The Role of Blockchain in Influencer Marketing and Digital Media Transparency

Vengesai Mavengano
Yeshiva University - Digital Marketing and Media

Gladstone Tonderai Chichaya
Yeshiva University - Digital Marketing and Media

Tingaitei Chisoro
Yeshiva University - Digital Marketing and Media

Anna Tanyaradzwa Audrey Chingono
Yeshiva University
Digital Marketing and Media

ABSTRACT
This paper addresses the disruptive potential of the Distributed Ledger Technology (DLT) that can serve to reduce endemic lack of transparency and trust in the digital media and influencer marketing ecosystems. Since online advertising losses through fraud are estimated to be over $45billion by 2026, and almost two out of every three brands are impacted by fraud, the decentralised, immutable and cryptographically secure nature of blockchain provides a solid solution to structural problems like ad fraud, cloudy payment channels and the inability to determine a true interaction. Two key areas of application of DLT, which are the subject of this paper, are, first, auditable and provable systems to track advertising expenditure and performance of the campaign to guarantee appropriate budget allocation and measure. Second, the creation of systems (Decentralised Identity, DID) and features (Verifiable Credentials, VCs) to authenticate the origin of influencers, verify metrics in the audience, and create content provenance, successfully overcoming the threat of bot-driven engagement and synthetic data. The study analyse the technical specifications of implementing the solutions, such as smart contract implementation and approaches to overcoming the technical scaling limitations and regulatory contradictions, such as the right to erasure of the GDPR. The report's conclusion is that the adoption of DLT can create a more transparent, efficient, and trustful digital campaign ecosystem and ensure that marketers are much more accountable and the return on investment.

Keywords
Blockchain, Distributed Ledger Technology (DLT), Influencer Marketing, Ad Fraud, Decentralized Identity (DID), Verifiable Credentials (VC), Transparency, GDPR.

1. INTRODUCTION
The advertisement industry has undergone a paradigm shift during the past two decades in which the sector has transitioned to become a multifaceted, hyper-fractured digital and programmatic landscape no longer focusing on consolidated model of the industry that used to be dominated by traditional media, in the form of print, radio, linear television. This development has freed unprecedented degrees of targeting and contact; but it has also brought deep degrees of operational dissipation. The modern digital media supply chain includes many intermediaries, called Demand-Side Platforms (DSPs), Supply-Side Platforms (SSPs), Ad Exchange, and verification vendors that intervene between advertisers and final publishers [1]. This complex, multi-layered deep structure creates a great deal of information asymmetry, in which advertisers often have no insight into how much money is being spent, how much of the fees are being consumed, and whether their advertisements are actually being seen by real consumers [1, 2]. The result of such a state of transparency is a breeding place of mismanagement and waste which contributes to the lack of trust that blockchain technologies are meant to address [1].

At the same time, the influencer marketing economy has become one of the key pillars of digital strategy, and it is estimated that the industry will have a value of about 24 billion by 2024 [3]. Influencer marketing is based on personalised recommendation of peers, taking advantage of intimate connections that social media influencers have with their followers [4, 5]. These relatable social media influencers are often more trusted by consumers, especially Generation Z, than traditional brand promotion or celebrity promotions [5]. As a result, influencer marketing always achieves one of the highest returns on investment (ROI) compared to other conventional advertising strategies [3]. However, this channel will only be as effective as the verifiable authenticity of the audience and metrics of engagement of the influencer, which makes the sector extremely susceptible to the new types of digital fraud [6].

The coincidence of programmatic supply chain obscurity and sector of influence vulnerability to the authenticity of the manufactured have resulted in the massive financial losses necessitating system reform requirements. It is estimated that the digital advertising market will lose more than $41.4 billion to fraud by 2025 [7], and that almost 60 percent of brands already have experienced influencer fraud with fake and artificial followings [8]. These fraud vectors corrupt campaign performance data, waste budgets and have a devastating impact on consumer trust, and undermine the integrity of the overall digital media ecosystem. The main problem is not just tracking the funds but the creation of a single and unmodifiable system, which can prove the integrity of both transactions and parties with whom the engagement is made.

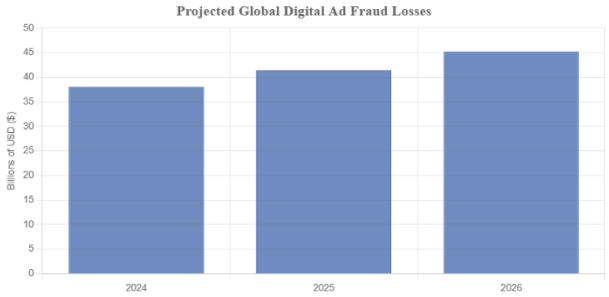

Figure 1: Financial Trajectory of Global Digital Ad Fraud Losses

Source: (Spider AF [7])

Its structural vulnerabilities inherent in its decentralized and intermediary-heavy digital media supply chain have led to a culture of systematic fraud and secrecy that has cost the supply chain a significant amount of money. Digital advertising fraud is a growing, multi-billion-dollar systemic challenge, and the losses are estimated to grow to $41.4 billion in 2025 and even higher, to 45.2 billion in 2026 [7]. Such financial waste, where the average rate of 10% invalid traffic (IVT) permeates the industry is a life-threatening force upon the integrity of the markets and the excessive distortion of the performance indicators [9]. The multidimensionality and high-tech nature of bot networks and cybercrime, where AI is becoming more crucial to mitigation, require sophisticated, metrics-based systems to ensure optimal performance and safety in these hybrid, enterprise level implementations [10, 11].

The forms of fraudulent undertakings occur in the ecosystem in various forms. Click spamming is the most significant source in programmatic ads and represents 76.6% of invalid traffic [7]. Additionally, bot traffic plays a key role, as automated scripts have up to 24% of all clicks in paid searches campaigns, and total non-human-generated traffic use up a considerable amount of digital money [9]. Small businesses are particularly harmed by such invalid traffic that can cost them up to 30 percent of their advertising budget to click fraud [9]. The failure of advertisers to modify campaign success metrics to capture these non-genuine interactions implies that they will overestimate their ROI [7].

The fabricated authenticity is a threat in the influencer sector. This is highlighted by an alarming statistic: 59.8% of brands indicated having experienced fraud in their presence in 2023, most commonly in the form of fake followers and artificial engagement [8]. The ultimate cause is an inherent absence of transparency on budget flow. Sometimes, advertisers are in business without an extensive view of cost models, fee structure, and performance intelligence throughout the programmatic supply chain [1, 2]. Such information asymmetry creates an environment in which mismanagement is fostered [1] and makes it extremely difficult to reconcile the campaign data, which makes the need to find a solution that brings about transparency in the way campaign initiation is done to the last payment [12].

Objectives

This study aims to provide solutions to the systemic issues by assessing the transformative capability of the Distributed Ledger Technology (DLT).

- **Objective 1 (Transparency)**: The first objective is to thoroughly examine how the fundamental principles of immutability and decentralization of the DLT can be used to develop a transparent, unified, and auditable registry of tracking digital advertising spending, especially the implementation of smart contracts in the performance-based implementation [13, 14].
- **Objective 2 (Authentication)**: A second objective is to explore the technical feasibility of the integration of the Decentralised Identity (DID) systems and Verifiable Credentials (VCs) to authenticate influencer identities, thus preventing bot-based fraud, Sybil attacks, and ensuring content provenance in the quickly changing environment of generative AI [15, 16].

The paper makes an important contribution as it summarizes the modern literature on the use of technology and empirical outcomes of its use in enterprises [17, 18]. It aims at creating a systematic taxonomy of blockchain applications to suit the aspect of quantifying digital media transparency [19], furthering the discussion beyond the conceptual models towards empirically verified technical platform and providing practical information to industry players with the goal of reinstating financial and reputational integrity.

2. LITERATURE REVIEW

2.1. Foundational Concepts of Trust and Transparency in the Digital Supply Chain

The lack of trust in the digital ecosystem is based on the fact that it relies on centralized data repositories. Such systems are controlled by individual entities that regulate the integrity and access of data [20], thus making other stakeholders unavailable. Such a hierarchy inherently limits transparency, which further creates information asymmetry and breeds deep consumer mistrust about online surveillance (also known as dataveillance) in the context of personalised advertisements [21]. A workable solution requires a solution that essentially transforms the fabric of accountability. The digital supply chain transparency is characterized not only as the visibility but the ability to provide objective and verifiable information concerning all cost, fees, and performance indicators in the complex programmatic setting [2]. The technology solution should be able to enable all the stakeholders, which include the advertisers, publishers, and the consumers to have equal access to the correct and uniform record of transactions [1].

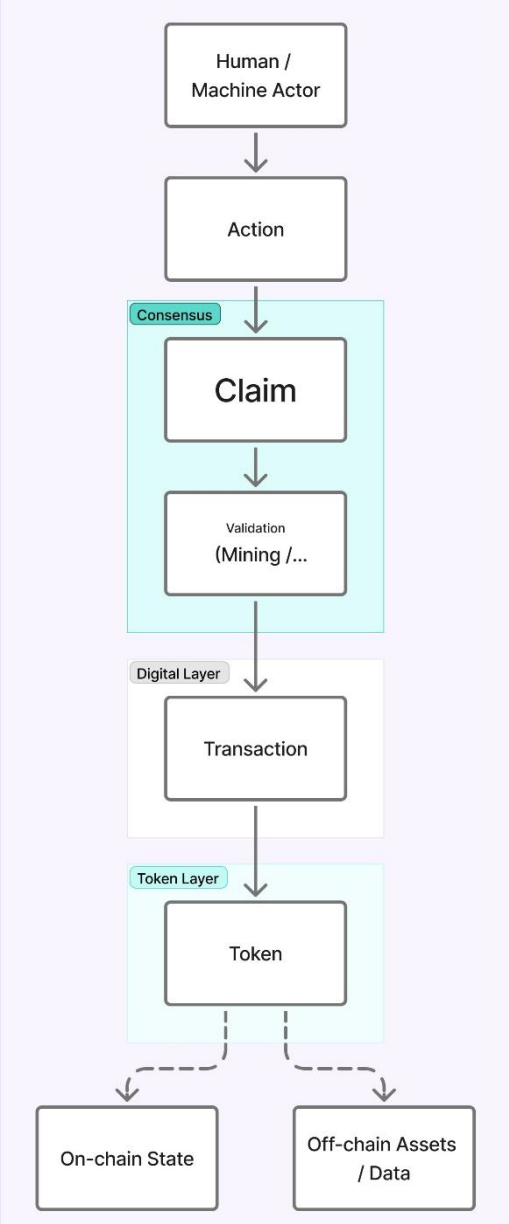

Figure 2: Conceptual Diagram of DLT's Core Principles

In Figure 2, a very basic sketch of the conceptual architecture that includes the four main concepts of DLT systems and their connection should be presented: action, consensus, distributed ledger and token (Adapted from Ballandies et al. [22]).

2.2. Mechanics of Fraud: Fraud and Deception by Influencers Explained and Measured

Digital media fraud is a complex issue that also aims at programmatic effectiveness and the integrity of personal recommendations.

Ad Fraud Vectors

Ad fraud takes advantage of technical control gaps in the intermediated ad delivery system. The highest percentage of invalid traffic is credited to click spamming as it constitutes 76.6 percent of non-genuine traffic [7]. The role of bots is significant, as automated scripts are responsible for up to 24 per cent of all clicks in paid-search campaigns, and non-human traffic in general accounts for a large share of the digital spend [9]. It is estimated that fraudulent losses will skyrocket, and worldwide statistics will reach $41.4 billion by 2025 [7]. This steady increment highlights the challenge of traditional practices in identifying and blocking advanced bot networks which can be used to falsify campaign data [9]. In addition to that, the emergence of Made for Advertising (MFA) websites, that use generative AI to generate low-quality content at a large scale, has introduced novel sources of invalid traffic and fake leads, further exacerbating the issue [7].

Fraud of Influencers and Fake Authenticity

Influencer fraud aims at corrupting perception and engagement statistics of the audience. This involves the common habit of buying fake followers and organizing coordinated schemes of engagement pods to artificially boost the rate of interactions. This impact is harmful to brands, and almost 60 per cent of brands in 2023 reported fraudulent practices, most commonly through fake followers and synthetic engagement [8]. In addition to vanity metrics, affiliate fraud poses a serious financial threat, costing businesses an estimated $3.4 billion in

2022 as a result of fraudulent clicks (17% of affiliate traffic) and methods of manipulation, including cookie stuffing and sub-ID fraud [9]. The fraud rates on mobile platforms (up to 50 per cent greater than desktop) also require strong, decentralized identity authentication mechanisms that can prove the human origin of interaction [9].

