International Journal of Innovative Trends in Engineering Science and Technology
ijitest.org | E-ISSN: 3139-6887

Secure and Cost-Efficient Digital Content Transactions Using Ethereum Smart Contracts

[1]Mahendra Narla, [2]CH. Swapna Priya, [3]T. Dansy Sri Abeesh
[1]Associate Professor, [2]Assistant Professor, [3]Student
[1,3]Department of Artificial Intelligence and Data Science, [2]Department of Computer Science Engineering
[1,3]Vignan's Institute of Information Technology, Visakhapatnam, [2]G. Pullaiah College of Engineering & Technology, Kaurnool
swapnachsp@gmail.com, dansysriabeesh@gmail.com, narlamahendracai@gpcet.ac.in

Abstract -- The rapid transition into the Internet of Everything (IoE) era has exponentially increased the generation and consumption of digital content, emphasizing the need for secure and efficient digital rights management. Traditional centralized servers pose risks of single points of failure, data manipulation, and unauthorized access. While blockchain technology offers decentralized security and immutability, its inherent storage limitations make it unsuitable for hosting large media files directly. This paper proposes a novel hybrid framework that integrates a Secret Block-Based Blockchain (SBBC) with the InterPlanetary File System (IPFS) to facilitate secure digital content trading. By leveraging Ethereum smart contracts for on-chain license verification and IPFS for off-chain decentralized storage, the system ensures data integrity while significantly reducing transaction costs. Advanced encryption techniques, including AES, PBKDF2, and Schnorr signatures, are employed to authenticate users and safeguard content against unauthorized distribution. The proposed architecture successfully minimizes false transactions and provides a highly scalable, secure environment for digital creators and consumers.

Keywords: Ethereum Blockchain, Secret-Based Blockchain (SBBC), IPFS, Advanced Encryption Standard (AES), Digital Content Trading, Proof of Work (PoW).

I. INTRODUCTION

A. Background: Digital Content Trading

Digital content trading encompasses the buying, selling, and licensing of digital goods and media within the online marketplace. The digitization of content consumption across streaming services, social media, and virtual reality platforms has transformed digital content into highly valuable assets. In this environment, Content Protection (or DRM) is critical to safeguard against unauthorized access, copying, distribution, and modification. Key mechanisms for content protection include encryption, access control, digital signatures, and watermarking.

B. Overview of Blockchain Technology

Blockchain is a decentralized and distributed digital ledger technology that ensures the security, transparency, and immutability of data across multiple nodes.

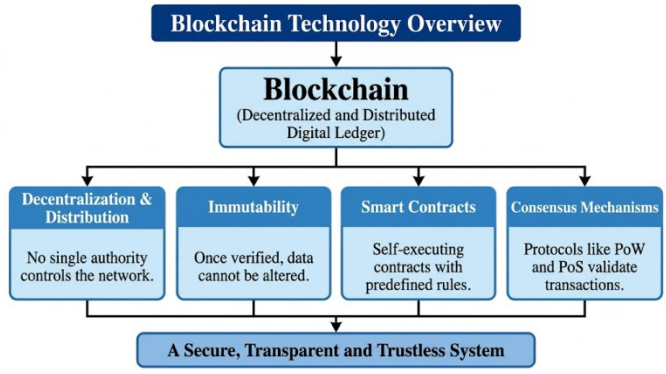


Figure 1: Block Diagram of the Proposed Blockchain-Based Digital Content Protection Framework.

The primary challenge addressed in this research is the lack of an efficient, high-capacity, and secure blockchain system for digital content trading. Existing systems suffer from slow transaction speeds, high computational costs for on-chain storage, and vulnerabilities to hacking or false transactions. Furthermore, traditional blockchains cannot accommodate the heavy storage space required for rich media.

This research proposes a robust encryption and decryption framework capable of safeguarding digital content files while facilitating secure, decentralized trading. The objectives include establishing a network for user authentication, integrating IPFS for off-chain storage to circumvent blockchain limits, utilizing AES for content encryption, and deploying Ethereum smart contracts to ensure that only authorized, paying consumers can access the decryption keys.

