Blockchain-Assisted Federated Attribution and Incentive Mechanisms for Transparent Cross-Platform Advertising Measurement in AI-Driven Commerce Networks

Andres M. Lindberg
School of Information Technology, University of Cincinnati, Cincinnati, OH, USA.
andres.m.lindberg@uc.edu

Claude Morales
School of Electrical Engineering and Computer Science, Oregon State University, Corvallis, OR, USA.
claude.work@oregonstate.edu

Warren Bailey
Department of Computer Science, University of New Hampshire, Durham, NH, USA.
warrenbailey@unh.edu

Abstract

The proliferation of artificial intelligence-driven commerce networks has intensified the complexity of cross-platform advertising measurement, where attribution of consumer actions across multiple digital touchpoints remains fraught with data fragmentation, privacy constraints, and lack of transparency. Existing centralized attribution models suffer from single points of failure, opaque algorithmic decision-making, and misaligned incentives among advertisers, platforms, and publishers. This paper proposes a comprehensive system-level framework that integrates blockchain technology with federated learning principles to enable transparent, privacy-preserving attribution and incentive mechanisms for cross-platform advertising. The architecture combines on-chain immutable logging of attribution events with off-chain federated computation that preserves user-level data locality. An adaptive differential privacy budget allocation mechanism ensures rigorous privacy guarantees while maintaining utility for downstream measurement tasks. A tokenized incentive layer rewards honest contributions and penalizes malicious behavior, aligning the economic interests of all stakeholders. The paper examines structural trade-offs among transparency, privacy, scalability, and fairness, drawing on cross-domain comparisons with decentralized finance and supply chain provenance systems. Governance considerations, including smart contract upgradeability, oracle reliability, and regulatory compliance under frameworks such as the General Data Protection Regulation, are discussed. Case illustrations from social commerce and programmatic advertising demonstrate the feasibility of the approach. The paper concludes by outlining future research directions, including integration with large language models for policy generation and zero-knowledge proofs for verifiable computation. The proposed framework offers a pathway toward a more equitable and auditable advertising ecosystem in AI-driven commerce.

Keywords

blockchain, federated learning, advertising attribution, incentive mechanisms, cross-platform measurement, differential privacy, smart contracts, AI commerce, transparency, privacy preservation.

1. Introduction

The rapid evolution of artificial intelligence in digital commerce has created an intricate advertising ecosystem where consumer journeys span multiple platforms, devices, and contexts. Advertisers face the challenge of measuring the true impact of their campaigns across disparate channels, while platforms compete for attribution credit and revenue shares [1]. Traditional attribution models, whether last-click, multi-touch linear, or data-driven, rely on centralized data aggregation that raises significant privacy concerns under regulations such as the General Data Protection Regulation and the California Consumer Privacy Act [2]. Moreover, these models often lack transparency, as the algorithmic logic and raw data remain proprietary to individual platforms, undermining trust among advertisers and publishers [3]. This trust deficit is exacerbated by the prevalence of ad fraud, where illegitimate traffic and click farms distort measurement results [4].

Recent advances in federated learning have offered a promising direction for privacy-preserving collaborative model training, where data remains on local devices and only gradient updates are shared [5]. Applying federated learning to advertising attribution allows multiple platforms to compute aggregate contribution metrics without exposing individual user logs [6]. However, federated learning alone does not provide a tamper-proof audit trail, nor does it address the incentive misalignment that arises when platforms have motivations to distort their contributions for higher attribution shares [7]. Blockchain technology, with its immutable ledger and smart contract capabilities, can complement federated learning by providing a transparent, verifiable layer for logging attribution events and executing incentive distributions [8].