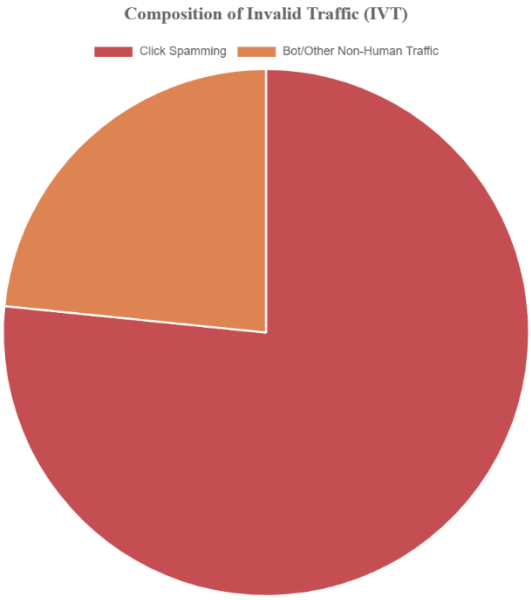

Figure 3: Composition of Invalid Traffic (IVT) sources, demonstrating the dominance of click spamming over general bot traffic

To explain the scale of this issue quantitatively, Table 1: Estimated Financial Impact and Prevalence of Digital Ad Fraud (Source: Spider AF [7]; TrafficGuard [9]; Firework [8]) summarizes the main financial indicators of fraud exposure in the digital media industry.

Table 1: Approximated Cost and Frequency of Digital Ad Fraud

Fraud Vector	Key Metric	Value (2025/2026 Forecast)	Source
Digital Ad Fraud (Global Losses)	Estimated Financial Loss	$41.4 Billion (2025); $45.2 Billion (2026)	[7]
Invalid Traffic (IVT) Rate	Overall Average Digital Advertising	10%	[9]
Bot Activity in Paid Search	Percentage of Non-Genuine Clicks	14% to 22%	[9]
Influencer Fraud Exposure	Brands Reporting Fraudulent Activity	59.8% (2023)	[8]
Affiliate Fraud Losses	Estimated Cost (2022)	$3.4 Billion	[9]

(SpiderAF [7]; TrafficGuard [9]; Firework [8])

2.3. Distributed Ledger Technology (DLT): Core Principles and Architecture

DLT is the architectural baseline that enables creating trust in an environment where there is mutual distrust among participants [14]. Fundamentally, DLT combines the cryptographic protection, consensus and distributed storage to form tamper-resistant record-keeping [23].

Decentralization and Distribution

A decentralized implementation is realized through the use of the ledger in a peer-to-peer network in which many independent nodes replicate and store the information [20], [23]. Contrary to conventional centralized databases, which are managed by one administrator, DLT is such that no one can have the overall power or control [20]. This decentralized character is essential; each participating entity is having an identical copy of the ledger and as a result, this single point of failure is removed and the risk of data modification by any single malicious actor is also eradicated [20, 23]. This decentralized trust value is the base value of distributed control [20].

Immutability via Cryptographic Hash Chains

Immutability guarantees that after a transaction or data entry is confirmed by the consensus protocol of the network and stored, it is virtually unattainable to modify it or erase it [23]. This is made possible by cryptographic hashing and chaining. The transactions in each block are cryptographically hashed, and their hash is represented in the header of the succeeding block. This forms a dependency chain, meaning that any attempt to modify a single transaction will necessitate re-calculating the hash of that block and all the following blocks, something computationally infeasible on a large, decentralized network [14]. This cryptographic solution is impossible to compromise to create financial accountability in online advertising [1]. DLT has the capability of ensuring a single source of truth (permanent and auditable) by capturing all ad transactions, including placement orders and final engagement metrics, in a permanent log that cannot be modified [14]. This verifiable history provides advertisers with confidence that their advertising money is grounded on the basis of real engagement and guarantees the publishers get the correct payments in terms of the tracked performance.

Consensus Mechanisms: Ensuring Distributed Agreement

Consensus mechanisms are advanced algorithms that allow geographically separated, mutually distrusting nodes to come to an agreement on the validity of transactions and the right state of the ledger [23]. This consensus serves as the online version of all the parties simultaneously nodding their heads before a new account is completed, avoiding fraud and providing data consistency between all copies of the ledger [14, 20, 24].

A network selection of a consensus mechanism is the key factor in deciding how secure the network is, transaction throughput and decentralisation. The major categories of mechanisms in the distributed ledger technology (DLT) applications are:

- **Proof of Work (PoW)**: PoW is based on competitive difficulty (mining). It is extremely safe yet slow, with

approximately seven transactions per second (TPS) of processing [25, 26]. This means that the resulting latency and energy consumption makes it inappropriate in real-time and high-volume programmatic advertising [26], [27].

- **Proof of Stake (PoS) and Delegated Proof of Stake (DPoS)**: PoS uses validators determined by the value they have in the network (stake) [20]. DPoS puts validation to a limited number of elected delegates. These systems tend to be on a faster and more energy-efficient scale than PoW.
- **Byzantine Fault Tolerance versions**: BFT-based systems, including Practical BFT or those implemented by Hyperledger Fabric, are more suitable in permissioned, enterprise settings whereby participants are known [20], [28, 29]. They put strong consistency in the presence of a minority of faulty nodes at a high priority, which is essential to make them well adapted to the AdTech supply chain; they focus on deterministic finality and high throughput [14, 28].

Table 2: Comparison of Consensus Mechanism Suitability for Programmatic DLT

Mechanism	AdTech Suitability	Typical Throughput (TPS)	Key Feature for AdTech
Proof of Work (PoW)	Low	~7	High Security (but too slow)
Proof of Stake (PoS)	Medium	~30+	Energy Efficiency
Byzantine Fault Tolerance (BFT)	High (fo Permissioned)	High/Configurable	Confidentiality & Performance at Scale [29]
Delegated PoS (DPoS)	Medium-High	High	Speed and Scalability [20]

(Source: Huang et al. [26]; Singh [25]; Akingbade [20]; IBM [29]**)**

2.4. Smart Contracts and Self-Sovereign Identity (SSI): The Technical Building Blocks

Smart Contracts (SCs) that facilitate the automation of processes and Self-Sovereign Identity (SSI) that facilitates authentication are the two key technological mechanisms that can be used to make the digital media ecosystem more transparent and trustful [13, 14, 16]. SSI is a paradigm shift in the identity management digitization, putting the power back in the hands of the user [30], [31].

2.4.1 Smart Contracts (SCs) and Automated Execution

Smart contracts (SCs) are computer specifications, which are saved on the blockchain and are automatically executed once the certain predefined conditions are met, thus providing transparency, safety, and impossibility of changing the terms agreed upon by the decentralized networks [13, 32]. The performance-based payouts in digital advertising are automated by SCs, simplifying sophisticated multi-party deals by the need to confirm that the specified performance metrics, like viewability or reliable audience engagement, have achieved the target [33, 34]. This automation does not need any manual action and removes cycles of dispute [14], which further decreases intermediation in invoicing, verification, and settlement, and, therefore, eradicates administrative costs and reduces the possibility of a human error [14, 35]. In addition, SCs make compliance easier, since they can be coded to automatically check that advertising programs meet previously agreed regulatory or ethical requirements before funds are disbursed [14, 36].

2.4.2. Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs)

According to the definition of the World Wide Web Consortium [30], Decentralized Identifiers (DIDs) are a new paradigm of verifiable, decentralized digital identity. Did is architecturally designed so that it is not dependent on registries and identity providers (centralized), allowing the controller to have exclusive cryptographic control over their identity with no requirements of external authentication [30, 37]. Critically, every DID is resolved to a DID Document, a machine-readable artefact, which contains the key identity-resolution metadata [30, 31]. The key elements of the DID Document include Cryptographic Public Keys, used to provide a secure way of communication and authentication [31]; Authentication Parameters, which outline the processes authorized by the controller to verify identities [30]; and Service Endpoints, which provide authenticated routes to interact with the DID subject [31].

Such autonomy of architecture plays a critical role in improving security, especially in reducing fraud including Sybil attacks [16]. The credibility in DID is obtained with the help of Verifiable Credentials (VCs), cryptographically protected statements about an entity [30, 31, 37]. The VC ecosystem follows three standardised roles [30, 37]: the Issuer (e.g., an independent auditor or verification company, Alj et al. [38]) who cryptographically signs the credential; the Holder (the entity, which stores the VC in his/her secure digital wallet, Dutta and Rao [39], n.d.); and the Verifier (such as a brand or advertiser, [40]) who requests Despite some metadata about issuance and revocation contained in VCs [37], the credentials are generally transferred off-chain to protect privacy and the verification is fully based on the cryptographic proofs stored on the immutable ledger [31].

Table 3: Roles and Functions within the Verifiable Credential Ecosystem

Role	Function in Influencer Marketing	Cryptographic Action	Source
Issuer	Certifies influencer's audience quality/authenticity score.	Creates and digitally signs the Verifiable Credential.	[37, 38]
Holder	The influencer manages and stores the VC in a digital wallet.	Controls the DID and generates cryptographic proof of possession.	
Verifier	The Brand/Advertiser requests proof of credentials before payment.	Validates the VC signature and authenticity against the DLT-anchored public key.	[37, 40]

(Source: [30], [37]**;** [38]**)**

Table 4: Comparison of Identity Models for AdTech

Criteria	Traditional (Cookies, IP, Device Fingerprinting)	Centralized Logins (e.g., Social Logins for Ad Profiles)	Blockchain-based DID/SSI
User Control	Low	Medium (within platform limits)	High (user holds keys, manages credentials)
Data Privacy	Low (often opaque data collection)	Medium (platform controls data, subject to policies)	High (selective disclosure, user consent)
Security against Impersonation	Medium (can be spoofed/mimicked)	High (for platform login)	Very High (cryptographic proofs)
Verifiability of Attributes	Low (inferred or self-declared)	Medium (platform may verify some attributes)	High (via Verifiable Credentials from trusted issuers)
Susceptibility to Bot/Fake Accounts	High	Medium (fake accounts still possible)	Low (high cost/complexity to create fake verified DIDs at scale)
Centralization	Mixed (data on device & ad-tech servers)	High (platform is central authority)	High Decentralization (user-centric; ledger is distributed)
Transparency of Use	Low (complex ecosystem, unclear data usage)	Medium (dependent on platform's transparency policies)	High (mechanism is transparent, user controls sharing, consent can be logged on-chain)

Table 4 compare the architecture of Traditional Identity Systems (centralized database, single point of failure) against Decentralized Identity (user controls DID/VCs, authentication via cryptographic proofs on a distributed network). Source: (Laneau [41])

2.4.3. Privacy Preservation via Zero-Knowledge Proofs (ZKPs)

One of the technological advancements that a privacy-preserving authentication system needs to implement to fulfill ethical uses of DLTs is the utilization of Zero-Knowledge Proofs (ZKPs), cryptographic schemes which allow a prover (an influencer) to prove that a statement is correct to a verifier (a brand) without disclosed information. Digitally, ZKPs eliminate the salient privacy versus authenticity problem by enabling an influencer to demonstrate, e.g. by playing an authenticity-verifying VC that they have at least 100,000 verified followers, the existence of that number of followers without revealing the sensitive personal or demographic data of those followers. Also, ZKPs help to provide the highly effective defence against the exploitation of bots; unlike the automated bots, ZKPs are unable to generate the complex cryptographic proofs of the unique DID; therefore, ZKPs can be used to strengthen the platform integrity, and the principle of Secure by Design cannot be established without intrusive data exposure [2, 16, 42].

2.5. Governance Models: Decentralized Autonomous Organizations (DAOs) and Enterprise DLT

Permissioned distributed ledger technologies (DLT) are the traditional method of ensuring confidentiality in enterprise advertising; however, the theoretical ideal of an entirely decentralized ecosystem is the Decentralized Autonomous Organization (DAO). A DAO is a blockchain-based structure that uses self-executable smart contracts to encode, render automatic, and implement governance policies, which removes the need to have a traditional centralized administration [43, 44].

Within the digital media environment, DAOs may be used to operate programmatic advertisement exchanges, or influencer platforms by enabling stakeholders to vote on:

- **Policy and Protocol Upgrades**: It is necessary to make sure that policy and protocol modifications should be community-based and transparent [44].
- **Dispute Resolution**: Arbitration process is automated with smart contracts and collective voting, and the platform is no longer moderated centrally [44].