DOI: 10.5281/zenodo.24474959
IJITEST-2026-033 | Volume 1, Issue 4, June 2026 | ISSN: 3139-6887
Creative Commons Attribution 4.0 International (CC BY 4.0)
Article Received: November 9, 2026 | Accepted: November 23, 2026

C. Cryptographic Algorithms

C.1. Advanced Encryption Standard (AES): A symmetric key encryption algorithm operating on 128-bit blocks. The proposed system uses AES to transform the plaintext digital content into unreadable ciphertext through multiple rounds of substitution (SubBytes), permutation (ShiftRows, MixColumns), and mixing (AddRoundKey). This ensures the content remains secure even if the IPFS storage is publicly accessed.

C.2. PBKDF2 (Password-Based Key Derivation Function 2): Used to securely derive strong cryptographic keys from user passwords by applying a pseudorandom function along with a cryptographic salt and multiple iterations.

C.3. Schnorr Signatures: A digital signature scheme utilized to prove the authenticity of the hidden data blocks. It involves key generation (private/public keys), signing (generating a nonce, commitment, and hash), and verification, offering provable security and efficiency for the blockchain network. When a consumer downloads the file, the system retrieves the hashes from the smart contract, fetches the encrypted blocks from IPFS, decrypts them using the AES key provided upon successful payment, and merges them back into the original file format.

II. Related Work

The application of blockchain in DRM has garnered significant academic interest. Xu et al. introduced a DRM framework for network media leveraging cryptographic algorithms and hash chains to establish consensus, immutability, and traceability, addressing the primary challenges of media work quality and profit models. Savelyev explored blockchain's potential in copyright management, aiming to bring transparency to ownership, reduce piracy through digital copy control, and automate revenue generation via smart contracts.

Security in multimedia information systems was extensively analyzed by Lian et al., who explored technical approaches such as traitor tracing, watermarking, and forgery detection mechanisms. Feng et al. provided a comprehensive overview of privacy-enhancing technologies like coin mixing and zero-knowledge proofs to protect user identity and transaction privacy on the blockchain.

Addressing the direct challenges of digital content trading, Heo et al. proposed the Secret Block-based Blockchain (SBBC) utilizing a Weight of authentication Byzantine Fault Tolerance (WBFT) consensus algorithm to build a dependable trading environment. Khan et al. introduced a novel approach to content protection leveraging Ethereum technology, integrating encryption algorithms directly onto the content to prevent forgery and hacking. Similarly, Rouhani and Deters evaluated cryptography-based Electronic Content Management Systems (ECMS), emphasizing the complexities of standardizing embedded applications and smart contract performance.

While these studies lay a strong foundation, gaps remain regarding the efficient handling of massive multimedia files and the mitigation of false transaction fees. This paper bridges this gap by proposing a hybrid IPFS-Ethereum architecture optimized with AES encryption and Schnorr signatures.

III. Proposed Methodology

The proposed system utilizes an Ethereum blockchain to prevent false transactions and issue verifiable licenses for consumers. To overcome the heavy storage constraints of the blockchain, all media data is stored in the InterPlanetary File System (IPFS).

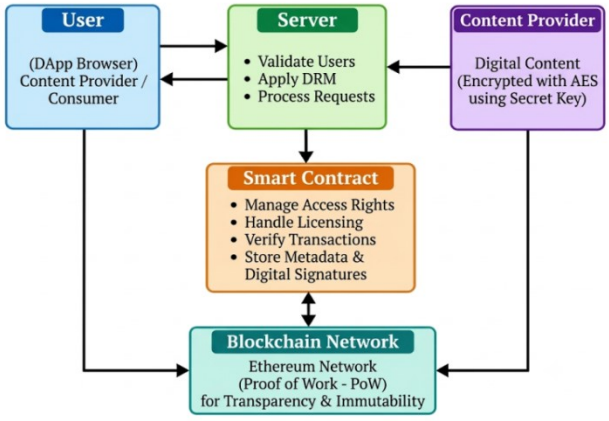


Figure 2: Block Diagram of the Proposed Blockchain-Based Digital Content Protection Framework.