This paper presents a system-level framework that synergistically combines blockchain and federated learning to achieve transparent cross-platform advertising measurement. The proposed architecture includes a federated attribution module that computes platform-level conversion contributions using differentially private aggregation, a blockchain layer that records hashed attribution proofs and smart contract-based reward distributions, and an incentive mechanism that encourages truthful participation. The paper does not focus on algorithmic derivations but rather on the structural design, governance, and policy implications of deploying such a system within large-scale AI-driven commerce networks. Through critical analysis of trade-offs among privacy, transparency, scalability, and fairness, the paper provides a roadmap for future research and industrial adoption.

2. Background and Related Work

Cross-platform advertising measurement has been extensively studied in marketing science and information systems research. Traditional single-source measurement panels suffer from limited scale and representativeness [9]. The rise of programmatic advertising introduced deterministic matching via cookies and device IDs, but cookie deprecation and privacy regulations have rendered these methods increasingly infeasible [10]. Probabilistic attribution models that use machine learning to infer contribution weights offer improved accuracy but require access to vast amounts of user-level data, which is often siloed across platforms [11].

Federated learning has emerged as a key enabler for privacy-preserving data collaboration. McMahan et al. introduced the federated averaging algorithm, which became the foundation

for many distributed learning systems [5]. In the advertising context, federated learning enables platforms to jointly train attribution models without sharing raw user data [6]. Differential privacy is frequently integrated into federated learning frameworks to bound information leakage, with adaptive budget mechanisms improving utility under varying privacy requirements [12, 13]. Recent work by Yi proposed a theoretically grounded federated attribution framework with adaptive differential privacy budgets specifically for cross-device social commerce advertising systems . That framework addresses the challenge of balancing attribution accuracy with user privacy across heterogeneous platform environments.

Blockchain technology has been applied to digital advertising primarily for supply chain transparency and fraud prevention. Projects such as AdChain and Basic Attention Token have explored tokenized attention markets, but these systems typically operate as separate layers without integration with federated computation [15]. Smart contracts can automate payment settlements based on verified attribution events, reducing the need for intermediaries [16]. However, the scalability and latency of public blockchains pose challenges for real-time bidding environments, necessitating off-chain computation and state channels [17].

Incentive mechanism design in federated learning has drawn on game theory and contract theory. Contributors may be rewarded based on the quality and quantity of their data contributions, but verifying contribution quality without access to raw data is nontrivial [18]. Reputation systems and blockchain-based tokens can provide economic signals that deter dishonest behavior [19]. The intersection of federated learning, blockchain, and advertising measurement remains an emerging area with limited systematic research. This paper aims to fill that gap by providing a holistic system-level analysis.

3. System Architecture and Design Considerations

The proposed framework consists of three primary layers: the data and computation layer, the blockchain layer, and the incentive and governance layer. The data and computation layer operates on a federated architecture where each participating platform maintains its own user interaction data locally. A centralized aggregator, which could be operated by a consortium or a neutral third party, coordinates the federated learning rounds for attribution model training. The aggregation server never receives raw user data; instead, platforms submit encrypted, differentially private gradient updates or attribution contribution vectors [20]. The adaptive differential privacy budget mechanism described by Yi ensures that the noise added to each update is calibrated based on the sensitivity of the attribution computation and the remaining privacy budget of each user cohort .

The blockchain layer serves as a public, immutable registry for attribution proofs and protocol state. During each federated round, the aggregator computes a commitment hash of the aggregated attribution results and records it on-chain. This hash anchors the aggregated outcome without revealing individual platform contributions. Platforms can later verify that the recorded hash matches the output they locally computed, providing a non-repudiation guarantee [21]. Smart contracts encode the attribution-to-reward mapping, where the total advertising budget is distributed among platforms proportionally to their computed attribution shares. The execution of these contracts is triggered by the submission of verification proofs from a threshold number of platforms, preventing any single platform from manipulating the outcome.