However, the general use of the DAOs in commercial institutions with high stakes is still limited to regulatory grey and the challenge of establishing accountability in a distributed system as a legal matter [43, 45]). This organizational difference underscores the fact that the enterprise DLT systems, like Hyperledger Fabric, are still the necessary mediating factor, as they offer a controlled permissioned governance that is in line with the current corporate structure and regulatory compliance requirements [20, 29].

2.6. The Shift to Continuous Auditing (CA) in DLT Systems

The audit methodology is radically different when it comes to the immutable and auditable nature of the records provided by the DLT, the audit methodology is shifted to Continuous Auditing (CA) as opposed to periodic and sample-based examinations [46, 47]. In traditional programmatic advertising, auditors have no choice but to use fragmented data silos and reliance on fragmented financial systems, which results in high levels of reconciliation expenses [14, 47].

Continuous Auditing with DLT addresses the problems by:

- **Real-Time Data Access and Resilience**: Auditors have real-time, permissioned access to the unchanging log of all transactions. The decentralized nature of the DLT guarantees access to data even when a node fails, which reduces downtime to a minimum and enhances audit resilience [14, 19, 46].
- **Automated Authentication of Transactions**: The use of smart contracts and the consensus mechanism automatically authenticate transactions during the recording stage, which offers an audit trail that is verifiable [14, 46]. This procedure saves a lot of time in terms of reconciliation [47, 48].
- **Complete Visibility**: Since each individual transaction is cryptographically authenticated and recorded, auditing no longer requires statistical sampling [49] but a complete monitoring [46, 47]. Automated machine-learning algorithms can be directly applied to shared ledger data by auditors to identify anomalies or fraud patterns immediately at the time they happen [47]. This feature shifts auditing into an avertive, real-time operation that results in quality and more efficient operations [46].

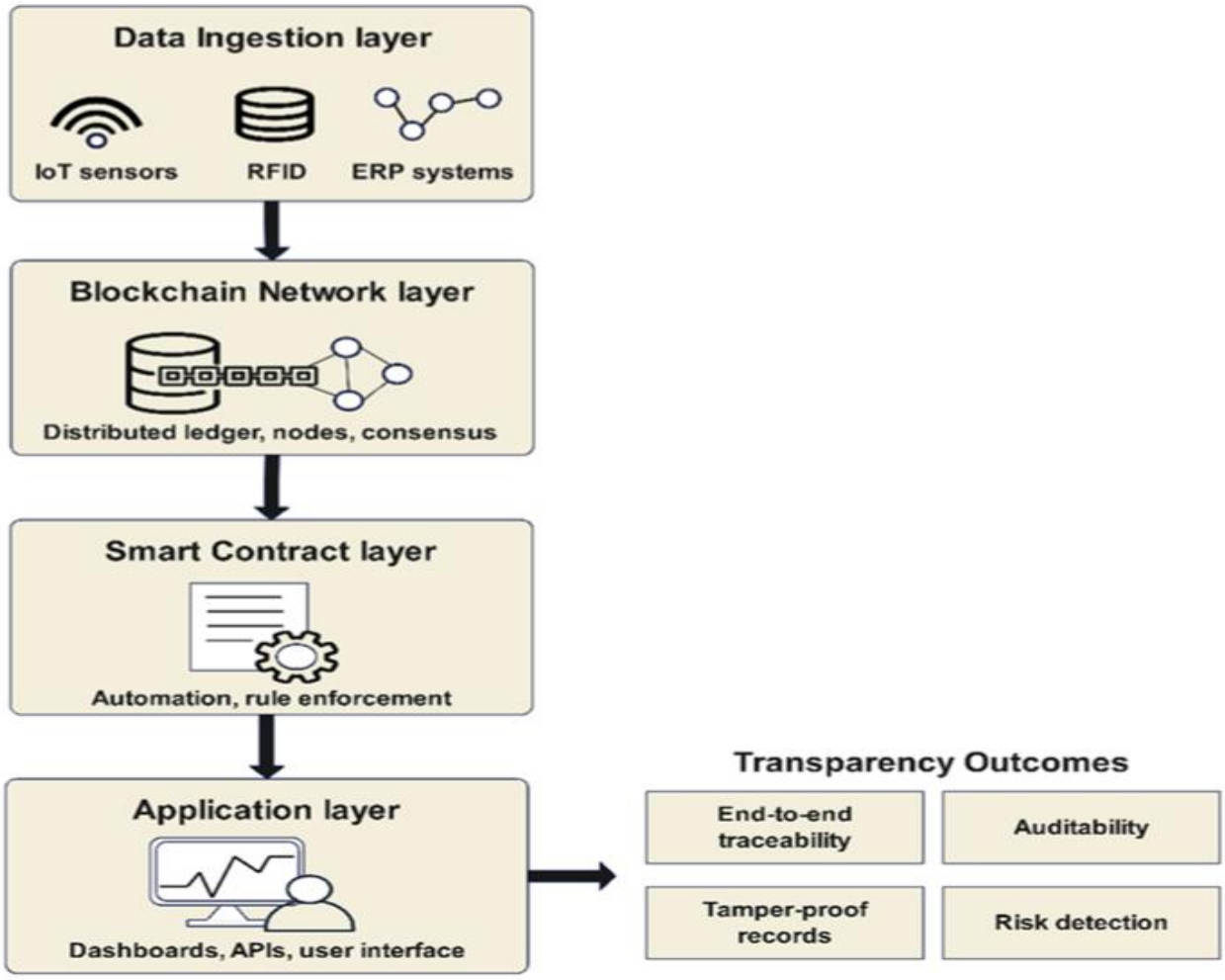

Figure 4: Conceptual Flow of DLT-Enabled Continuous Auditing
Source: (Chen [50])

This migration, in turn, enhances the quality and efficiency of audit, as well as the stakeholder confidence, as data integrity can always be verified [14]. Based on this, the strategic necessity of brands incorporating DLT is not limited to fraud prevention but rather to the realised benefit of real-time, comprehensive financial oversight and increased audit effectiveness [46].

3. BLOCKCHAIN MECHANISMS FOR AD SPEND TRANSPARENCY AND AUDITABILITY

3.1. Modeling the Transparent Advertising Supply Chain (TASCS)

The introduction of DLT requires the re-organization of the digital media supply chain in concept, resulting in a Transparent Advertising Supply Chain System (TASCS). This paradigm transforms the opaque and mediated supply chain, traditionally, into a collocated and peer-to-peer network and thus affords all authorised parties, including advertisers, agencies and publishers, with both read/write access to one, consistent, immutable datastore [1]. TASCS framework is based on the layered architecture that provides full traceability, auditability, and trust [50]. The Data Ingestion layer stores crude ad event data (impressions, clicks). This information is hashed and stored on the DLT Network layer creating the immutable ledger. The Smart Contract layer will execute the agreed-upon business logic in Automated mode, whereas an Application layer will include the user interface of real-time monitoring and auditing [50]. This change has eradicated gaps, as it excludes data silos and offers a single and real-time audit journal [14].

applications

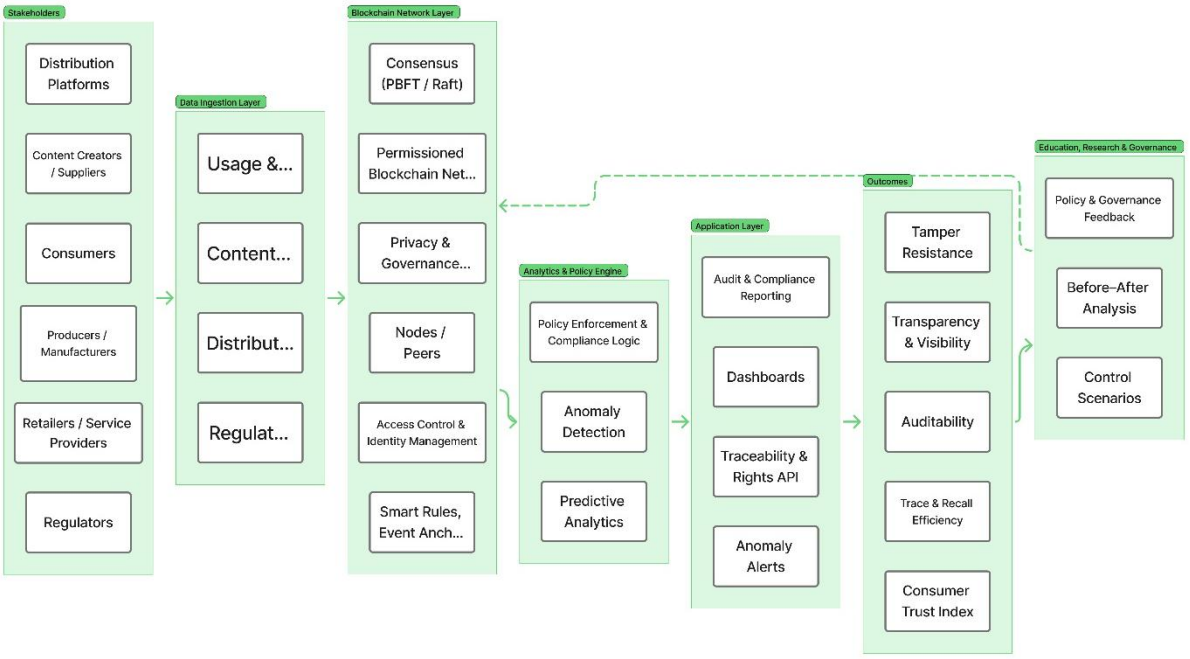

Figure 5: Conceptual Framework of a Blockchain-Enabled Digital Media Supply Chain

Figure 4: Illustration of the four-layer architecture of the TASCS model: *Data Ingestion (Ad Events) → DLT Network (Immutable Ledger) → Smart Contract Layer (Automated Execution) → Application Layer (Audit/Analytics Dashboard).* **Source:** Chen [50].

3.2. Automated Budget Distribution via Smart Contracts

The introduction of smart contracts will be essential in changing the situation with budget distribution that is subject to a discrepancy into an automated and performance-based system [13, 34]. Smart contracts are used to execute contracts automatically, which means the payment is automatically released once it is verified that the predefined conditions have been met, e.g., having reached a certain campaign reach or viewability level [34].

Combining automated execution and the immutable ledger provides several operational efficiencies. Smart contracts facilitate the distribution of revenue, minimize administrative overheads, and enable the publication and influencers to receive adequate and fair compensation in a timely manner through the reduction of the need to rely on human mediation of invoicing and verification [13, 34, 35]. Moreover, the given impossibility of the transaction log changes considerably decreases the time and cost related to the billing and reconciliation processes, which conventionally require a lot of resources because of the high data discrepancies [14]. This factual automation instills confidence between parties where the payment is explicitly tied to the provably actual performance.

Table 5: Comparison of Traditional vs. Blockchain Ad Spend Metrics

Metric Category	Traditional AdTech	Blockchain-Enabled DLT	Benefit
Transparency	Limited, siloed data, information	Full, open ledger access for authorized parties [1]	Unbiased cost/fee visibility [2]

	asymmetry [1]		
Fraud Mitigation	Reactive, relies on third-party verification (A3Logics, n.d.)	Proactive, crypto-based verification, single source of truth (A3Logics, n.d.)	Eliminates click fraud/false impressions (A3Logics, n.d.)
Payment & Reconciliation	Manual invoicing, high data discrepancy [14]	Automated via Smart Contracts, real-time logging [14]	Reduced disputes, enhanced efficiency [14]

3.3. Technical Architecture for Transaction Logging: The Permissioned Approach (e.g., Hyperledger Fabric)

The bulky size of transactions and the need to keep the data confidential in the enterprise advertising requires an optimised technical architecture that is sensitive to both the performance and privacy. As a result, permissioned distributed ledger technologies (DLTs) are preferred to open public blockchains [27, 28, 29]. Additionally, the needs of enterprise platforms require solid, metrics-based systems to improve security and performance continuity in the hybrid deployment [10].

