International Journal of Computer Techniques–IJCT Volume 13 Issue 2, March-April - 2026

Open Access and Peer Review Journal ISSN 2394-2231 https://ijctjournal.org/

RESEARCH ARTICLE OPEN ACCESS

Blockchain-Based Authentication Systems for Securing E-Commerce Transactions: Design, Prototype Implementation, and Comparative Evaluation

Onyeagoziri Precious Akams
School of Computing, Engineering and Physical Sciences
University of the West of Scotland, Paisley, Scotland, UK
preciousakams@yahoo.com

--*************************--------------------------------

Abstract:

E-commerce platforms are increasingly targeted by sophisticated cyber-attacks that exploit the inherent vulnerabilities of centralised authentication architectures. Password-based systems, two-factor authentication, and centralised identity stores have demonstrated persistent susceptibility to phishing, credential stuffing, man-in-the-middle interception, and large-scale data breaches. This paper investigates the design, implementation, and evaluation of a blockchain-based authentication system as a structural response to these limitations. The proposed system leverages Ethereum's public-key cryptographic infrastructure, MetaMask wallet integration, Web3.js, JSON Web Tokens (JWT), React.js, and Node.js to deliver a decentralised, tamper-proof, and privacy-preserving authentication flow for e-commerce applications. A proof-of-concept prototype was built and evaluated against conventional authentication methods across eleven analytical dimensions, including security architecture, data integrity, identity management, scalability, trust models, and regulatory alignment. Results confirm that the blockchain-based approach eliminates credential database attack surfaces, enables non-repudiable transaction signing, supports Zero-Knowledge Proof (ZKP) verification, and implements Self-Sovereign Identity (SSI) principles that return data ownership to users. Scalability under high transaction volumes and user onboarding complexity are identified as the primary adoption barriers, suggesting that hybrid architectures may offer the most pragmatic near-term deployment pathway. The study contributes an empirically grounded, real-world implementation perspective to the growing literature on blockchain security applications, and provides actionable guidance for e-commerce operators, security practitioners, and researchers exploring decentralised identity systems.

Keywords — **Blockchain Authentication, E-Commerce Security, Ethereum, Metamask, Decentralised Identity, Zero-Knowledge Proofs, Self-Sovereign Identity, JWT, Smart Contracts, Credential Stuffing, Public-Key Cryptography**.

--*************************--------------------------------

I.INTRODUCTION

The global e-commerce sector has experienced extraordinary growth over the past decade, with worldwide online retail revenues exceeding $5.8 trillion in 2023 and projected to surpass $8 trillion by 2027 (Statista, 2024). This expansion has been accompanied by an equally significant escalation in cybercrime targeting digital commerce platforms. The volume of sensitive data processed by e-commerce systems, including payment credentials, personal identifiers, shipping addresses, and behavioural profiles, makes them high-value targets for adversaries operating across the spectrum from opportunistic script kiddies to organised criminal syndicates and nation-state actors.

At the core of e-commerce security lies the authentication problem: how can a platform reliably verify the identity of users and the integrity of transactions in an open, adversarial network environment? Traditional approaches to this problem have relied primarily on centralised authentication mechanisms, username-password combinations, server-side session management, and increasingly, two-factor authentication (2FA) via

SMS or authenticator apps. While these mechanisms have served as workable solutions during the formative years of digital commerce, their architectural foundations are fundamentally fragile. Centralised credential stores represent singular, high-value attack targets. Passwords are routinely reused across platforms, creating cascading breach risks. 2FA implementations dependent on SMS are vulnerable to SIM-swapping and SS7 protocol attacks. Trusted third-party Certificate Authorities, which underpin SSL/TLS and traditional Public Key Infrastructure (PKI), have experienced high-profile compromises (Wilson and Ateniese, 2015).

Blockchain technology presents a structurally different approach to authentication. By distributing trust across a decentralised network of cryptographically linked nodes, eliminating central credential repositories, and enabling users to authenticate through mathematically verifiable signatures rather than shared secrets, blockchain addresses the root architectural vulnerabilities of conventional systems. The technology's core properties, immutability, decentralisation, transparency, and programmability via smart contracts, create a foundation for authentication that is resistant to the systemic failures that plague centralised alternatives (Kshetri, 2017; Zheng et al., 2018).