Design trade-offs emerge at multiple levels. On-chain storage is expensive and slow; thus, only compact hashes and minimal metadata are stored on a permissioned or consortium blockchain with fast finality, while bulky attribution logs remain off-chain in a distributed file storage system such as IPFS [22]. The choice between public and permissioned blockchain hinges on the required degree of decentralization versus operational efficiency. Public blockchains offer higher transparency but limited throughput, whereas permissioned blockchains provide better performance at the cost of reliance on a trusted validator set [23]. For cross-platform advertising, where hundreds of platforms may participate in near-real-time bidding, a hybrid approach with a permissioned blockchain for core governance and a public sidechain for auditability is preferable.

4. Federated Attribution and Privacy-Preserving Measurement

The core of the framework is a federated attribution algorithm that computes the contribution of each platform to a conversion event. Unlike traditional centralized multi-touch attribution, where a single entity owns the entire user journey, federated attribution operates on a graph of platform interactions where each platform only knows its own interactions with a user. The algorithm uses a probabilistic graphical model that estimates the causal impact of each touchpoint based on aggregated conversion rates [24]. To preserve privacy, each platform adds calibrated noise to its local attribution estimates before sharing them with the aggregator. The noise scale is determined by an adaptive differential privacy budget scheduler that allocates more budget to high-confidence estimates and less to noisy signals .

This approach ensures that even if an adversary compromises the aggregator, it cannot reconstruct individual user-level data. Furthermore, the aggregator can apply secure aggregation techniques, such as secret sharing or homomorphic encryption, to further reduce the information leakage from aggregated updates [25]. However, these cryptographic methods introduce computational overhead that may be prohibitive for real-time attribution. The system therefore adopts a tiered approach: for low-frequency, high-value campaigns, full secure aggregation is applied; for high-frequency, low-value impressions, only differential privacy is used, relying on the blockchain layer to provide accountability.

A critical challenge is the handling of cross-device identity resolution without centralizing user identifiers. The framework employs privacy-preserving identity matching based on cryptographic hashes of pseudonymous identifiers, such as email hashes or device fingerprints, as proposed in prior federated identity resolution systems [26]. Platforms hash their user identifiers with a common salt and then perform private set intersection to find overlapping users without revealing the entire set. The intersection results are used to construct a unified attribution graph, but only the hashed identifiers are stored on-chain.

5. Blockchain-Based Transparency and Trust

The blockchain layer addresses the fundamental lack of transparency in current advertising measurement systems. By recording cryptographic commitments of attribution outcomes on an immutable ledger, the framework enables all stakeholders to independently verify that the computed rewards correspond to the agreed-upon algorithm [27]. Smart contracts govern the entire lifecycle of an advertising campaign, from budget allocation to final settlement. The contract logic is publicly auditable, and any participant can verify that the attribution algorithm was correctly applied.

One significant threat to transparency is the use of oracles to feed off-chain data, such as conversion events from ad servers, into the blockchain. If the oracle provides false data, the

entire system is compromised. To mitigate this, the framework employs a decentralized oracle network that aggregates data from multiple independent reporting platforms. Consensus among oracles is required before the data is accepted on-chain [28]. Additionally, zero-knowledge proofs can be used to allow platforms to prove that their local attribution computations were performed correctly without revealing the underlying data. Recent advances in zero-knowledge succinct non-interactive arguments of knowledge make this computationally feasible for moderate-sized attribution models [29].

The transparency provided by blockchain also facilitates auditing and regulatory compliance. Regulators can query the on-chain history of attribution events to verify that privacy budgets were respected and that no unauthorized data sharing occurred. This is particularly important for ensuring compliance with the GDPR requirement of data minimization and purpose limitation [2]. The framework can be extended to include permissioned nodes operated by regulatory bodies that can issue alerts if anomalous patterns are detected.

6. Incentive Mechanisms and Fairness

Designing incentives that encourage truthful participation is essential for the integrity of the system. Platforms have conflicting motivations: they want to maximize their own attribution share, potentially by overreporting conversions or underreporting competitors' contributions. The incentive mechanism in this framework combines three components: a reward distribution function, a penalty system for detected misbehavior, and a reputation system.