3.3.1. Enterprise Requirements and Hyperledger Fabric

Moderate networks, like those provided by Hyperledger Fabric, create trust among a specific group of actors, and this is also necessary to conduct commercial relationships between brands, agencies, and publishers [29]. This is in sharp contrast with public blockchains that are based on anonymity and heavy computer computations, which cannot be accommodated by commercial interests [28]. The modular architecture of Hyperledger Fabric enables high-performance scale operation and supports the needs of enterprises to maintain confidentiality of their data [29]. Channels ensure confidentiality, which is a private sub-network that is only visible to authorised participants; therefore, transactions and other smart contract (chaincode) data can only be seen by those participants (Hyperledger Fabric Documentation, n.d.). Maintaining privacy and maintaining a shared ledger that is immutable and unchanged is central to managing commercially sensitive campaign information among competitors [29].

3.3.2. Case Study: IBM and Mediaocean

One of the most successful examples of implementation of a permissioned DLT strategy in the field of advertising is its use by IBM and Mediaocean. This project is Hyperledger Fabric-based and was designed to simplify the supply chain and build trust among the involved parties, which included the big brands, such as Kellogg, Kimberly-Clark, Pfizer, and Unilever. Critical transactions, such as budget allocation, authorisation, orders, verification, invoicing, and payments, were accurately logged into the system that allowed participants to trace activity in a consolidated audit journal [48, 51]. Results showed an increase in levels of transparency in the advertising supply chain and a significant decrease in data anomalies, which confirms the feasibility of the model as a real-time, auditable service that large-scale enterprise transactions [14]. This system is augmented with the Mediaocean advertising platform that manages more than 140 billion dollars of annual advertisements [48].

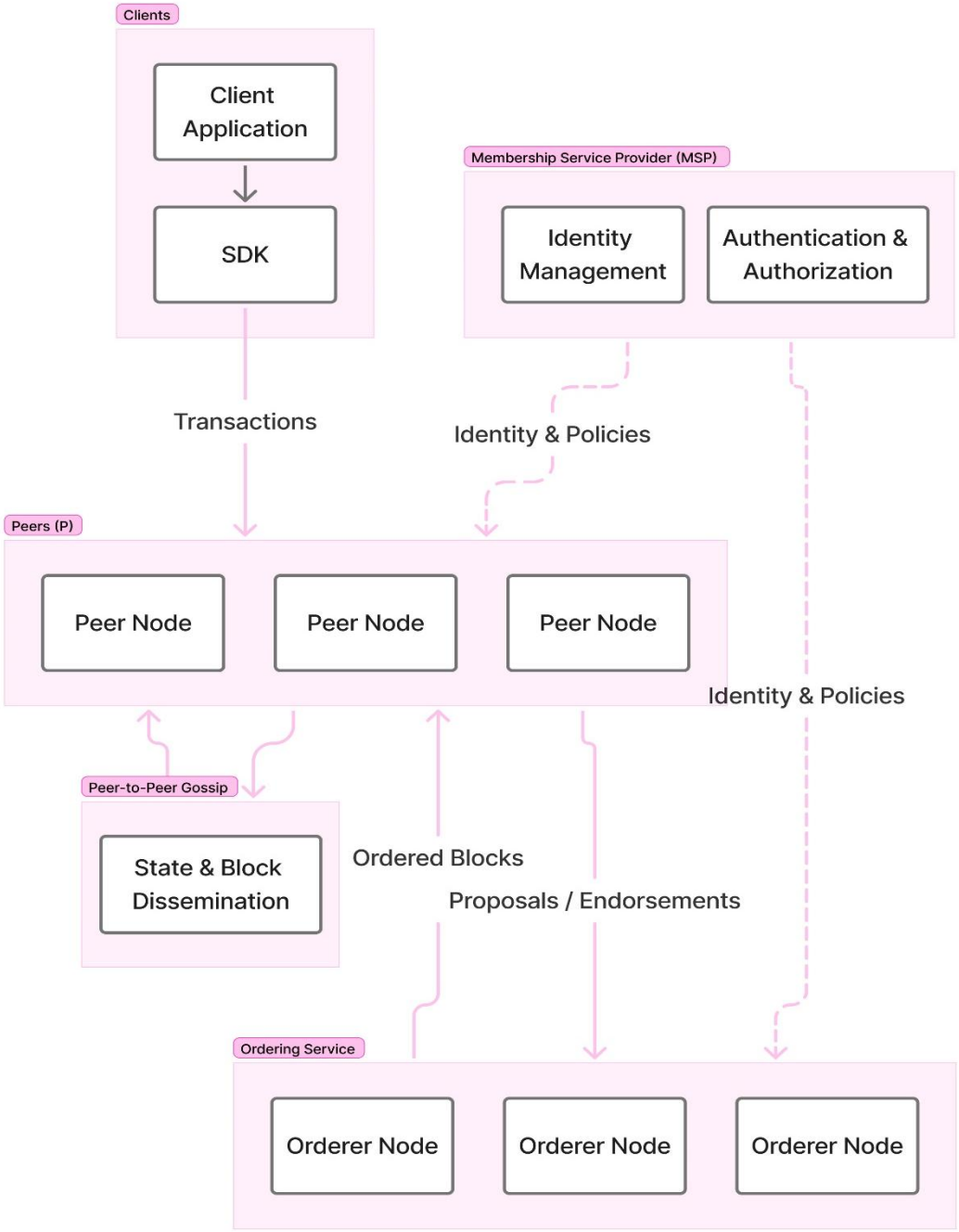

Figure 6: Hyperledger Fabric Architecture for AdTech Enterprise

Figure 5 illustrates the Hyperledger Fabric permissioned network architecture. The modular design, composed of Peers (P), an Ordering Service, and the Membership Service Provider (MSP), is utilized by enterprise consortia (e.g., brands, agencies, and publishers). The architecture is critical for AdTech because it enables confidential transactions by supporting Channels (not explicitly shown but configured on Peers), which isolate transaction data and Chaincode execution to only the authorized, recognized participants.

3.4. Data Validation using Blockchain Oracles for Off-Chain Campaign Metrics

It is necessary to have a critical point of integration between on-chain smart contract logic and off-chain performance data, including viewability measurements, audience demographics, and conversion metrics [13]. The use of oracles helps in overcoming this challenge. Oracles are secure mediating processes via which external information is brought back by APIs, databases, or analytics systems, authorized and checked on its authenticity and accuracy and sent safely to the blockchain ecosystem to be executed using a smart contract [13]. Applied to the advertisement setting, oracles confirm that performance data of campaigns meet contract-stipulated standards, such as ensuring that a certain percentage of impressions was truly shown [34]. Decentralised oracle further improves reliability through the aggregation of many sources of data and use of a distributed network of validators [13]. Oracles allow smart contracts to make payments in response to objective, real-world events by having them verified and tamper-proof off-chain data feeds, which will help ensure that the contractual agreements are fully enforced and directly maximise the campaign ROI [18, 22].

4 COMBATING FRAUD, VERIFYING AUTHENTICITY, AND IMPLEMENTATION BARRIERS

4.1. Decentralised Identity (DID) Solution of Influencer Verification.

The overall problem of manufactured authenticity in influencer marketing, where almost 60% of brands are faced with fraud [8], requires a systematic fix that focuses on identity verification instead of the transparency of transactions. A basic monitoring of funds spent on bot traffic only proves that this is a wasted investment; the answer to the problem is that the party of the campaign counterpart is a human being, with a unique and non-fictional personality, and thus will overcome Sybil attacks when one individual generates several false identities [11, 16]. The W3C defines Decentralised Identifiers (DIDs), which offer the appropriate cryptographic framework. Didis enable the influencer with self-sovereign ownership of their digital identity, regardless of centralised platform registries [30]. The cryptographic proofs needed by DID systems to establish existence and control over an identifier cannot be created by automated programmes (bots) [16, 41]. This cryptographic tool is a strong security measure, as it means that any dealings on the platform are between individuals that are proven and real, which makes the environment significantly more resistant to fraudulent activity conducted by a bot [16].

4.2. Adoption of Verifiable Credentials (VCs) of Reputation and Performance Metrics.

Verifiable Credentials (VCs) are secure and cryptographically verifiable statements about an entity, including age evidence, professional qualification, or, most importantly in marketing, a verified history of engagement or profile of demographic audience. The issuance of these VCs is digitally signed by a trusted issuer (e.g. an independent auditor or platform) and stored in the DID owner in his or her digital wallet, therefore directly connecting reputation to the self-sovereign identity of the influencer [39].

4.2.1. Distributed Reputation Systems

Decentralised reputation systems can be created through blockchain technology where the reputation of an influencer is based on a record of verified performance data and attested credentials that are impossible to change, not a metric of the influencer on the platform that can be easily manipulated [35, 41]. With time, these attestations may add up to the DID of an influencer, building a credible reputation score that is publicly available to brands and cannot be controlled through the manipulations of the platforms [35]. This type of system essentially rewards genuine behaviour and punishes fraudulent acts.

4.2.2. SC Integration with VCs

VCs can be combined with smart contracts, creating a strong automation and authentication layer. Smart contracts can have their programming such that they automatically check identity and performance compliance [40]. To take an example, the smart contract may check the DLT to ensure that the DID of an influencer has an up-to-date VC rating an Authenticity Score over X% or a particular audience demographic before releasing payment to a campaign [39]. It is then only after the successful cryptographic verification of the VC that the transaction is executed and the brand will only pay when it demonstrates genuinely verified engagements by the verified entities [40]. This figure 6 demonstrates the blockchain architecture with multiple layers to suit the automated influencer payments with the help of the Blockchain Network layer to provide the secure and transparent registration of transactions. The flow takes the Data Ingestion layer to ingest actual performance into real-world performance metrics using Oracles into the Smart Contract layer, which enforces the contractual terms, one of which is the validation of the Influencer Verified Credentials (VCs). When the specified KPIs are reached, the Smart Contract automatically transacts the token payment, otherwise it can activate the Risk detection mechanism. The design provides End-to-end traceability and encourages trust in the digital marketing ecosystem.

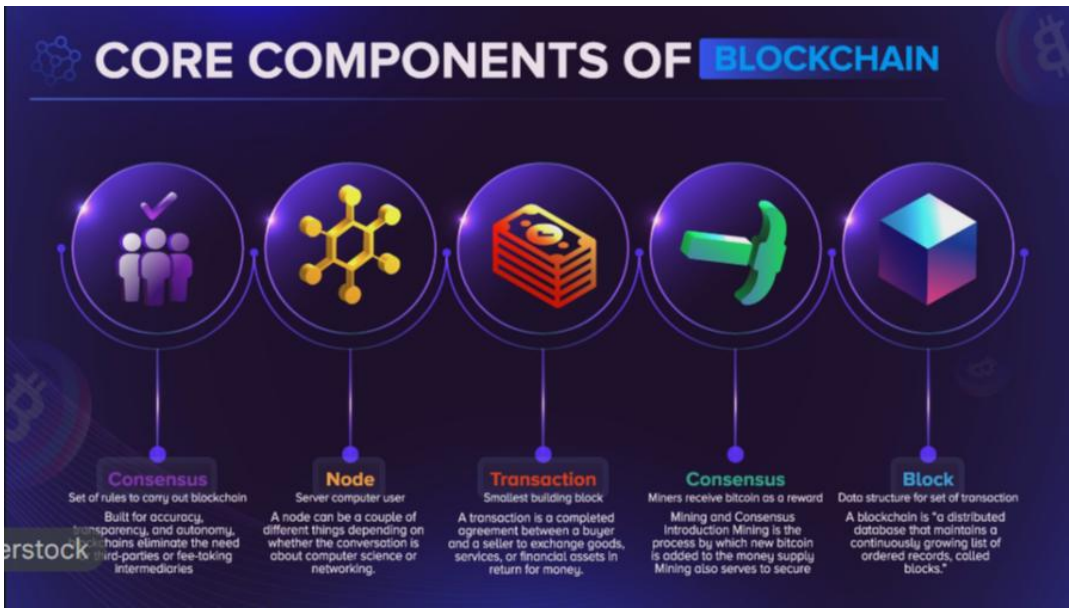

Figure 7: Smart Contracts Layered Architecture to execute payment of influence campaign verification.

4.3. Fake Engagement, Bot Traffic, and Sybil Attacks Mitigation

The DLT-DID system offers a strong, technical protection against advanced fraud techniques. The concept of decentralized identity authentication means that proven human beings are involved in digital relations, and the platform ecosystem is hostile to bot nets [16].

The system uses the cryptographic techniques, including the zero-knowledge proofs, so that users can demonstrate their exclusive human quality or their possession of an identity without revealing personal information [16]. This privacy-insensitive verification scheme helps to ensure the security of the user and, at the same time, increases the reliability of the interactions on the platform. More so, the forced build-up of verifiable, attested credentials introduces an economic barrier to the fraudsters; it is much harder and more expensive to build and maintain a legacy of verifiable contacts than it is to just build temporary bot accounts, which once more brings integrity to the digital communities [31, 41]. Further actions to safeguard against ad fraud include the cryptographically encrypted verification system [52], which also helps prevent the system.

