security threats, and privacy design but at the big time they do shed light on the identical potential of employing blockchain to reach true transparency, fairness, and as well as privacy in a hearty ad ecosystem.

4 Proposed Work

Creaboost is a decentralized platform that lives on the XDC blockchain and is designed to repair the current advertising and rewards problem that the platform has had for quite some time. The platform pays content creators moderately for the true engagement of their audience while utilizing federated learning to ensure user's complete privacy.
The platform is built around the following three main features:

1. Private Ad Targeting: A clever model operates directly on each creator's device, learning from likes, views, and shares. The model itself does not send your open data anywhere. It simply sends unknown updates from the model. These updates are merged to form one noticeable spheric model that itself knows ad preferences without always letting user privacy down.
2. Blockchain Powered Rewards: Our system of smart contracts on the blockchain is the XDC where we automate the creator payments. The contracts that we have in place track engagement, verify activity, and send rewards directly. The whole process is made transparent and trustworthy by Creaboost thus cutting off the middlemen, who are the main beneficiaries of the process, so that every transaction is secure, verifiable, and fair and also ensuring the trust of the users in the system.
3. Simple dApp Interface: Through a web app, creators can access the platform and connect their XDC wallet (such as XDCPay or MetaMask). After that, they can submit engagement data, manage ad-preferences, and claim their rewards. Each and every transaction is digitally signed and recorded on the blockchain so as to guarantee complete security and also authenticity.

By merging blockchain with a privacy-first AI, Creaboost is creating an advertising community that is more transparent, fair, and data-driven, which will be of great help both to the creators and to the advertisers. The system architecture of Creaboost is shown in the Fig. 1.

4.1 System Architecture

- Client Device: The intelligent model that supports users' phones or computers is what runs locally with the users. It figures out likes based on users' interaction with the content, but their personal information is never out of their devices.
- The Federated Learning Server: It can be thought of as the main conductor. It only gathers the anonymous updates (not the data) from the users' devices. It merges those updates in order to have one united global model that is more intelligent, hence the system can be extended without privacy being compromised.
- The Blockchain (XDC/Ethereum): This is the layer that provides the trust. Smart contracts that manage ad preferences in an automated manner, record engagement and, thus, most importantly, distribute rewards to creators are run by it.

- The Web App (Front-End): This is the straightforward interface which user use. It is the place where the user can log into the account, alter their preferences, look over their earnings, and keep track of their content's progress.

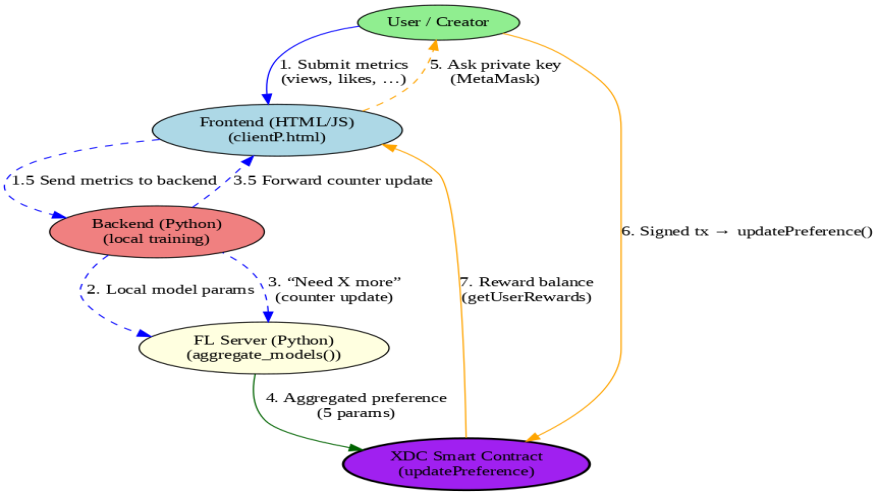


Fig. 1 Simplified Creaboost Architecture

4.2 Workflow

1. While users are browsing content and watching ads, their device keep a local model updated.
2. On receiving the anonymous update, the server incorporates the information into the global model.
3. Users' ad preferences are put on the blockchain through a secure transaction that only users can authorize with their private key.
4. Ultimately, the smart contracts keep a record of all the ad revenue and make the payments to the creators automatically. The whole procedure is open to everyone and can be checked at any time.