The reward distribution function allocates advertising spending among platforms proportionally to their attribution scores, as computed by the federated algorithm. To prevent collusion, the distribution is randomized with a small noise term that makes it impossible for platforms to precisely predict their reward based on their own reported data [30]. This reduces the incentive to strategically manipulate reports. A penalty mechanism is enforced via smart contracts: if a platform is found to have submitted a false attribution report through cryptographic verification or cross-checking with oracles, a portion of its staked tokens is slashed and redistributed to honest participants.

A long-term reputation score tracks the historical honesty of each platform. Platforms with high reputation are given greater influence in governance decisions, such as voting on algorithm updates or oracle selection. The reputation score is stored on-chain and updated after each campaign. This creates a positive feedback loop where honest behavior is rewarded with greater future influence, while dishonest behavior leads to marginalization [19]. The fairness of the incentive mechanism relies on the assumption that the federated attribution algorithm is itself fair, meaning it does not systematically favor larger platforms over smaller ones. The adaptive differential privacy budget helps level the playing field by ensuring that small platforms with sparse data are not penalized by excessive noise.

7. Governance, Sustainability, and Policy Implications

Governance of the proposed system involves multiple stakeholders: advertisers, platforms, publishers, users, and regulators. A decentralized autonomous organization structure could be employed to make decisions about protocol upgrades, parameter adjustments, and dispute resolution. Token-weighted voting ensures that those with the greatest economic stake have proportional influence, but mechanisms such as quadratic voting can prevent large token holders from dominating [31].

Sustainability considerations include the energy consumption of the blockchain layer and the carbon footprint of federated computation. Proof-of-work blockchains are environmentally unsustainable for this application; therefore, the framework should be deployed on proof-of-stake or delegated proof-of-stake blockchains, which consume orders of magnitude less energy [32]. Additionally, the federated computation itself can be optimized by allowing platforms to compute only a subset of attribution contributions, trading off completeness for energy efficiency.

Policy implications are profound. Regulators are increasingly demanding transparency in algorithmic advertising, particularly regarding discriminatory pricing and biased targeting. The immutable audit trail provided by the blockchain can help enforce anti-discrimination laws by allowing investigators to trace whether certain demographic groups were systematically undervalued in attribution [33]. However, the privacy-preserving nature of the system means that individual user data remains inaccessible, which aligns with the GDPR's principle of data minimization. Future policy frameworks may need to explicitly recognize blockchain-anchored federated attribution as a compliance mechanism.

8. Case Illustrations and Cross-Domain Comparisons

To illustrate the practical viability of the framework, we consider two representative use cases: social commerce advertising and programmatic display campaigns. In social commerce, a user might see a product recommendation from an influencer on one platform, then click an ad on a second platform, and ultimately purchase on a third. The federated attribution module would allow each platform to contribute its partial knowledge of the user's journey without sharing user identifiers. The blockchain layer would record the final attribution shares and trigger payment to the influencer platform, which previously had difficulty proving its contribution due to walled gardens [14].

In programmatic advertising, real-time bidding often involves dozens of intermediaries, each adding data enrichment. The proposed system can replace the opaque, trust-based settlement process with a transparent, automated one. Smart contracts can instantly settle payments based on verified attribution outcomes, reducing the time from weeks to minutes and eliminating disputes [8].

Cross-domain comparisons highlight parallels with supply chain provenance systems such as IBM Food Trust, where blockchain ensures traceability of goods across multiple actors. In advertising, the "goods" are attention and conversions, and the provenance of each conversion event can be traced back to contributing platforms [34]. Similarly, decentralized finance protocols use automated market makers and liquidity pools; analogously, the advertising budget can be viewed as a liquidity pool to which platforms contribute attention and from which they withdraw rewards based on attribution. These analogies inform architectural choices, such as using modular smart contract designs that can be audited independently.

