International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 11 | Nov - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Blockchain Based Ad Revenue System

Hari Om Anand[1], Kanishk Chaudhary[2], Md. Shayan Tanweer[3], Swarnim[4], Ganashree R.[5]

[1,2,3,4] *UG Student Department of Computer Science and Engineering (Internet of Things), Sir M. Visvesvaraya Institute of Technology, Bengaluru, Karnataka, India*

[5] *Assistant Professor of Department of Computer Science and Engineering (Internet Of Things), Sir M. Visvesvaraya Institute of Technology, Bengaluru, Karnataka, India*

Abstract-The rapid growth of digital advertising has highlighted persistent issues related to transparency, user privacy, and fair revenue distribution. Traditional ad-based platforms often operate with opaque data practices, centralized control, and limited incentives for users whose attention drives the ecosystem. This research project proposes a **Blockchain-Based Ad Revenue System** designed to create a decentralized, transparent, and privacy-preserving advertising model. The system utilizes blockchain smart contracts to record ad interactions, verify user engagement, and automate reward distribution without relying on intermediaries. By integrating user profiles, advertiser inputs, and ad-view verification mechanisms, the platform ensures that users are compensated fairly for engagement while advertisers gain verifiable insights into campaign performance. The project demonstrates how decentralization, immutability, and cryptographic security can enhance trust and efficiency in digital advertising. The findings show that the proposed system can significantly reduce fraud, increase accountability, and promote an ethical, user-centric advertising ecosystem.

Index Terms: Blockchain Blockchain Technology, Smart Contracts, Digital Advertising, Ad Revenue Model, Decentralized Applications (DApps), User Engagement Verification, Cryptographic Security, Transparency, Reward Distribution .

1. INTRODUCTION

Digital advertising has become the backbone of the modern internet economy, enabling platforms to offer free services while monetizing user attention. However, the traditional advertising ecosystem is heavily centralized, dominated by intermediaries who control data, dictate revenue distribution, and influence how advertisements reach end users. This centralized structure introduces several longstanding challenges, including lack of transparency, ad fraud, intrusive data collection practices, and inadequate compensation for users who actively contribute to engagement metrics. As a result, user trust in online advertising continues to decline, while advertisers face increasing difficulty in ensuring that their investments lead to genuine and measurable engagement. attacks . Phishing attacks primarily use email messages with deceptive content that appears to come from a trusted legitimate source, although multimedia messaging service text messages are also used. This research paper introduces a **Blockchain-Based Ad Revenue System** that aims to shift the digital advertising paradigm from a platform-centric model to a **user-centric and trust-driven ecosystem**. The proposed system verifies ad views using blockchain mechanisms, ensures fair reward distribution through smart contracts, and preserves user privacy by eliminating the need for invasive tracking methods.

2. Threat Landscape and Requirements

The digital advertising ecosystem faces a wide range of security and operational threats due to its highly centralized structure, heavy dependence on user data, and susceptibility to manipulation. One of the most significant challenges is ad fraud, where malicious actors generate fake impressions, clicks, or conversions using automated bots or fabricated identities. This not only inflates engagement metrics but also results in substantial financial losses for advertisers who are unable to verify the authenticity of user interactions. In addition to fraud, data privacy concerns are growing due to the widespread practice of user tracking and large-scale data collection. Traditional advertising platforms store vast amounts of personal information on centralized servers, making them vulnerable to unauthorized access, data breaches, and misuse of user behavior insights. Such practices often violate privacy expectations and regulatory frameworks, further eroding user trust. Smart contract vulnerabilities represent another crucial threat within blockchain-based systems. While smart contracts ensure transparency and automation, any flaw in their design or coding can lead to exploits, financial loss, or unintended system behavior. Issues such as reentrancy attacks, logic errors, and improper access control can compromise the entire reward distribution mechanism. Additionally, blockchain networks themselves are not immune to threats. For instance, attackers may launch denial-of-service attacks on application servers or attempt a 51% attack to manipulate on-chain data. Even front-running attacks, where malicious actors exploit transaction visibility in the mempool, pose a risk to fairness within decentralized applications.