Pseudo-code of Workflow

1. User Submit Engagement: The user (or creator) opens the web app and submits their engagement data—such as views, likes, and shares.
   SubmitMetrics(views, likes, shares)
2. Local Training & Privacy: The app silently trains a small model on the user's device with the provided data. Only the anonymous model parameters are sent to our server — your raw data stays on the user's device.
   local_model_params = train_local_model(Metrics)
   send_to_server(local_model_params)

3. Server Aggregation: The Federated Learning server collects the user updates in a queue. It does not process them until it receives updates from a sufficient number of users. This aggregated global model is then sent to the server.
   If received_models < required_clients:
       notify_frontend("Waiting for more updates")
   endif
   AggregatedPreference = aggregate_models(local_model_params)
4. Connect your wallet (e.g., MetaMask or XDCPay) to the web app to sign this newly aggregated update. Thus, the user is authenticated.
   SignedTx = sign_transaction(updatePreference, AggregatedPreference)
5. Wrap it up with the chain: The smart contract, which is a part of the XDC blockchain and handles users' requests, gets the user's signed transaction and safely updates their ad preferences vault.
   SmartContract.updatePreference(SignedTx)
6. On-Chain Storage: The smart contract permanently stores users' new preferences on the blockchain.
7. Get Paid: The smart contract figures out user rewards based on how much he/she contributed and sends it to the user's wallet according to its evaluation. The user's new balance is then displayed by the web app.
   RewardBalance = getUserRewards(UserAddress)
   Display (RewardBalance)

4.3 Advantages of Proposed Work

- Privacy: Users' data always stays on their device. Federated learning is powerful in that sense of privacy.
- Transparency: All payouts are then managed by the permanent smart contracts. Users can see everything if they want.
- Fair Monetization: This method shatters the link to centralized ad giants, which means that creators are free to earn the real value that they deserve.
- Scalability: The architecture of the network enables unlimited expansion, and thus, more users and creators can be added without any bottlenecks.

5 Security Analysis

We have built the Creaboost platform with security at its very foundation. Our aim is to protect data and ensure every transaction is legitimate. We accomplished this by mixing the entire aspect of federated learning with the privacy first architecture. The following are the security features, which are covered in Creaboost.

1. Data Privacy in all sensible data remains on the device. This is used as an open model update, and not the open engagement data, which drastically reduces exposure, even if important server gets attacked.
2. XDC blockchain records every transaction and maneuver modification, thereby guaranteeing transparency and preventing frauds.
3. Performing sensitive tasks, such as issuing credential-based rewards, will require users to authenticate themselves first. Using this wallet-based identity negates the necessity of risky, centralized logins and thus the necessity of credential theft is lowered significantly.
4. Any time before information is being shipped off to the blockchain one needs to give it a digital signature with their private key. Even if a hacker were to intervene in the transaction, they will not be able to alter it or create a new one without the signature. This in turn gives the assurance that the data is genuine and saves anyone from fraud.
5. Protection Against Common Attacks includes
    - Man-in-the-Middle (MITM) Attack: Encrypted communication prevents third parties from intercepting, reading, or altering the data which is being transmitted.
    - Server Compromise Attack: Suppose that our server is hacked, in that case, the attackers will not be able to get hold of the valid raw data. What they would get are the anonymous model updates.
    - Sybil Attack: By connecting every user with a unique blockchain wallet, it becomes very hard for the perpetrator of the attack to create a large number of fake identities thus controlling the system.
    - Identity Spoofing: Public-key cryptography is what makes the genuine users' identities invulnerable. That is, no one can impersonate a genuine user without having access to his private key.
    - Data Tampering: The main point of the blockchain is that it puts strong measures in place to preclude data modifications after they have been verified. The network would reject any attempts of tampering automatically.
    - Data Privacy: By making sure that the genuine user's data is stored locally, we are able to provide privacy-first analytics. Data cannot be leaked if it is never sent.