4.4. Ensuring Content Provenance and Disclosure in the Age of Generative AI.

The use of sophisticated Generative AI tools has created a heightened demand of verifiable content provenance. The existence of realistic fake media may easily deceive the audience, so platforms such as YouTube, Meta, and Tik Tok are introducing certain disclosure policies tied to provenance metadata [53]. The possibility of impersonation on the mass scale and manipulation of synthetic data in consumer-related scenarios, including healthcare, highlight the importance of verification and responsibility [15]. The application of the concepts of Secure by Design, with the additions of AI-based security features, is crucial in the protection of software products and securing content integrity in the DLT-based systems [42].

This tracking can be provided through a blockchain technology. Blockchain ensures that the ultimate source of content is documented with an unpremodifiable record of content creation metadatas and modification histories on a distributed ledger [54]. Such ability makes sure that a viewer and advertisers can determine whether content was produced by a human influencer or it was digitally manipulated or synthetically produced by AI [53, 54]. This type of content modification history and transaction trail anchoring in an unaltered ledger offers a safe, non-modifiable audit trail that not only increases market transparency, but also ethical and legal responsibility of creators and platforms [19, 55]. as shown in figure 7 this structure demonstrates the two-layered authentication process of multimedia content at the client. It starts by retrieving a special string with a blockchain transaction ID, and compressed sensing (CS) samples in their media, which then initiates the process of watermark extraction.

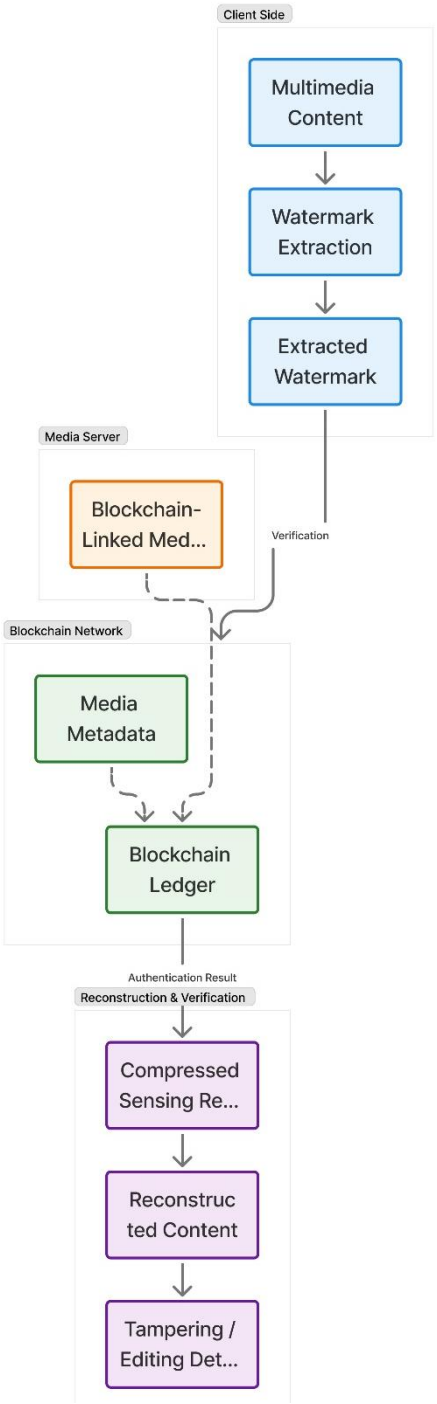

Figure 8: Content Provenance and Verification Flow

4.5. Case Study Analysis: Quantifiable Benefits and ROI Uplift

Empirical evidence that supports the transition to DLT is that there is a direct correlation between transparency and optimization of campaign performance. The verifiable information that blockchain systems can offer advertisers will allow the latter to effectively follow the actions of consumers that result in sales and calculate the quantifiable change in budget allocation off of fraudulent or black market channels [18, 35].

This economic advantage had been validated by the pilot partnership between Toyota and Lucidity. Implementation of

an advertising solution based on a blockchain that maximized advertising budget by providing precise tracking and eliminating middleman waste resulted in Toyota recording a significant 21 percent improvement in campaign performance [17]. This is a clear sign of joy that confirms the claim that transparency through DLT results directly to improved operational performance and greater marketing performance [35]. Equally, the IBM/mediaocean pilot, which engaged large consumer packed goods brands, was able to record transactions and minimize the data discrepancies successfully [14, 48], which confirms that immutable single source of truth generates measurable positive outcomes in dispute resolution and the effectiveness of reconciliation [14]. In some sectors, such as Real Estate and Finance, strategies based on blockchain are said to result in the growth of ROI up to 23 percent [18].

Table 6: Summary of DLT Impact on Key Marketing Metrics

Metric	Improvement/Status	Key Mechanism	Source
Campaign Performance (Toyota Pilot)	21% lift	Clear tracking & intermediary elimination	[17]
Overall ROI (Finance/Real Estate)	Up to 23% increase	Trust, consistency, and reduced fraud losses	[18]
Transaction Reconciliation	Significant reduction in time/cost	Single source of truth (Immutable Ledger)	[14], [48]
Audience Authenticity	Enhanced verification	DIDs, VCs, and ZKPs	[16]; [31]

(Source: Swartz. Nagarsheth, and Capel [17]; Verma et al. [18]**)**

4.6. Technical Implementation Barriers: Scalability, Latency, and Throughput Analysis

The smooth adoption of DLT into the programmatic advertising supply chain is severely limited by the basic technical constraints, which can be network scalability, latency, and throughput of the transactions. These limitations are frequently ignored during the theoretical discussion, but constitute the face of reality in an industry where data processing is performed in real time and with high frequency [27].

Throughput Limitation

The processing of millions of ad requests and ad transactions per second are needed as programmatic ad exchanges are executed at huge scale. The existing leading mass public blockchain networks, including Bitcoin and Ethereum, can process transactions only at a very low speed with 7 TPS and 30 TPS, respectively [25, 26]. This is disastrously insufficient to cater to programmatic advertising. In case the DLT system is not capable of managing the amount of programmatic bids and impressions needed, the technology is operationally invalid within AdTech [27].

Cost and Latency

This combined with the inherent constraints of block capacity and dependence on computationally burdensome consensus mechanisms cause high transaction costs and unacceptable delays (latency) at times of peak network usage [25]. In real-time bidding exchanges, high-frequency trading requires no delays, and the fees are prohibitive, which makes it economically impractical to record individual and low-value ad impressions. The DLT architecture has to change to offer a reasonable Quality-of-Service (QoS) level to meet the industry speed and cost demands [27]. In addition, effective attack prevention in critical sectors such as ransomware is based on the layered defense approach which balances security, performance, and efficiency throughout the infrastructure [56].

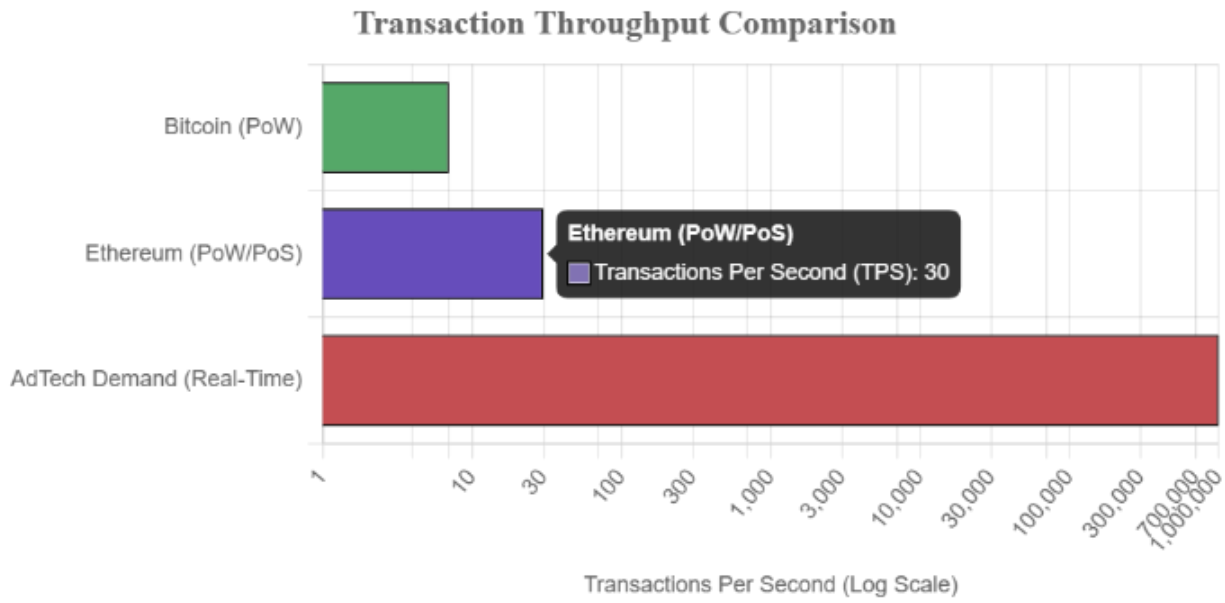

Figure 8: Comparative analysis of transaction throughput (TPS) between base-layer blockchains (Bitcoin, Ethereum) and typical AdTech real-time bidding requirements

Note the logarithmic scale indicating the magnitude of the scalability gap.

4.7. Scaling Solutions: Layer 2 Networks and Sidechains

In order to accommodate the high-volume throughput needs of the digital media, DLT needs to embrace specialized scaling solutions, which puts premium on the Layer 2 solutions, which decongest the primary network [57]. These solutions should be anchored on the layered defenses and capitalise on the state-of-the-art techniques such as Federated Learning to provide secure and scalable performance [56, 58].

Layer 2 Strategy

The protocols implemented on top of the primary blockchain but that execute transactions off-chain are known as layer 2 scaling solutions that guarantee transactions that are faster and less expensive than those made on the primary blockchain without compromising the security and finality of the latter through cryptographic techniques [13, 57]. This plan plays a critical role in enabling DLT to manage the millions of ad transactions needed every day by programmatic transactions.

Types of Solutions

Rollups (as well as Optimistic rollups and Zero-Knowledge rollups) combine a large amount of off-chain transactions into a single transaction, which is then posted to the main blockchain to be settled [13]. This batching approach provides a great deal of throughput without affecting the security assurances of the underlying network. Sidechains are autonomous blockchains that are attached to the main chain to enable them to have their own specialized consensus mechanisms to handle rapid and high-volume transactions [57]. This sidechain design is inherently aligned with the business requirement of permissioned DLT (such as Hyperledger Fabric), in which businesses can keep a business-controlled, high-throughput setting to perform business operations utilizing the security core of a DLT architecture [29]. The fact that such scaling technologies are necessary proves that the adoption of DLT in AdTech has to focus on the engineered performance rather than the theoretical decentralization [27].

Table 7: Overview of DLT Scaling Solutions for AdTech

Solution Type	Mechanism	Primary Benefit	Applicability to AdTech
Rollups	Bundles off-chain transactions into single on-chain submission.	Increases throughput; retains main chain security.	Handling massive impression/ click volume efficiently.
Sidechains	Independent DLT connected to the main chain.	Enables specialized, high-speed consensus mechanisms.	Private, high-speed processing for enterprise consortiums (e.g., Hyperledger).
State Channels	Direct off-chain communication between transacting parties.	Near-instant, free transactions once established.	Micro-transactions (individual bid/impression logging).

(Source: Solulab [57]; Rapid Innovation [13]; Huang et al. [26]**)**

4.8. Regulatory Conflicts: Reconciling DLT Immutability with GDPR (Right to Erasure)

Implementing immutable ledgers in regulated markets creates a direct opposition to any primary data privacy laws, especially the General Data Protection Regulation (GDPR) in the EU [45]. The nature of personal data management in immutable ledges only emphasizes the importance of AI in enhancing privacy and safety because, in this decentralized environment, conventional ways of doing things have difficulties with the challenges of digital forensics and cybercrime [11].