3. LITREATURE SURVEY

The evolution of digital advertising has been widely documented in academic and industrial research, with early studies emphasizing the dominance of centralized platforms such as Google and Facebook in managing ad delivery, user targeting,

and revenue distribution. These studies highlight that while centralized advertising models offer scalability and convenience, they also suffer from issues of opacity, limited accountability, and a lack of user empowerment. Research conducted over the past decade consistently points to widespread ad fraud, with reports estimating billions of dollars lost annually due to invalid traffic, bot-generated clicks, and fraudulent impressions. Several works have analyzed fraud detection algorithms and machine-learning techniques used by ad networks, yet findings reveal that many attacks exploit the centralization and asymmetry of information inherent in traditional systems. Another strand of literature investigates the application of smart contracts in trustless environments. Scholars have highlighted how smart contracts eliminate intermediaries, reduce operational overhead, and enforce rules automatically without human intervention. Studies also discuss the importance of secure smart contract development practices, citing vulnerabilities that have previously led to exploits and network-wide failures. Alongside this, researchers have examined decentralized identity frameworks and anti-Sybil mechanisms, which are crucial in distinguishing real users from automated or malicious entities in incentive-driven ecosystems.

4. Blockchain-Based Ad Revenue System Architecture

A blockchain-based ad revenue system consists of interconnected components responsible for ad delivery, engagement verification, reward distribution, identity management, security, and analytics. The architecture emphasizes decentralization, transparency, and trust, ensuring that the flow of advertisements, user interactions, and reward mechanisms occurs without reliance on a central authority. Each layer contributes to transforming raw engagement data into verifiable on-chain records, maximizing accountability while minimizing fraud and manipulation. The system is designed to support modular expansion, enabling integration of new ad formats, advanced verification techniques, or additional blockchain protocols as the ecosystem evolves. This modularity enhances long-term scalability and future readiness.

4.1 Client Interaction and Interface Layer

The client interaction layer forms the user-facing component of the system, enabling both users and advertisers to access functionalities through web or mobile applications. Users can log in, view advertisements, connect their wallets, and track their earned rewards. Advertisers interact through a dedicated dashboard that allows them to create campaigns, set targeting parameters, allocate budgets, and monitor real-time performance metrics. This layer focuses on ensuring a seamless user experience while facilitating secure wallet integration and authenticated interactions. By abstracting underlying blockchain complexity, the interface layer provides an accessible and intuitive environment for all stakeholders.

4.2 Backend Services and Off-Chain Processing

The backend layer acts as the operational core responsible for coordinating communication between the user interface and the blockchain. It handles business logic such as campaign validation, user session management, ad selection algorithms, and preliminary verification of engagement events. Since blockchain operations are computationally expensive, the backend performs lightweight off-chain processing, filtering invalid or suspicious events before submitting final records to smart contracts. This layer also manages storage of non-sensitive data, including ad metadata, media assets, and system logs, using relational or NoSQL databases. By balancing off-chain efficiency with on-chain security, the backend ensures smooth system performance.

4.3 Blockchain Network and Smart Contract Framework

The blockchain layer serves as the foundation of trust within the system, providing immutable, tamper-resistant storage for critical interactions such as ad impressions, verified clicks, and reward transactions. Smart contracts automate the lifecycle of advertising campaigns, from creation and funding to engagement verification and reward distribution. The campaign contract records advertiser budgets and parameters, while the engagement contract logs verified user interactions and prevents duplication. A dedicated reward contract ensures that users are compensated fairly based on on-chain evidence of their participation. If a custom token is used, a token contract manages minting, supply constraints, and wallet balances. This automated smart contract ecosystem reduces manual intervention and guarantees unbiased, real-time execution of system rules.

4.4 Engagement Verification and Anti-Fraud Engine

To address the prevalence of bot traffic and fraudulent activity in digital advertising, the system includes a specialized verification engine that scrutinizes user interactions before they are recorded on the blockchain. This engine applies hybrid techniques such as device fingerprinting, session analysis, rate-limit checks, and human validation tasks like CAPTCHAs. It identifies anomalous patterns, filters automated behavior, and ensures that only legitimate impressions and clicks are forwarded for on-chain logging. By combining behavioural analysis with technical verification, the anti-fraud layer minimizes false engagements and strengthens advertiser confidence in the accuracy of campaign performance metrics.

4.5 Identity, Wallet, and Security Management

Identity and wallet management play a crucial role in maintaining a secure and privacy-preserving environment. Users and advertisers authenticate using decentralized wallets, ensuring that all system interactions are cryptographically verified and traceable without exposing personal data. The

system enforces strict security controls, including encrypted communication channels, access validation, and protection against common web threats. Privacy considerations are addressed through pseudonymization of identities, minimal personal data collection, and adherence to global data protection guidelines. This security-focused approach safeguards the system from attacks such as Sybil attacks, account spoofing, and unauthorized access, ensuring reliable participation across all stakeholders.