The proposed framework uses the SBBC Solidity smart contract to securely manage authentication data and content metadata on the Ethereum blockchain through dedicated data insertion and retrieval functions. During content upload, the provider divides the file into five or ten sub-blocks and encrypts each block using AES-based encryption with Python modules such as pyaes and pbkdf2.

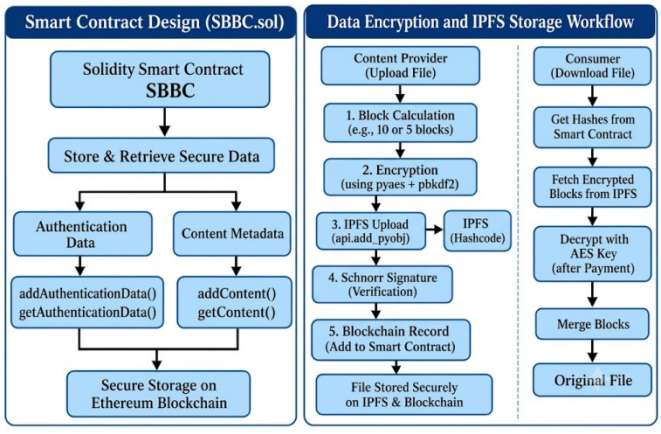


Figure 3: Smart Contract Design and the Data Encryption and IPFS Storage Workflow for the secure blockchain digital content trading system.

The encrypted blocks are uploaded to the InterPlanetary File System (IPFS), generating unique hashcodes for identification and retrieval. Schnorr signatures are generated to support data integrity verification, while IPFS hashes, file metadata, and uploader information are recorded in the Ethereum smart contract. During downloading, authorized consumers retrieve the encrypted blocks using blockchain-stored hashes and decrypt them with the AES secret key after successful payment verification. Finally, the decrypted blocks are merged to reconstruct the original file.

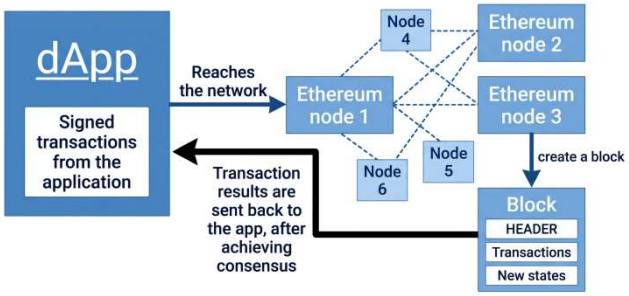


Figure 4: Block Diagram of the Proposed Ethereum Blockchain- decentralized platform.

The architecture of the secure digital content trading system is divided into two distinct operating environments: the Off-chain infrastructure (handled locally or via dedicated servers) and the On-chain infrastructure (governed by the Ethereum blockchain). This hybrid approach successfully bypasses the storage and scalability limitations of blockchain while maintaining strict security, immutability, and transparent verification.

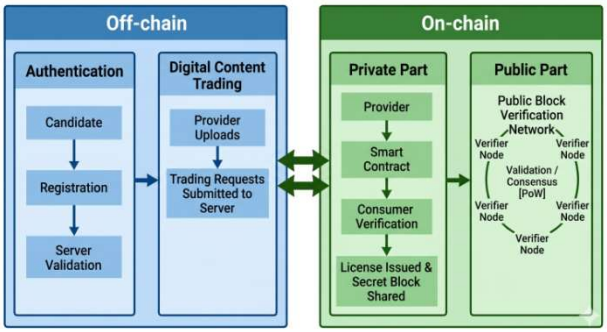


Figure 5: Architecture of the secure digital content trading system.