The Immutability Paradox

The key principle of blockchain the irreversible and immutable register [59] is literally contrary to the key GDPR principles, in particular, the right to be forgotten (right to erasure) of data subject and the right to rectification [60]. Provided that personal data is permanently stored in a ledger, then it is technically impossible to respond to a legal request to have the data erased, and this makes organizations directly in breach of the EU legislation [45, 61]. Moreover, complex research of encrypted or sensitive data in a decentralized system, including that provided by the DLT solutions, requires frameworks [62].

Responsibility and Authorization.

This can also make it harder to comply with due to the decentralized character of DLT which blurs the legal distinction between data controllers and data processors. It is also hard to hold anyone accountable when the data is shared in global, permissionless networks because no single organization can even imagine holding all data instances accountable [45]. These institutional problems pose significant barriers to accountability and compliance along multi-jurisdictional networks.

4.9. Solutions for Compliance: Hybrid Architectures and the CRAB Model

To find the required path in the legal environment with maintaining the integrity of the DLT, the tendency towards hybrid architectural and data management approaches is occurring

Hybrid Storage Systems

The best technical mitigation that is possible is to define a hybrid data architecture. This necessitates off-chain storage of sensitive or personal customer data (PCD) on compliant and centralized storage systems [59]. The ledger of blockchain is then dedicated to the storage of non-personal information, cryptographic distributions, and hash of metadata [59, 63]. The specified method enables the required modification or deletion of sensitive data in the centralized store to abide by the regulatory requirements, with the ledger maintaining the unchangeable integrity to verify the transactions [59, 64].

The CRAB Model for Erasure

A specific example of the model that can be suggested to deal with the right to erasure is the CRAB (Create, Read, Append, Burn) model [65]. Such a mechanism does not involve the physical deletion of the immutable chain record. Rather, the encryption keys that enable access to the off-chain stored personal data are burned or irreversibly destroyed with an erasure request is received [59, 65]. This will make the data permanently unreadable and thus, ensures functional compliance with the erasure requirement, but will not violate the immutability of the ledger [65]. The further evolution of governance systems should be based on the essential requirement to connect legal professionals and technologists to create responsive frameworks that would support the benefits of the DLT as well as privacy standards.

Personal Identifiable Data (PID) is stored off-chain in a centralised and editable database, and only cryptographic hashes and non-personal metadata are stored on-chain in the immutable ledger as shown in Figure 4.4 (Hybrid Data Architecture for GDPR Compliance). Once an erasure request has been made, the system performs the step of the CRAB model called Burn; this step involves permanently destroying the encryption keys that connect the on-chain reference to the off-chain personal data. This makes the data permanently unreadable, which effectively erases the data without breaking the principle of blockchain immutability.

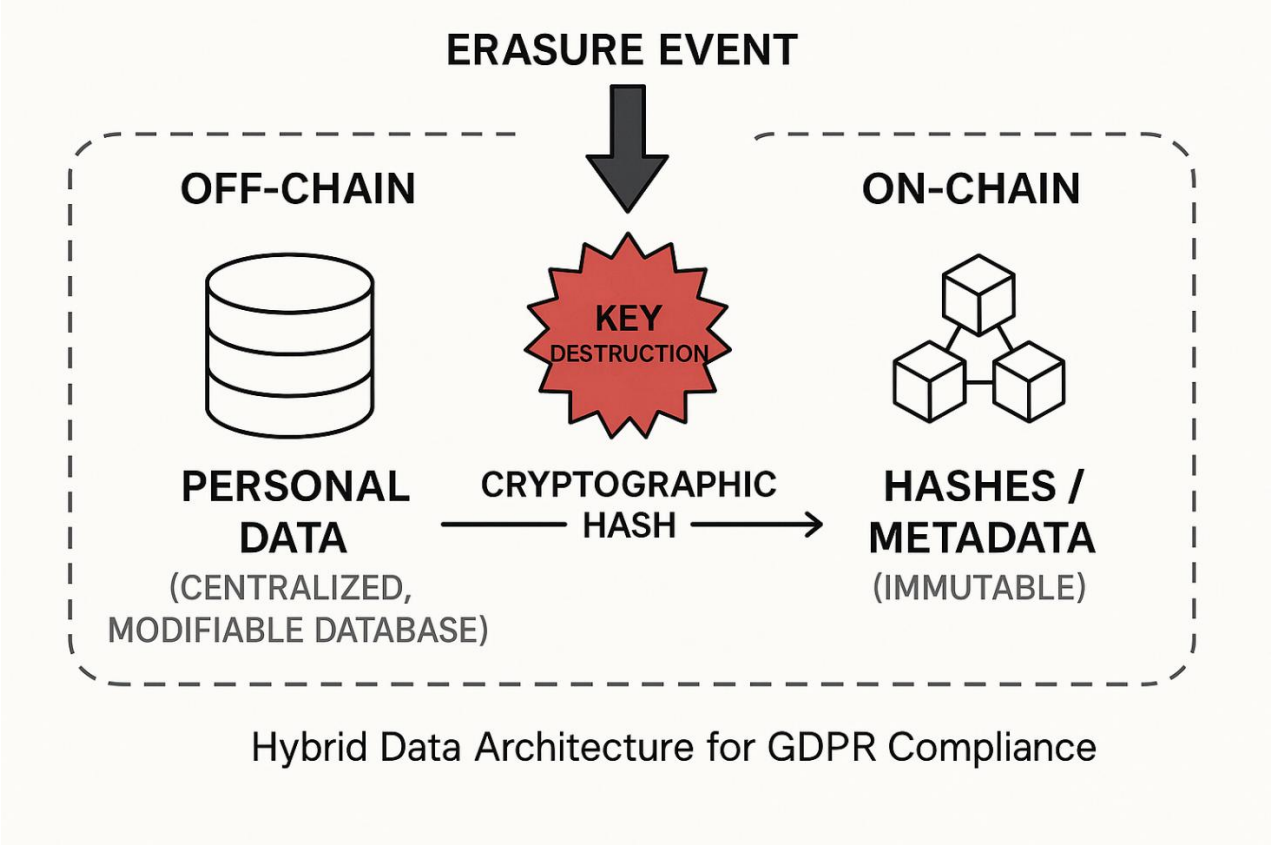

Figure 9: Hybrid Data Architecture for GDPR Compliance

5. COMPARATIVE REVIEW: PROPOSED DLT FRAMEWORK VS. TRADITIONAL ADTECH

In an attempt to establish the feasibility of the suggested Distributed Ledger Technology (DLT) framework, this research paper presents a comparative analysis to the existing digital media supply chain. The analysis is based on four essential dimensions: transparency to architecture, the anti-fraud measures, efficiency in financial settlement, and data privacy.

5.1 Architectural Transparency: Information Asymmetry Solution

The traditional programmatic supply chain is based on a hyper-fractured architecture where information are stored in siloed centrally controlled servers that are managed by the myriad of intermediaries, including Demand-Side Platforms (DSPs), Supply-Side Platforms (SSPs) and Ad Exchanges. This kind of structure creates a black box effect resulting in a high level of information asymmetry where the advertisers do not see how 40 and 50 percent of their budgets are spent on intermediary fees [1]. In such an environment, it is almost impossible to verify the value chain on a timely basis, with every intermediary holding a distinct, and frequently incompatible, transmission record.

The suggested Transparent Advertising Supply Chain System (TASCS), however, alleviates these silos by introducing a single, tamperproof ledger. The architectural change is essential: the traditional system is based on the different datasets which need to be reconciled by hand, the DLT system is based on the “Single Source of Truth, common to all the permissioned nodes. This common ground makes all the participants view the same set of transactions, which makes hidden costs and obscured markups impossible to hide.

The Toyota and Lucidity pilot shows that such transition allows identifying wasted spend in real-time. A 21% increase in campaign performance was registered by the pilot [17], which is empirically confirmed with the fact that information asymmetry reduction is directly related to Return on Ad Spend (ROAS) improvement. The ecosystem returns to its financial integrity by abandoning a trust-based model (the decision being based on the intermediary reports) and adopting a verification-based model (auditing the ledger).

5.2 Fraud Mitigation: Probabilistic and Deterministic Verification

An essential difference is the method of verification. The existing fraud-prevention tactics are mostly probabilistic and reactive. They rely on third-party vendors to examine the patterns of traffic once the impressions were made in order to sift out invalid traffic (IVT). This method is especially insufficient to counteract high-tech attacks, including click spamming, which at 76.6 0 of IVT [7]. In many cases, the IP addresses are blocked when a large amount of money has already been wasted on these interactions with bots, which makes the prevention of frauds a neverending game of whack-a-mole.

The suggested DLT system, with the use of Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), proposes a deterministic and proactive model of security. In contrast to the modern model, which permits traffic by default, the DLT architecture uses a verify-then-trust identity-first architecture. Access is provided only when a valid credential is provided. The system mathematically excludes interactions between bots by requiring a cryptographically signed VC prior to a smart

contract executing a transaction. Bots with no access to the private key of authenticated human identities cannot produce the necessary digital signatures [16]. This transformation is highly effective in curbing Sybil attacks and directing marketing funds solely to human interaction, which has been verified as authentic, moving the industry out of fraud detection into fraud prevention.

5.3 Settlement Efficiency Automated vs. Manual Reconciliation

The current ecosystem is labor-intensive and often can take 60 to 90 days due to the lack of data discrepancies between advertiser logs and publisher reports to reconcile its finances [14]. This latency not only ties up working capital, but it also increases administrative overheads since dispute resolution is needed at all times. Advertisers and agencies use resources heavily to manually check invoices against performance reports which is prone to human errors and antagonism. With Smart Contracts, this logic is automated and manual invoicing is discontinued in favor of code-based execution. The conditions of the order of insertion (e.g., pay $X when 1,000 verified impressions) are simply an inscription in the blockchain in this model. As it occurred with the IBM and Mediaocean deployment, automated settlement minimized the data discrepancies to almost zero [48].

This comparative advantage works in two planes speed and accuracy. The settlement is immediate when a set of predefined Oracle data is verified and the removal of human involvement in billing process eradicates error and dispute expenses. What has been produced is an atmosphere of mistrust where the security of payment is established by a convention of code and not company name so publishers will be compensated in a timely way and advertisers will only pay on proven performance.

5.4 Privacy Paradigm: Zero-Knowledge Prooves vs. Dataveillance

The conventional AdTech paradigm is based on the concept of dataveillance, monitoring user activity online in order to create profiles, which is becoming less and less consistent with laws, including the GDPR and the Right to Erasure [21]. The fixed nature of blockchain also poses a theoretical Immutability Paradox with respect to such rights: with a ledger that cannot be modified, how is it possible to delete the data of a user? This is a major compliance challenge to traditional blockchain applications. This tension designated to the proposed framework is resolved with the help of a hybrid architecture and the CRAB (Create, Read, Append, Burn) model. The system does not store Personally Identifiable Information (PII) on-chain but instead just stores cryptographic hashes or references, and the real user information is stored in off-chain and GDPR-compliant databases. When a user bigs out, the decryption keys of the off-chain data are burnt, making the data irretrievable without breaking the integrity of the ledger [65]. In addition, the inclusion of Zero-Knowledge Proofs (ZKP) provides a better model of compliance than the existing invasive tracking. ZKPs allow influencers or users to demonstrate a certain audience demographic (e.g., “Audience is over 18) without providing actual data. This model of Sovereign identity reinstates the authority on the user, and it is possible to target without the massive collection of personal information.

5.5 Summary of Comparative Advantages

Table 8 overviews the structural change of the existing model to the proposed blockchain-based architecture.

Table 8: Comparative Analysis of Traditional AdTech vs. Proposed DLT Framework

Evaluation Metric	Traditional AdTech Model	Proposed DLT Framework	Operational Outcome
Trust Mechanism	**Institutional:** Reliance on third-party intermediaries.	**Cryptographic:** Reliance on immutable code and consensus.	Eliminates counterparty risk and intermediary bias.
Data Architecture	**Siloed:** Fragmented databases requiring manual reconciliation.	**Unified:** Shared Ledger (Single Source of Truth).	documented 21% performance uplift [17].
Fraud Prevention	**Reactive:** Blacklisting IPs post-event; vulnerable to click spamming.	**Proactive:** Cryptographic authentication (DIDs/VCs).	Prevents bot interaction before budget is spent.
Settlement Speed	**High Latency:** Net-60 to Net-90 days; manual disputes.	**Real-Time:** Automated via Smart Contracts.	Optimizes working capital and reduces admin costs [14].
Privacy Model	**Intrusive:** Cookie-based tracking; GDPR friction.	**Sovereign:** Hybrid storage (CRAB Model) & ZKPs.	Enhanced GDPR compliance and user trust.