5. Methodologies and Techniques

5.1 Smart Contract-Based Automation

Smart contracts serve as the operational backbone of the system, enabling trustless automation of core advertising functions. They govern essential processes such as advertiser campaign creation, budget allocation, impression logging, and reward distribution without requiring human intervention. These contracts enforce rules transparently, ensuring that engagement data is immutable and rewards are distributed based on verifiable events. Techniques such as event-driven triggers, secure modifiers, and gas-optimized logic ensure efficient execution. The deterministic nature of smart contracts eliminates ambiguity, allowing advertisers and users to rely on verifiable, rule-based outcomes.

5.2 Decentralized Data Recording and Ledger Integrity

To ensure that engagement records cannot be altered or manipulated, the system employs blockchain-based ledger techniques that guarantee immutability, transparency, and decentralized consensus. Ad impressions, verified clicks, and reward transactions are stored on the blockchain, providing a tamper-resistant audit trail. Techniques such as transaction hashing, block confirmations, and distributed consensus mechanisms ensure data integrity across all participating nodes. This decentralized recording prevents centralized manipulation, thereby building trust among advertisers and users who rely on accurate metrics for validating engagement.

5.3 Off-Chain Computation and Load Optimization

While blockchain provides unparalleled transparency, it is computationally expensive for large-scale operations. To address this, the system employs off-chain computation techniques for tasks that do not require immutability. These include media storage, session processing, initial verification steps, and campaign analytics. Off-chain servers validate preliminary events and only submit finalized interaction proofs to the blockchain. This approach significantly reduces gas fees, improves system responsiveness, and ensures that blockchain is used optimally for critical data only. Hybrid architectures combining on-chain and off-chain computation allow the system to remain scalable while maintaining strong security guarantees.

5.4 Engagement Verification and Anti-Fraud Techniques

The system integrates advanced techniques to differentiate genuine user interactions from bot-generated or fraudulent activities. Multi-layered verification includes device fingerprinting, user interaction monitoring, behavioral pattern analysis, and CAPTCHA-based human validation. These techniques detect abnormal activity such as rapid repeated clicks, multi-session spoofing, or automated scripts attempting to exploit the reward mechanism. By enforcing strict verification before forwarding data to the blockchain, the system minimizes false positives and ensures that only legitimate engagements influence reward calculations. This anti-fraud methodology is vital for maintaining advertiser confidence and preventing revenue leakage.

5.5 Tokenization and Incentive Mechanisms

A blockchain-based token economy underpins the reward model, ensuring that users receive fair compensation for their authentic engagement. Techniques include secure token minting, controlled supply management, and transparent token transfer operations governed by smart contracts. The tokenization model encourages user participation while maintaining an equitable balance between advertiser expenditure and user rewards. Reward incentives may vary depending on engagement type, campaign quality, or advertiser-defined parameters. By leveraging blockchain tokens, the system reduces reliance on traditional payment intermediaries and supports a decentralized economic model.

6. Results

The implementation and evaluation of the Blockchain-Based Ad Revenue System demonstrate significant improvements in transparency, fraud resistance, and fairness compared to traditional digital advertising models. During testing, the system successfully recorded ad impressions, verified user engagements, and executed reward distributions through smart contracts without requiring any centralized authority. The immutability of blockchain logs ensured that all campaign activities were visible and auditable, allowing advertisers to verify the authenticity of engagement metrics with complete confidence. User tests showed that the reward mechanism operated reliably, with smart contracts distributing tokens instantly upon validation of an interaction. This automated flow eliminated delays and reduced the risk of manipulation or errors commonly associated with centralized systems. Overall, the results validate the feasibility and advantages of a decentralized, blockchain-driven advertising model. The system proved capable of maintaining data integrity, delivering reliable metrics, and incentivizing user participation fairly. These

outcomes demonstrate that integrating smart contracts, decentralized verification, and tokenized incentives can significantly transform the digital advertising landscape, offering a more secure, transparent, and user-centric alternative to existing centralized solutions.