6. The blockchain is the ultimate source of truth that we rely on to keep our records. To improve the operational speed, our backend database also keeps a fragment of the records. In the event of any interruption, we have strong rollback and sync mechanisms to make sure that the database and the blockchain are in full agreement.

6 Performance Analysis

6.1. Experimental Configuration

6.1.1 Artillery Core v2.0.19 - Quick Overview

Artillery Core v2.0.19 is a modern time advanced, Node.js-based load testing tool which was released in August 2024. It simulates a scenario of real users hitting your APIs, microservices, or websites to test the performance of the services under heavy traffic. Think of it as creating thousands of virtual pseudo users that interact with your app simultaneously to check how well it can handle the load. This provides a resourceful test for services before deployment. Artillery helps you in catching performance problems before users do. Instead of discovering your app crashes at 100 simultaneous real time users in production, you test with 1,000 virtual users in a safe environment first to get an idea of the working of the model.

6.1.2 Test Specifications

Here included in the test configuration were:

- ❖ Time: 60 seconds (six 10-second intervals).
- ❖ 302 Redirects: There are 1,800 virtual users in total (arrival rate: 30 people per second).
- ❖ Situations: Three user flows that are weighted here are as follows:
  - ➢ Only submit metrics were 34.5%.
  - ➢ Reward submission plus cheque here was 33%.
  - ➢ Submit, aggregate, update preference in this order then 32.5% is the complete workflow.
- ❖ Target: XDC Apothem Testnet-connected Flask server (127.0.0.1:5000)

6.1.3 Infrastructure

- Server: NVIDIA GTX 1660 Ti (6GB VRAM), Intel Core i7-9700K (8 cores at 3.6GHz), and 16GB DDR4 RAM
- Network: XDC Testnet
- Database: SQLite 3.42 (high-throughput operations in in-memory mode)
- Framework: PyTorch 2.0.1 (deep learning), accelerated with CUDA 11.8

6.2. Performance Metrics & Results

6.2.1 HTTP Response Analysis

In total Over 3,600 total requests processed during the 60-second test window:

- 200 OK (Success): 1,179 requests (32.8%) — This count of requests were Successful API interactions.
- 302 Redirects: 1,800 requests (50.0%) — This count of requests got Authentication flow redirects.
- 400 Bad Requests: 621 requests (17.2%) — This count falls under Input validation failures.

6.2.2 Response Time Breakdown

Table 1 shows the response time breakdown for the test.

Table 1. Response Time Analysis

Status Code	Min (ms)	Median (ms)	Mean (ms)	p95 (ms)	p99 (ms)	Max (ms)
2xx (Success)	0	16.9	25.8	67.4	94.6	128
3xx (Redirect)	0	10.9	18.4	58.6	76.0	95
4xx (Error)	303	459.5	565.1	925.4	3828.5	4513
Overall	0	19.9	115.1	561.2	889.1	4513

6.2.3 Key Observations

1. Successful responses (2xx) maintained sub-100ms latency at p99, demonstrating the true efficiency of the API processing.
2. Error responses (4xx) showed significantly higher latency (mean: 565.1ms), attributed so that it falls under comprehensive input validation routines.
3. Maximum amount of response time of 4.5 seconds was seen during simultaneous aggregation + blockchain write operations.

6.2.4 Throughput Analysis

Table 2. represents throughput with respect to user arrival rate.