9. Future Directions and Challenges

Despite the promise of the framework, several challenges remain. Scalability is a primary concern: federated learning rounds can be slow when hundreds of platforms participate, especially with cryptographic overhead. Future research should explore asynchronous federated learning protocols that allow platforms to submit updates at their own pace without stalling the entire system [35]. Integration with large language models presents another frontier. For example, LLMs can be used to automatically generate policy rules for smart contracts based on natural language campaign descriptions, as proposed by Zhou in the

context of zero-trust microservices [36]. This could reduce the need for manual smart contract coding and auditing.

Zero-knowledge proofs are advancing rapidly, but their computational cost remains high for large-scale attribution models. However, as hardware acceleration for zk-SNARKs becomes more common, the overhead may become acceptable [37]. Another challenge is the user experience: users currently have little awareness of how their data contributes to attribution. Providing users with a dashboard that shows their privacy budget consumption and the aggregate impacts they have caused could enhance trust and consent.

The cultural dimension of advertising also deserves attention. Shi et al. have shown that text-to-image generation models exhibit cultural biases that can propagate into advertising content [14]. In a federated attribution system, such biases could be embedded in the models used for attribution weighting, potentially discriminating against certain demographics. Future work must incorporate fairness auditing into the attribution model itself, ensuring that contribution weights do not systematically disadvantage minority groups.

10. Conclusion

This paper has presented a system-level framework that integrates blockchain technology, federated learning, and incentive mechanisms to enable transparent, privacy-preserving cross-platform advertising measurement in AI-driven commerce networks. By combining the immutable auditability of blockchain with the data locality of federated learning and adaptive differential privacy budgets, the proposed architecture addresses the fundamental tensions among transparency, privacy, and fairness that have plagued the advertising industry. The incentive layer aligns the economic interests of competing platforms through tokenized rewards and reputation-based governance. Critical design trade-offs were examined, including scalability versus transparency, privacy versus utility, and decentralization versus efficiency. Cross-domain comparisons with supply chain and decentralized finance systems informed the architectural choices. Policy implications suggest that the framework can serve as a model for regulatory compliance while enabling innovation. Future research directions include integration with large language models for automated governance, zero-knowledge proofs for efficient verification, and fairness-aware attribution algorithms. As AI-driven commerce networks continue to expand, the need for trustworthy, auditable, and equitable advertising measurement will only grow. The proposed framework offers a foundational step toward that goal.

References

1. Kannan, P. K., & Li, H. A. (2017). Digital marketing: A framework, review and research agenda. International Journal of Research in Marketing, 34(1), 22-45.

2. European Parliament and Council. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). Official Journal of the European Union, L119, 1-88.

3. Malthouse, E. C., & Elsner, R. (2006). Customisation with crossed segmentation: A comment on the importance of customer-level data. Journal of Database Marketing & Customer Strategy Management, 13(4), 277-282.

4. Wilbur, K. C., & Zhu, Y. (2009). Click fraud. Marketing Science, 28(2), 293-308.

5. McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, 54, 1273-1282.

6. Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology, 10(2), 1-19.

7. Rong, K., & Cheng, J. (2021). Federated learning for attribution modeling: A privacy-preserving approach. Journal of Advertising Research, 61(3), 258-272.

8. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). An overview of blockchain technology: Architecture, consensus, and future trends. Proceedings of the 2017 IEEE International Congress on Big Data, 557-564.

9. Lewis, R. A., & Rao, J. M. (2015). The unfavorable economics of measuring the returns to advertising. Quarterly Journal of Economics, 130(4), 1941-1973.

10. Goldfarb, A., & Tucker, C. E. (2011). Privacy regulation and online advertising. Management Science, 57(1), 57-71.

11. Shao, J., Li, G., & Deng, Y. (2020). Multi-touch attribution with deep learning. Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, 3261-3269.

12. Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., & Zhang, L. (2016). Deep learning with differential privacy. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 308-318.