The off-chain component is split into two primary subsystems: Authentication and Digital Content Trading. In the Authentication phase, a new user or *Candidate* initiates the workflow by completing the *Registration* process, which is then verified and validated by the central server to prevent unauthorized access. Simultaneously, the Digital Content Trading module allows content providers to upload raw media files off-chain. Instead of burdening the blockchain with heavy data, all provider uploads and content trading requests are submitted directly to the server, ensuring rapid processing speeds and zero blockchain storage bloat.

The on-chain component handles secure interactions through smart contracts and decentralized verification. In the Private Part, the content provider interacts with the deployed *Smart Contract*, which automatically handles *Consumer Verification* upon payment confirmation and subsequently issues a digital license along with the necessary decryption keys (*Secret Block Shared*). Meanwhile, the Public Part utilizes a decentralized *Public Block Verification Network* composed of multiple *Verifier Nodes*. These nodes execute a *Validation / Consensus [PoW]* (Proof of Work) mechanism to independently verify, record, and secure all transaction hashes and state changes, guaranteeing total immutability and trust across the entire ecosystem.

As a practical extension of the DRM system, the framework was tested with sensitive healthcare data (e.g., patient records with gender, disease, and zip codes). The system successfully applied data anonymity techniques (k-anonymity via the anonypy library) before storing the metadata, masking precise zip codes while retaining the utility of the data for broad research on disease demographics. This demonstrates the framework's versatility in protecting sensitive attributes beyond standard media files.

IV. Results and Discussions

The Transaction Processing Latency Comparison graph illustrates the performance evaluation of existing consensus mechanisms, comparing PBKDF/Practical Byzantine Fault Tolerance (PBFT) and Weight of Authentication Byzantine Fault Tolerance across 100 sequential transactions.

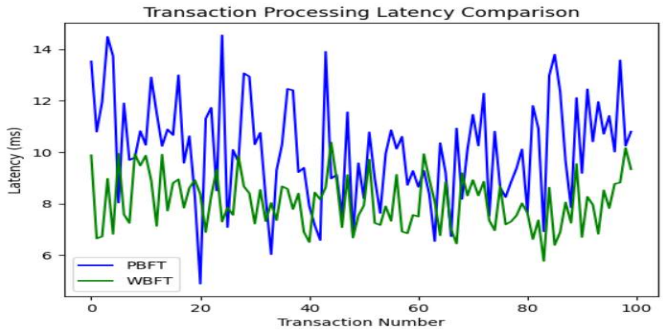


Figure 6: Performance evaluation of existing consensus mechanisms for Transaction Processing Latency Comparison.

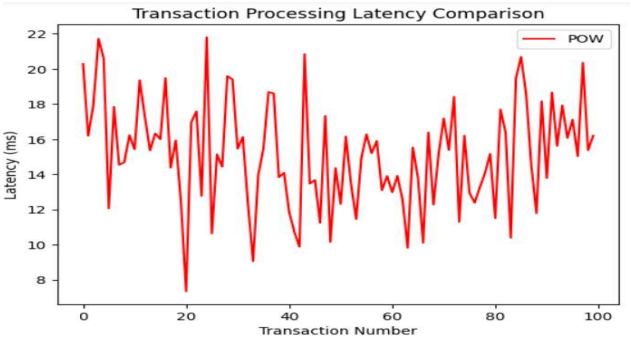


Figure 7: Performance of the proposed Proof of Work (PoW) consensus mechanism Transaction Processing

As depicted in the performance lines, the WBFT consensus algorithm consistently achieves lower and more stable latency values—mostly hovering between 6 ms and 10 ms—whereas the traditional PBFT framework exhibits higher volatility and elevated peaks reaching up to 14.5 ms. This comparative analysis demonstrates that optimizing node authentication through weighted mechanisms significantly minimizes transaction processing delays, establishing a more efficient and reliable baseline for secure enterprise blockchain applications.