Table 2. Request throughput scaled linearly with user arrival rate

Time Window	Request Rate (req/s)	Active VUsers	Cumulative Requests

0-10s	34	99	198
10-20s	34	130	458
20-30s	49	233	924
30-40s	62	301	1526
40-50s	77	378	2282
50-60s	89	437	3156
60-65s	103	222	3600

Average sustained throughput: 65 requests/second
Peak throughput: 103 requests/second (final 5-second burst).
Hence, overall, this represents 3.25% utilization of XDC's theoretical 2,000 TPS capacity, indicating a substantial headroom for horizontal scaling here.

6.2.5 User Session Analysis

Virtual user session lengths (1,800 completed sessions):

- Minimum: 2.7 ms (authentication-only session)
- Median: 83.9 ms (typical metric submission)
- Mean: 237.5 ms (includes aggregation wait time)
- p95: 742.6 ms (full workflow with blockchain write)
- p99: 1,107.9 ms (concurrent aggregation + high network load)
- Maximum: 4,528.8 ms (worst-case: 5 consecutive aggregations)

User sessions were completed with consistently low latency levels, with even complete blockchain workflows remaining well within acceptable limits.

7 Conclusion

Creaboost was created to address two major issues with advertisements which are invasions of privacy and exploitation of creators. Now with the help of its functionalities the problems of the users will definitely be reduced. In this proposed application, user with their own devices, can train a small model using actual statistics; no data ever leaves. Our server compiles the updates, adds a preference score to the XDC blockchain, and immediately pays the

creator according to their following five successful submissions. No intermediary. No monitoring is required, just pay rewards that are fair.

7.1 Future Extent

- Mobile App: Make the file clientP.html into a React Native application so that developers can submit from their mobile devices in a much smoother way.
- Real Users: To obtain actual engagement data, start a beta with more than 100 YouTubers to test the model with real life users.
- More Intelligent Incentives: For high engagement posts (e.g., 100k + views = 5 XDC), pay more.

Although it is not completely flawless yet, Creaboost is functional, real, and prepared to expand. We're creating something that creators will truly use, and have the motivation to keep making their good content.

Conflict of Interest Statement

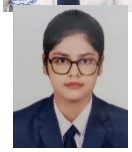
The authors declare no conflict of interest.

References

1. X. Li, Y. Lin, and Y. Zhang, "A privacy-preserving framework for advertising personalization incorporating federated learning and differential privacy," in *Proc. 2025 Int. Conf. Artificial Intelligence and Foundation Model (AIFM '25)*, ACM, 2026. https://doi.org/10.1145/3786709.3786710. (Conference Paper)
2. J, Liu, C. Chen, Y. Li, L. Sun, Y. Song, J. Zhou, B. Jing, and D. Dou, "Enhancing trust and privacy in distributed networks: a comprehensive survey on blockchain-based federated learning," *arXiv preprint arXiv:2403.19178*, 2024. https://doi.org/10.48550/arXiv.2403.19178. (Preprint)
3. Y. Tang, Y. Zhang, T. Niu, Z. Li, Z. Zhang, H. Chen, and L. Zhang, "A survey on blockchain-based federated learning: categorization, application and analysis," *Comput. Modeling Eng. Sci.*, vol. 139, no. 3, pp. 2451–2477, 2024. https://doi.org/10.32604/cmes.2024.030084. (Journal Article)
4. ZL. Teo, X. Zhang, Y. Yang, L. Jin, C. Zhang, S. S. J. Poh, W. Yu, Y. Chen, J. B. Jonas, Y. X. Wang, W. C. Wu, C. C. Lai, Y. Liu, R. S. M. Goh, and D. S. W. Ting, "Privacy-preserving technology using federated learning and blockchain in protecting against adversarial attacks for retinal imaging," *Ophthalmology*, 2024. https://doi.org/10.1016/j.ophtha.2024.10.017. (Journal Article)
5. DC. Nguyen, M. Ding, Q. V. Pham, P. N. Pathirana, L. B. Le, A. Seneviratne, J. Li, D. Niyato, and H. V. Poor, "Federated learning meets blockchain in edge computing: opportunities and challenges," *arXiv preprint arXiv:2104.01776*, 2021. https://doi.org/10.48550/arXiv.2104.01776. (Preprint)
6. Z. Jovanovic, Z. Hou, K. Biswas, and V. Muthukkumarasamy, "Robust integration of blockchain and explainable federated learning for automated credit scoring,"