5.6 Strategic Trade-offs and Scalability

Although the analysis shows the superiority of the DLT framework concerning transparency and security, there is the need to appreciate the trade-off in terms of throughput. Conventional centralized servers can support millions of requests per second (RPS) with insignificant latency, and base-layer blockchains like Bitcoin (around 7 TPS) or Ethereum (around 30 TPS) [26] have in the past had difficulties scaling to such levels. It would be prohibitively expensive, and would push the network to congestion as one would have to record all ad impressions on a public mainnet. But as discussed in Section 4.7, this can be avoided by Layer 2 scaling solutions (Rollups) and Sidechains (e.g., Hyperledger Fabric channels). These mechanisms allow the suggested framework to package transactions off-chain and thus achieve the same speed as a standard AdTech system, whilst maintaining the benefits of on-chain auditability. As a result, the analysis concludes that, despite the architectural complexity that follows the introduction of DLT, benefits in fraud mitigation and financial efficiency in the long term surpass the implementation costs. The system does not have to displace the speed of real-time bidding, but rather, it serves as a settlement layer which cannot

be changed and proves whether the high-speed transactions are valid.

6. CONCLUSION AND STRATEGIC RECOMMENDATIONS

6.1. Summary of Transformative Potential

A systemic solution that could address the issue of lack of trust in the digital media and influencer marketing sectors is the blockchain technology, which is based on cryptographic trust, immutability, and decentralization [23]. The analysis of Chapter 2 and Chapter 3 illustrates that, under a necessary auditable defense, the endemic problems of opacity and fraud that cost the industry billions in a year are prevented by DLT [7]. The qualitative characteristics of the cryptographic nature of the DLT are fundamentally related to the reconciliation issues inherent to the intermediated programmatic supply chain, and provides a single source of truth of the financial transactions and performance measures [14].

DLT offers two technological benefits: to track ad spend, it offers a powerful and transparent ledger, which is possible through automation of payment and verification operations via smart contracts [13]. Second, and most importantly, it provides a required identity layer (DID/VC) to cryptographically protect human authenticity in influencer interactions, which directly eliminates Sybil attacks and faked authenticity [16, 31]. The case studies, including the implementation of Toyota/Lucidity, confirm that higher transparency was directly associated with the performance optimization that measured results, providing a significant 21 percent increase in campaign effectiveness [17]. This supports the main hypothesis: DLT increases accountability and thus marketing performance and ROI [18].

6.2. Strategic Recommendations for Industry Stakeholders

The way towards the general acceptance of DLT must be the concerted effort of regulatory, technological, and corporate spheres to eliminate the scaling and compliance hurdles identified.

In the case of Brands, Advertisers and Agencies (Commercial Strategy): Organisations should actively make investments in moving out of legacy systems that continue to make opaque media buys. It will necessitate a shift to approach towards DLT-enabled platforms, with a focus on those employing performance-oriented, permissioned architectures, including Hyperledger Fabric to guarantee the required data confidentiality and manage high volumes of transactions [10, 29]. In addition, the industry needs to unify the need to have Verifiable Credentials (VCs) verified by certified and third-party auditors. This standardization will take the market further than the current platform vanity metrics (likes, follower counts) to cryptographically verifiable metrics of audience authenticity and quality [38, 39]. The brands need to invest in the creation of smart contracts directly linked to these approved VC metrics in particular to ensure that only authentic engagement is paid.

In the case of AdTech Platforms and DLT Providers (Technical and Operational Strategy): Scalability is still the main technical challenge. The Layer 2 scaling solutions, especially Rollup and Sidechain, should be imposed and implemented immediately to realize the transaction rates needed to run the real-time programmatic bid and delivery [26], [57]. The Layer 2 solutions need to be incorporated by the providers in order to minimize the latency and transaction costs to make the logging of high level, low value ad events economically feasible.

More importantly, global privacy regulations (such as GDPR) should be observed with the implementation of hybrid models of data storage, i.e., sensitive personal data (PCD) will be maintained off-chain in encrypted and centralized vaults, but only cryptographic verifications and metadata hashes will be recorded on the immutable ledger [59, 63, 64]. The CRAB (Create, Read, Append, Burn) model that providers have to adopt has to manage the right to erasure by effectively destroying the encryption keys associated with the off-chain data has to be implemented in a way that does not violate the immutability of the ledger [65]. Lastly, the DLT systems should follow a philosophy of Secure by Design and combine the concept of layered defense [56] and AI-driven security mechanisms to constantly detect threats [42].

In the case of Regulators and Policy Makers (Governance Strategy): To gain a legal clarity and speed up the adoption of DLT in multi-jurisdictional markets, policy harmonization is necessary. The regulators should turn their attention to creating the coherent frameworks that will specify the responsibility of data controllers in the context of decentralized networks, as well as define the liability routes [45]. Also, regulators should officially identify and certify advanced technical solutions, including irreversible destruction of key (the CRAB model) as a valid and legal tool of satisfying the rights to erasure of data subject under the current privacy legislation [60, 65]. Legal professionals, technologists, and regulators should collaborate to develop flexible model governance that honors the benefits of DLT and basic privacy.

6.3. Limitation of the Research and Future Directions.

Low adoption is another limitation of current research, as they are mainly based on pilot program data and conceptual modeling, as opposed to generalized market outcomes [66]. The quantitative information on ROI is still developing particularly due to the implementation of DID effect in different social platforms.

Empirical studies should focus on the following in the future:

- **Consumer Behavioral Research**: An experiment on consumer trust reaction to authenticity disclosures based on blockchain technology to identify whether this technology can actually boost consumer engagement and intention to purchase [67].
- **Interoperability Standards**: Exploring the creation of effective cross-chain standards between various solutions of AdTech DLT (e.g., how Hyperledger Fabric can interact with an Ethereum sidechain).
- **More Sophisticated Cryptographic Auditing**: Studies on the development of privacy-preservation cryptographic schemes (e.g. fully homomorphic encryptions) to perform identity checks at scale, with no requirement to reveal a raw value [31, 63].
- **Decentralized Forensics**: The creation of strong forensic analysis systems that can examine encrypted information and detect fraud in decentralized, immutable systems [62].

The successful deployment of DLT promises a transparent, efficient, and fraud-resistant digital media ecosystem, contingent upon resolving these crucial technical, regulatory, and commercial challenges through strategic collaboration.

7. ACKNOWLEDGMENTS

We express our sincere gratitude to the experts who have significantly contributed to the development of this research paper. Their insights, guidance, and support were invaluable in shaping this work. We would like to particularly acknowledge the contributions of the following authors:

Vengesai Mavengano, Yeshiva University - Digital Marketing and Media (Email: vmavenga@mail.yu.edu), for leading the research and manuscript preparation.

Gladstone Tonderai Chichaya, Yeshiva University - Digital Marketing and Media (Email: chichayagladstone@gmail.com), for his critical analysis and valuable inputs throughout the study.

Tingaitei Chisoro, Yeshiva University - Digital Marketing and Media (Email: ashleytee63@gmail.com), for her support in data interpretation and framework validation.

Anna Tanyaradzwa Audrey Chingono, Yeshiva University - Digital Marketing and Media (Email: achingon@mail.yu.edu), for her technical expertise and assistance in data analysis.

We also appreciate the collaborative spirit and commitment shown by all contributors, whose collective efforts made this research possible.

8. REFERENCES

[1] Khunkhana, F. n.d. “Ad Tech with Blockchain: Improving Trust and Visibility.” Faijal Khunkhana Blogs. Accessed January 10, 2025. https://www.khunkhanablogs.com/2025/01/ad-tech-with-blockchain-improving-trust.html.

[2] ACA (Association of Canadian Advertisers). n.d. “New Study Shows Effective Programmatic Ad Buys Remain Elusive Due To Transparency And Complexity Concerns |.” Accessed November 10, 2025. https://acaweb.ca/en/about/for-media/new-study-shows-effective-programmatic-ad-buys-remain-elusive-due-transparency-complexity-concerns/.

[3] Alda, M. n.d. “Influencer marketing worldwide - statistics & facts.” Statista. Accessed November 28, 2025. https://www.statista.com/topics/2496/influence-marketing/#topicOverview.

[4] Lammertink, S. n.d. “The Future of Influencer Marketing for direct-to-consumer brands.” The Cirqle. Accessed November 12, 2025. https://thecirqle.com/blog-post/the-future-of-influencer-marketing-for-direct-to-consumer-brands.

[5] Digital Marketing Institute. 2024. “20 Surprising Influencer Marketing Statistics.” Accessed November 28, 2025. https://digitalmarketinginstitute.com/blog/20-influencer-marketing-statistics-that-will-surprise-you.

[6] Lohar, A. n.d. “Ethical Influencer Marketing: Building Trust and Authenticity in the Digital Age.” CyberMarketing Hub. Accessed November 11, 2025. https://gracker.ai/cybersecurity-marketing-101/ethical-influencer-marketing.

[7] Spider Af. n.d. “Ad Fraud 2025: Top Threats & Solutions for Advertisers.” Spider Af Articles. Accessed November 28, 2025. https://spideraf.com/articles/ad-fraud-trends-2025-key-threats-and-how-to-combat-them.

[8] Zheng, C. n.d. “38+ influencer marketing statistics: The game-changer in 2024.” Firework. Accessed November 28, 2025. https://firework.com/blog/influencer-marketing-statistics.

[9] Traffic Guard. n.d. “Click Fraud Statistics 2026: Global Costs & Key Trends.” Accessed November 12, 2025. https://www.trafficguard.ai/click-fraud-statistics.

[10] Awoleye, J., S. Mavire, T. B. Chatukuta, and E. Katenda. 2025. “AN ANALYTICS-DRIVEN, METRICS-BASED FRAMEWORK FOR OPTIMISING SECURITY AND PERFORMANCE IN HYBRID ENTERPRISE ZERO TRUST DEPLOYMENTS.” *Int J Comput Appl* 187, no. 16 (June): 42–56. doi: 10.5120/ijca2025925221.

[11] Ogunsanya, V. A., et al. 2025. “The Role of Artificial Intelligence in Strengthening Privacy and Security in the Era of Cyber Crime and Digital Forensics.” *Int J Sci Manag Res* 08, no. 05: 177–98. doi: 10.37502/IJSMR.2025.8515.

[12] Skandul, Emily. n.d. “Budgets on the Blockchain: Maximally Transparent Transactions.” Institute Global. Accessed November 28, 2025. https://institute.global/insights/tech-and-digitalisation/budgets-blockchain-maximally-transparent-transactions.

[13] Rapid Innovation. n.d. “Blockchain Oracles: Essential Guide to Connecting On-Chain and Off-Chain Data.” Accessed November 15, 2025. https://www.rapidinnovation.io/post/blockchain-oracles-essential-guide-connecting-on-chain-off-chain-data.

[14] Raghavendra, G. 2024. “Blockchain Technology In Digital Advertising: Transparency, Fraud Prevention And Trust.” *Educ Adm Theory Pract* 30, no. 4: 3041–49. doi: 10.53555/kuey.v30i4.1477.

[15] Mashinge, R., K. B. Muhwati, K. Magora, and J. Awoleye. 2025. “MITIGATING DEEPFAKE-BASED IMPERSONATION AND SYNTHETIC DATA RISKS IN REMOTE HEALTHCARE SYSTEMS.” *Int J Comput Appl* 187, no. 41 (September): 27–42. doi: 10.5120/ijca2025925724.

[16] Humanity Protocol. n.d. “The Role of WTO in the Fight Against Poverty.” Accessed November 29, 2025. https://www.humanity.org/blog/the-role-of-did-in-the-fight-against-bots.

[17] Swartz, J., H. Nagarsheth, and O. Capel. n.d. “How blockchain will disrupt digital advertising.” Kearney. Accessed November 29, 2025. https://www.kearney.com/service/digital-analytics/article/-/insights/how-blockchain-will-disrupt-digital-advertising.

[18] Verma, A., C. Ciliberto, and L. Bhatia. 2025. “AI and Blockchain-Driven Digital Marketing.” In *Strategic Blueprints for AI-Driven Marketing in the Digital Era*, 365–92. doi: 10.4018/979-8-3373-3897-2.ch011.

[19] Qureshi, A., and D. Megías Jiménez. 2020. “Blockchain-Based Multimedia Content Protection: Review and Open Challenges.” *Appl Sci* 11, no. 1 (December): 1. doi: 10.3390/app11010001.