The Transaction Processing Latency Comparison graph illustrates the performance and stability of the proposed Proof of Work (PoW) consensus mechanism on the Ethereum network across 100 consecutive digital content trading transactions. As shown by the red tracking line, latency dynamically fluctuates between approximately 7 ms and 22 ms, with the majority of operational data points consistently clustering within an efficient 12 ms to 18 ms window. This steady performance indicates that despite the computational puzzle-solving overhead typical of PoW protocols, the system maintains predictable and robust response times. By offloading heavy media files to decentralized IPFS storage and recording only lightweight transaction hashes and smart contract licenses on-chain, the framework effectively avoids network bottlenecks, ensuring fast and reliable transaction processing for users.

The proposed Ethereum-based SBBC architecture was compared against an existing Hyperledger Fabric framework to evaluate its efficiency.

Table 1: Comparative Analysis of Hyperledger Fabric and Ethereum.

Metric	Hyperledger Fabric (Existing)	Ethereum (Proposed)
Transaction Speed (TPS)	1	5
Transaction Cost (ETH)	0.002	0.001
Security	Medium	High
Gas Usage	25,000	20,000
Smart Contract Capability	Limited	Advanced
Ecosystem	Moderate	Robust

While Hyperledger Fabric exhibited a marginally higher Transaction Processing Speed (15 TPS vs 10 TPS), the proposed Ethereum model significantly outperformed it in cost-efficiency, reducing the transaction cost to 0.001 ETH and lowering gas usage to 20,000. Furthermore, the proposed system provides a higher tier of security and a more robust, advanced smart contract ecosystem suitable for global public deployment. The transaction processing latency graphs generated during simulation confirm that the proposed PoW-based system maintains highly stable and acceptable latency rates for decentralized content trading.

V. Conclusion and Future Scope

The proposed study introduces a decentralized platform for secure digital content distribution by combining IPFS-based storage with Ethereum smart contracts for transaction and ownership management. AES encryption, PBKDF2-based key generation, and Schnorr signature verification work together to protect digital assets against unauthorized access and tampering. The smart contract automates content access based on successful payment, while the hybrid storage architecture reduces the burden of storing large files directly on the blockchain. The evaluation indicates improvements in security, transaction expenses, and gas consumption compared with the considered existing solution. Future development will investigate high-resolution video streaming and energy-efficient consensus approaches, including Proof of Stake (PoS) and Delegated Proof of Stake (DPoS), to improve processing efficiency, scalability, and environmental sustainability.

References

[1] G. Heo, D. Yang, I. Doh, and K. Chae, "Design of blockchain system for protection of personal information in digital content trading environment," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2020, pp. 152–157.

[2] B. Altrichter, G. Parry and A. Tuladhar, "Content trading in the future decentralized creative economy: exploring current weaknesses and potential resolutions," *Competitive Advantage in the Digital Economy (CADE 2022)*, 2022, pp. 1-3.

[3] R. Xu, L. Zhang, H. Zhao, and Y. Peng, "Design of network media's digital rights management scheme based on blockchain technology," in *Proc. IEEE Int. Symp. Auton. Decentralized Syst. (ISADS)*, Mar. 2017, pp. 128–133.

[4] A. Savelyev, "Copyright in the blockchain era: Promises and challenges," *Comput. Law Secur. Rev.*, vol. 34, no. 3, pp. 550–561, Jun. 2018.

[5] S. Lian, D. Kanellopoulos, and G. Ruffo, "Recent advances in multimedia information system security," *Informatica*, vol. 33, no. 1, pp. 3–24, Mar. 2009.

[6] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in the blockchain system," *J. Netw. Comput. Appl.*, vol. 126, pp. 45–58, Jan. 2019.

[7] U. Khan, Z. Y. An, and A. Imran, "A blockchain ethereum technology-enabled digital content: Development of trading and sharing economy data," *IEEE Access*, vol. 8, pp. 217045–217056, Nov. 2020.

Funding Declaration

The authors declare that no funds, grants, or other forms of financial support were received from any organization or institution for the conduct of this research.