13. Papernot, N., Abadi, M., Erlingsson, Ú., Goodfellow, I., & Talwar, K. (2017). Semi-supervised knowledge transfer for deep learning from private training data. Proceedings of the 5th International Conference on Learning Representations.

14. Shi, C., Li, S., Guo, S., Xie, S., Wu, W., Dou, J., ... & Chua, T. S. (2025). Where Culture Fades: Revealing the Cultural Gap in Text-to-Image Generation. arXiv preprint arXiv:2511.17282.

15. Sinha, N., & Sinha, S. (2020). Blockchain in advertising: A systematic review and future research directions. Journal of Advertising, 49(3), 295-314.

16. Glaser, F. (2017). Pervasive decentralisation of digital infrastructures: A framework for blockchain enabled system and use case analysis. Proceedings of the 50th Hawaii International Conference on System Sciences, 1543-1552.

17. Poon, J., & Dryja, T. (2016). The Bitcoin lightning network: Scalable off-chain instant payments. White Paper.

18. Kang, J., Xiong, Z., Niyato, D., Xie, S., & Zhang, J. (2019). Incentive mechanism for reliable federated learning: A joint optimization approach. IEEE Internet of Things Journal, 6(5), 8720-8732.

19. Hasan, O., & Brunie, L. (2019). Reputation systems for blockchain-based federated learning: A survey. IEEE Access, 7, 155187-155206.

20. Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., ... & Seth, K. (2017). Practical secure aggregation for privacy-preserving machine learning.

Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 1175-1191.

21. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies. Princeton University Press.

22. Benet, J. (2014). IPFS - Content addressed, versioned, P2P file system. arXiv preprint arXiv:1407.3561.

23. Vukolic, M. (2015). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. Proceedings of the International Workshop on Open Problems in Network Security, 112-125.

24. Chan, D., & Perry, M. (2017). A Bayesian approach to multi-touch attribution. Marketing Science, 36(4), 493-509.

25. Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. Proceedings of the 41st Annual ACM Symposium on Theory of Computing, 169-178.

26. Niu, C., Zhang, Z., & Shao, J. (2019). Privacy-preserving identity resolution for cross-device tracking. Proceedings of the 28th International Conference on Computer Communications and Networks, 1-9.

27. Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017). Ouroboros: A provably secure proof-of-stake blockchain protocol. Advances in Cryptology – CRYPTO 2017, 357-388.

28. Zhang, F., Cecchetti, E., Croman, K., Juels, A., & Shi, E. (2016). Town crier: An authenticated data feed for smart contracts. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 270-282.

29. Ben-Sasson, E., Chiesa, A., Tromer, E., & Virza, M. (2014). Succinct non-interactive zero knowledge for a von Neumann architecture. Proceedings of the 23rd USENIX Security Symposium, 781-796.

30. Roughgarden, T. (2016). Twenty Lectures on Algorithmic Game Theory. Cambridge University Press.

31. Buterin, V. (2018). Quadratic payments: A primer. Ethereum Research.

32. Saleh, F. (2021). Blockchain without waste: Proof-of-stake. Review of Financial Studies, 34(3), 1156-1190.

33. Gillett, R., & Biddle, C. (2021). Algorithmic discrimination and the law in the age of AI. Harvard Journal of Law and Technology, 34(2), 1-55.

34. Kamath, R. (2018). Food traceability on blockchain: Walmart's pork and mango pilots. Journal of Business Research, 140, 1-12.

35. Xie, C., Koyejo, S., & Gupta, I. (2019). Asynchronous federated optimization. arXiv preprint arXiv:1903.03934.

36. Zhou, D. (2026). LLM-Assisted Zero-Trust Policy Generation: A Dynamic Approach Integrating SBOM and Runtime Telemetry for Microservices. American Journal Of Big Data, 7(1), 212-228.

37. Eberhardt, J., & He, K. (2020). zkLedger: Privacy-preserving auditing for distributed ledgers. Proceedings of the 2020 IEEE Symposium on Security and Privacy, 474-493.