Comput. Netw., 2024. https://doi.org/10.1016/j.comnet.2024.110303. (Journal Article)
7. M. Chakraborty and A. Khekade, "XDC gasless subnet: gasless subnet staking dApp for XDC network," *ResearchGate*, 2024. https://doi.org/10.13140/RG.2.2.12643.77600. (Technical Report)
8. M. Goldin, A. Soleimani, and J. Young, *The adchain registry*, Technical White Paper, May 31, 2017. (Technical Report)
9. K. Khan, "Smart contracts on blockchain for microtransactions and transparent revenue sharing in content monetization," *Int. J. Multidiscip. Res. Publ.*, vol. 6, no. 7, pp. 149–155, 2024. (Journal Article)
10. Y. Liu, Z. Ai, S. Sun, S. Zhang, Z. Liu, and H. Yu, "Fedcoin: A peer-to-peer payment system for federated learning," in *Federated Learning: Privacy and Incentive*, Cham: Springer Int. Publ., Nov. 26, 2020, pp. 125–138. (Book Chapter)
11. T. McConaghy, "Ocean protocol: tools for the web3 data economy," in *Handbook on Blockchain*, Cham: Springer Int. Publ., Nov. 4, 2022, pp. 505–539. (Book Chapter)
12. S. Niu, X. Zhou, N. Wang, W. Kong, and L. Chen, "Privacy-preserving and efficient verifiable federated learning scheme based on proxy re-signature," *Expert Syst. Appl.*, 2025. https://doi.org/10.1016/j.eswa.2025.128422. (Journal Article)
13. A. Ali, I. Ilahi, A. Qayyum, I. Mohammed, A. Al-Fuqaha, and J. Qadir, "A systematic review of federated learning incentive mechanisms and associated security challenges," *Comput. Sci. Rev.*, 2023. https://doi.org/10.1016/j.cosrev.2023.100593. (Journal Article)
14. C. Tang, B. Yang, X. Xie, G. R. Chen, M. A. A. Al-Qaness, and Y. Liu, "An incentive mechanism for federated learning: a continuous zero-determinant strategy approach," *IEEE/CAA J. Autom. Sinica*, vol. 11, no. 1, pp. 88–102, 2024. https://doi.org/10.1109/JAS.2023.123828. (Journal Article)

Ritesh Kumar Shaw is a Computer Science undergraduate (2026) with interests in Artificial Intelligence, Machine Learning, federated learning, and blockchain. He works on computer vision and intelligent retrieval systems, focusing on real-world applications.



Safiya Ahmed is a Computer Science undergraduate (2026) specializing in AI & ML with interests in machine learning, artificial intelligence, cybersecurity, blockchain and full stack development. She currently works as a Risk and Regulatory Intern at PwC, gaining experience in real-world industry applications.

Stuti Sinha is a final undergduate, pursuing B-Tech in University of engineering and management, Kolkata. She is keen about all fields of technology, especially development and artificial intelligence and machine learning, and is currently working as an intern at Kyptronix LLP, gaining experience from real life projects that focus on helping businesses integrate all suitable forms of technology.

Subhangi Chatterjee is a Computer Science undergraduate (2026) specializing in AI/ML, with strong interests in Artificial Intelligence, Machine Learning, federated learning, and blockchain. She currently works as a Machine Learning Intern at Sasken Technologies Limited, gaining experience in real world intelligent voice systems, computer vision pipelines, and AI-driven financial platforms, focusing on real-world, performance-driven applications.