[20] Akingbade, A. n.d. “Distributed Ledger Technology: A Complete Overview.” UEEx Technology. Accessed November 12, 2025. https://blog.ueex.com/distributed-ledger-technology/.

[21] Strycharz, J., and C. M. Segijn. 2024. “Ethical side-effect of dataveillance in advertising: Impact of data collection,

trust, privacy concerns and regulatory differences on chilling effects." *J Bus Res* 173 (February): 114490. doi: 10.1016/j.jbusres.2023.114490.

[22] Ballandies, M. C., M. M. Dapp, and E. Pournaras. 2022. "Decrypting distributed ledger design—taxonomy, classification and blockchain community evaluation." *Cluster Comput* 25, no. 3 (June): 1817–38. doi: 10.1007/s10586-021-03256-w.

[23] PRISM. n.d. "Decentralized Ledger → Term." Accessed November 29, 2025. https://prism.sustainability-directory.com/term/decentralized-ledger/.

[24] Jolene. n.d. "Consensus Mechanisms: How DLT Systems Agree." Medium. Accessed November 12, 2025. https://hellojojo.medium.com/consensus-mechanisms-how-dlt-systems-agree-a4a125d0f782.

[25] Singh, D. n.d. "What is Blockchain Scalability and Its Impact on Growth?" Debut Infotech. Accessed November 29, 2025. https://www.debutinfotech.com/blog/what-is-blockchain-scalability.

[26] Huang, J., Y. Niu, X. Li, and Z. Li. 2025. "Comparative Analysis of Blockchain Systems." May. http://arxiv.org/abs/2505.08652.

[27] Webisoft. n.d. "How Blockchain Scalability Impacts Adoption & Efficiency." Accessed November 15, 2025. https://webisoft.com/articles/blockchain-scalability/.

[28] IBM Documentation. n.d. "Hyperledger Fabric." Accessed November 29, 2025. https://www.ibm.com/docs/en/blockchain-platform/2.5.2?topic=reference-hyperledger-fabric.

[29] IBM. n.d. "What Is Hyperledger Fabric?" IBM Developers. Accessed November 22, 2025. https://www.ibm.com/think/topics/hyperledger.

[30] Reed, D., M. Sporny, and C. Allen. 2019. "Decentralized Identifiers (DIDs) v1.0." W3C, November, 1–56. Accessed November 29, 2025. https://www.w3.org/TR/did-1.0/.

[31] Mazzocca, C., A. Acar, and S. Uluagac. 2025. "A Survey on Decentralized Identifiers and Verifiable Credentials." *IEEE Commun Surv Tutor* 27, no. 4: 1–28. doi: 10.1109/COMST.2025.3543197.

[32] Cheng, J.-C., N.-Y. Lee, C. Chi, and Y.-H. Chen. 2018. "Blockchain and smart contract for digital certificate." In *2018 IEEE International Conference on Applied System Invention (ICASI)*, 1046–51. IEEE. doi: 10.1109/ICASI.2018.8394455.

[33] Pranata, Sudadi, Fajrinoor Fanani, Dini Hidayati, Rosa Lesmana, and Zinhle Ndlovu. 2025. "Implementation of Smart Contracts in TikTok Influencer Marketing." *Blockchain Front Technol* 4, no. 2: 84–97. doi: 10.34306/bfront.v4i2.688.

[34] Gain Scale. n.d. "Blockchain & Programmatic Ads with Transparent Supply Chains." Accessed November 29, 2025. https://www.gainscale.co/blockchain-unleashed-revolutionizing-programmatic-advertising-with-transparent-supply-chains/.

[35] GenX AI. n.d. "Blockchain for Influencer Marketing Transparency: GenX AI Revolutionizing Trust in the Digital Age." Accessed November 29, 2025. https://medium.com/@genxaiblogs/blockchain-for-influencer-marketing-transparency-genx-ai-revolutionizing-trust-in-the-digital-age-592e9e081f35.

[36] Willson, M. n.d. "Blockchain on Marketing and Advertising." Blockchain Council. Accessed November 12, 2025. https://www.blockchain-council.org/blockchain/impact-of-blockchain-on-marketing-and-advertising/.

[37] Sporny, Manu, D. Longley, D. Chadwick, and Ivan Herman. 2024. "Verifiable Credentials Data Model v2.0." W3C Recommendation Draft 19 October 2024. Accessed November 29, 2025. https://www.w3.org/TR/vc-data-model-2.0/.

[38] Alj, K. S., R. Akkaoui, and Y. S. Alj. 2025. "A Blockchain-based Framework for Academic Credential Verification and Revocation: Morocco Case Study." In *2025 IEEE 8th Congress on Information Science and Technology (CiSt)*, 571–76. IEEE. doi: 10.1109/CiSt65886.2025.11224125.

[39] Dutta, S., and P. Rao. 2022. "Blockchain in Digital Identity Management." *IEEE Blockchain Trans* 10: 345–59. Accessed November 15, 2025. https://www.blockchainappfactory.com/blockchain-identity-management.

[40] Tencent Cloud. n.d. "How can digital identity authentication be combined with smart contracts to achieve automated trust?" Accessed November 18, 2025. https://www.tencentcloud.com/techpedia/127117.

[41] Laneau, A. n.d. "Leveraging Blockchain and Decentralized Identity to Combat Ad Fraud: A Strategic Analysis." HackerNoon. Accessed November 10, 2025. https://hackernoon.com/leveraging-blockchain-and-decentralized-identity-to-combat-ad-fraud-a-strategic-analysis.

[42] Abbas, Rianat, Sunday Jacob Nwanyim, Joy Awoleye Adesina, Augustine Udoka Obu, Adetomiwa Adesokan, and Jeremiah Folorunso. 2025. "Secure by design - enhancing software products with AI-Driven security measures." *Comput Sci IT Res J* 6, no. 3 (April): 184–200. doi: 10.51594/csitrj.v6i3.1880.

[43] Hassan, S., and P. De Filippi. 2021. "Decentralized Autonomous Organization." *Internet Policy Rev* 10, no. 2 (April). doi: 10.14763/2021.2.1556.

[44] Nnadi, P. D., and Chikezie Sunday Onoh. 2025. "EFFECT OF DISTRIBUTED LEDGER TECHNOLOGY (DLT) ON PERFORMANCE OF DEPOSIT MONEY BANKS IN ENUGU STATE." *Res J Bus Adm* 13, no. 2. doi: 10.5281/zenodo.15706842.

[45] Zafar, A. 2025. "Reconciling blockchain technology and data protection laws: regulatory challenges, technical solutions, and practical pathways." *J Cybersecurity* 11, no. 1 (January). doi: 10.1093/cybsec/tyaf002.

[46] Prakashchand, L. 2024. "Industry News 2024 Beyond the Blockchain Bubble Distributed Ledger Technology for a Resilient Audit Landscape." ISACA. Accessed November 29, 2025. https://www.isaca.org/resources/news-and-trends/industry-news/2024/beyond-the-blockchain-bubble-distributed-ledger-technology-for-a-resilient-audit-landscape.

[47] Debreceny, R., G. L. Gray, W. Tham, K. Goh, and P. Tang. 2003. "The Development of Embedded Audit Modules to

Support Continuous Monitoring in the Electronic Commerce Environment." *Int J Audit* 7, no. 2 (July): 169–85. doi: 10.1111/1099-1123.00067.

[48] Ledger Insights. n.d. "Mediaocean, IBM advertising blockchain goes live." Accessed November 30, 2025. https://www.ledgerinsights.com/mediaocean-ibm-advertising-blockchain/.

[49] Simões, E. P., and A. B. de Sousa Júnior. 2020. "Auditoria interna: contextualização teórica e aplicações em empresas comerciais brasileiras." *Entrepreneurship* 4, no. 2 (April): 13–24. doi: 10.6008/CBPC2595-4318.2020.002.0002.

[50] Chen, S. 2025. "Blockchain-Enabled Traceability Framework to Improve Transparency in Supply Chain Management." *Inf Resour Manag J* 38, no. 1 (October): 1–29. doi: 10.4018/IRMJ.389708.

[51] Mediaocean Team. n.d. "Mediaocean and IBM partner to integrate blockchain across the media ecosystem." Accessed November 30, 2025. https://www.mediaocean.com/ibm-blockchain.

[52] Takyar, Akash. n.d. "Blockchain Advertising use cases - Add Transparency and Privacy." LeewayHertz. Accessed December 1, 2025. https://www.leewayhertz.com/blockchain-advertising-use-cases/.

[53] Anastasov, K. n.d. "AI Disclosure Rules by Platform: YouTube, Instagram/Facebook, and TikTok Labeling Guide." Influencer Marketing Hub. Accessed December 1, 2025. https://influencermarketinghub.com/ai-disclosure-rules/.

[54] Syed, H. A. n.d. "Blockchain in Journalism: Restoring Trust in Media." Medium. Accessed December 1, 2025. https://medium.com/@syedhasnaatabbas/blockchain-in-journalism-restoring-trust-in-media-90e7a74dcbd2.

[55] Bhowmik, D., and T. Feng. 2017. "The multimedia blockchain: A distributed and tamper-proof media transaction framework." In *International Conference on Digital Signal Processing, DSP*. doi: 10.1109/ICDSP.2017.8096051.

[56] Mavire, S., K. B. Muhwati, N. Kota, and J. A. Awoleye. 2025. "Mitigating Ransomware in the Energy and Healthcare Sectors through Layered Defense Strategies." *Int J Sci Manag Res* 08, no. 04: 143–66. doi: 10.37502/IJSMR.2025.8609. *(Note: This is a duplicate of entry [9] from the previous request, maintained in sequence.)*

[57] Garg, S. n.d. "Layer-1 Vs. Layer-2: The Blockchain Scaling Solutions." Solulab. Accessed November 13, 2025. https://www.solulab.com/blockchain-layer-1-vs-layer-2-scaling-solutions/.

[58] Mavire, S., K. B. Muhwati, C. D. Kudaro, and J. Awoleye. 2025. "A Federated Learning Approach to Secure AI-Based Patient Outcome Prediction Across Hospitals." *Int J Sci Manag Res* 8 (October). doi: 10.37502/IJSMR.2025.8806. *(Note: This is a duplicate of entry [5] from the previous request, maintained in sequence.)*

[59] Ambros. n.d. "How Immutable Ledgers Impact GDPR Compliance." Serverion. Accessed November 18, 2025. https://www.serverion.com/uncategorized/how-immutable-ledgers-impact-gdpr-compliance/.

[60] Godyn, M., M. Kedziora, Y. Ren, Y. Liu, and H. H. Song. 2022. "Analysis of solutions for a blockchain compliance with GDPR." *Sci Rep* 12, no. 1 (September): 15021. doi: 10.1038/s41598-022-19341-y.

[61] Deloitte. 2025. "The impact of blockchain technology on audit." Accessed November 30, 2025. https://digi-solutions.com/the-impact-of-blockchain-technology-on-digital-marketing/.

[62] Awoleye, J., S. Mavire, A. Munyira, and K. Magora. 2025. "FORENSIC ANALYSIS FRAMEWORKS FOR ENCRYPTED CLOUD STORAGE INVESTIGATIONS." *Int J Comput Appl* 187, no. 17 (June): 8–19. doi: 10.5120/ijca2025925241.

[63] Ghafourian, M., et al. 2025. "Blockchain and Biometrics: Survey, GDPR Analysis, and Future Directions." October. http://arxiv.org/abs/2302.10883.

[64] Nododile, T., and C. Nyirenda. 2025. "A Hybrid Blockchain-IPFS Solution for Secure and Scalable Data Collection and Storage in Smart Water Meters." In *2025 IST-Africa Conference (IST-Africa)*, 1–9. IEEE. doi: 10.23919/IST-Africa67297.2025.11060537.

[65] Palomares, J. n.d. "Immutable Yet Compliant: Harmonizing Blockchain with GDPR." EMILDAI. Accessed November 18, 2025. https://emildai.eu/immutable-yet-compliant-harmonizing-blockchain-with-gdpr/.

[66] Difrancesco, R. M., P. Meena, and G. Kumar. 2023. "How blockchain technology improves sustainable supply chain processes: a practical guide." *Oper Manag Res* 16, no. 2 (June): 620–41. doi: 10.1007/s12063-022-00343-y.

[67] Antsipava, D., E. A. van Reijmersdal, J. Strycharz, and G. van Noort. 2025. "Can Blockchain-Based Authenticity Disclosures Increase Consumer Trust in Online Advertising?" *J Advert*. 1–28. doi: 10.1080/00913367.2025.2510233.