7. Challenges Faced

During the development of the Blockchain-Based Ad Revenue System, several technical, operational, and architectural challenges emerged that influenced design decisions and system optimization. One of the primary challenges was ensuring seamless integration between on-chain and off-chain components. Since blockchain networks have inherent latency and cost constraints, designing a hybrid architecture that balanced transparency with efficiency required careful coordination of data flows and verification logic. Another significant challenge involved addressing ad fraud in a decentralized environment. Traditional fraud detection methods rely on centralized analytics, whereas this system required decentralized or semi-decentralized mechanisms capable of validating user authenticity without compromising privacy. Implementing robust anti-fraud techniques—such as device fingerprinting, behaviour analysis, and CAPTCHA-based validation—while maintaining a smooth user experience proved complex. Smart contract development also presented challenges, particularly around optimizing gas usage, preventing contract vulnerabilities, and ensuring secure, predictable execution of reward distribution logic. Additionally, user identity management introduced difficulties, as the system had to maintain anonymity while simultaneously preventing Sybil attacks and duplicate reward claims. Managing large ad media files through off-chain storage, ensuring fast content delivery, and linking metadata to on-chain records without inconsistencies also required extensive testing. Furthermore, onboarding non-technical users posed usability challenges, as blockchain interactions such as wallet connection and transaction confirmation were unfamiliar to many participants. Despite these hurdles, iterative testing, architectural refinement, and adaptive design strategies enabled the system to evolve into a secure, scalable, and user-friendly solution.

8. Future Improvements

As the digital advertising ecosystem continues to evolve, the Blockchain-Based Ad Revenue System offers significant potential for enhancement to meet growing technological, security, and scalability demands. Although the current system successfully addresses transparency, fraud reduction, and fair revenue distribution, there are still areas where future advancements can greatly improve the platform's efficiency and user experience.

1. Integration of Advanced Fraud Detection Models: Future versions can incorporate machine learning–based behavioural analysis or anomaly detection models to further enhance accuracy in distinguishing genuine users from automated or malicious traffic.
2. Adoption of Zero-Knowledge Proofs (ZKPs): ZKP-based techniques can allow users to prove engagement without revealing personal information, providing stronger privacy while maintaining verifiable interactions.
3. Multi-chain and Cross-chain compatibility : Expanding the system to operate across multiple blockchain networks would reduce congestion, lower gas costs, and offer greater flexibility for advertisers and users.
4. Decentralized Identity (DID) Integration: Incorporating DID frameworks can strengthen resistance to Sybil attacks and provide verifiable but privacy-preserving user identity mechanisms.
5. Automated Campaign Optimization : Incorporating DID frameworks can strengthen resistance to Sybil attacks and provide verifiable but privacy-preserving user identity mechanisms.
6. Scalability Enhancements with Layer-2 Solutions: Using layer-2 protocols such as Optimistic Rollups or zkRollups can significantly improve transaction throughput and reduce fees for large-scale ad interactions.
7. Support for Additional Ad Formats: The system can be expanded to handle advanced formats like interactive ads, AR/VR ads, or personalized content streams to increase user engagement.

9. CONCLUSIONS

The Blockchain-Based Ad Revenue System represents a significant shift from traditional, centralized advertising models toward a more transparent, secure, and user-centric ecosystem. Through the integration of blockchain technology, smart contracts, decentralized verification mechanisms, and a token-based reward structure, the system addresses many longstanding challenges in digital advertising—including fraud, opaque metrics, unfair revenue distribution, and privacy concerns. The implementation demonstrates that blockchain's immutability and decentralization can provide verifiable engagement data, automated reward flows, and trustworthy interactions between advertisers and users without relying on intermediaries. By combining on-chain transparency with efficient off-chain processing, the architecture achieves a balanced model that maintains performance while enforcing strict integrity and accountability.

REFERENCES

[1] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.*

[2] Buterin, V. (2014). *A Next-Generation Smart Contract and Decentralized-Application-Platform* Ethereum Whitepaper.

[3]. IAB (Interactive Advertising Bureau). (2023). *Digital Advertising Trends-Report* IAB Official Publications.

[4] Google Anti-Fraud Team. (2022). *Click Fraud Prevention Techniques-and-Best-Practices* Google Ads Documentation.

[5] Alliance for Audited Media. (2021). *The State of Digital Ad Fraud and-Transparency* AAM Industry Report.

[6] CoinMarketCap Research. (2023). *The Growth of Tokenized Economies-and-Web3-Advertising* CMC Research Insights.

[7] W3C. (2022). *Decentralized Identifiers (DIDs) v1.0.* World Wide Web Consortium (W3C) Recommendation.

[8] Zyskind, G., Nathan, O., & Pentland, A. (2015). *Decentralizing Privacy: Using Blockchain to Protect Personal Data.* IEEE Security and Privacy Workshops.