This paper investigates the practical application of blockchain technology as an authentication mechanism for e-commerce platforms. It makes three principal contributions: first, a detailed architectural proposal for a blockchain-based authentication system integrated with standard web development technologies; second, a working proof-of-concept prototype implemented on the Ethereum blockchain using MetaMask wallet integration; and third, a systematic comparative evaluation of the proposed system against traditional authentication methods across eleven analytical dimensions. The research is guided by the question: How can blockchain technology be leveraged to provide a secure, decentralised, and practically deployable authentication solution for e-commerce transactions?

The remainder of this paper is organised as follows. Section 2 reviews the relevant literature on blockchain technology, authentication mechanisms, and e-commerce security threats. Section 3 presents the proposed system architecture and design rationale. Section 4 describes the prototype implementation methodology. Section 5 presents the comparative analysis results and discussion. Section 6 addresses limitations and future research directions. Section 7 concludes the paper.

II. BACKGROUND AND LITERATURE REVIEW

A. Evolution and Core Properties of Blockchain Technology

Blockchain technology was introduced by (Nakamoto 2008) as the underlying infrastructure for Bitcoin, a peer-to-peer electronic cash system. At its core, a blockchain is a distributed ledger technology (DLT) that maintains a continuously growing list of records, called blocks, which are cryptographically linked to form an immutable chain. Each block contains a cryptographic hash of the preceding block, a timestamp, and transaction data. This structure ensures that any retroactive alteration of a recorded block would invalidate all subsequent blocks, requiring the collusion of the majority of network nodes to succeed, a computationally and economically prohibitive task for well-established networks (Zheng et al., 2017).

The technology has evolved through several generational stages. Blockchain 1.0 (2008–2013) was dominated by cryptocurrency applications, with Bitcoin establishing the foundational concepts of decentralised consensus and cryptographic transaction verification. Blockchain 2.0 (2013–2015) saw the emergence of programmable blockchain platforms, most notably Ethereum, which introduced Turing-complete smart contracts, a self-executing code stored on the blockchain that automatically enforces agreement terms when predefined conditions are met (Buterin, 2014). Blockchain 3.0 and beyond (2015–present) has focused on scalability, interoperability, and enterprise integration, producing platforms such as Hyperledger Fabric, Polkadot, and Cardano, each optimised for specific use-case requirements.

The core properties that make blockchain relevant to authentication include: decentralisation, which eliminates single points of failure by distributing consensus across multiple independent nodes; immutability, which ensures that recorded data cannot be altered without network-wide consensus; transparency, which allows any participant to independently verify transactions; and programmability, which enables complex authentication logic to be encoded in smart contracts that execute automatically and transparently (Voshmgir and Zargham, 2020). Together, these properties address the structural vulnerabilities inherent in centralised authentication architectures.

B. Authentication Mechanisms in Blockchain Systems

Blockchain systems employ a layered suite of authentication mechanisms that collectively provide stronger security guarantees than conventional approaches.

I. Public-Key Cryptography:

All blockchain-based authentication is grounded in asymmetric cryptography. Each user possesses a private key, which is a secret large random number, and a corresponding public key derivable from it. To authenticate, a user signs a message or transaction with their private key, producing a digital signature. Any verifier can confirm the signature's authenticity using the public key, without ever accessing the private key. This eliminates the need for shared secrets, a fundamental vulnerability of password-based systems, because no sensitive credential is ever transmitted or stored on a server (Zheng et al., 2018). Ethereum implements this through the Elliptic Curve Digital Signature Algorithm (ECDSA) over the secp256k1 curve.

II. Zero-Knowledge Proofs:

Zero-Knowledge Proofs (ZKPs) are cryptographic protocols enabling one party (the prover) to demonstrate knowledge of a value to another party (the verifier) without revealing the value itself (Goldwasser, Micali and Rackoff, 1989). In authentication contexts, ZKPs allow a user to prove they satisfy authentication criteria, such as possessing a valid credential, meeting an age threshold, or holding a minimum account balance without disclosing the underlying data. This property is particularly valuable in e-commerce, where authentication requirements frequently intersect with data privacy obligations under regulations such as the GDPR. Practical ZKP constructions used in blockchain systems include Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs), deployed in privacy coins such as Zcash, and Zero-Knowledge Scalable Transparent Argument of Knowledge (zk-STARKs) which eliminate the trusted setup requirement of zk-SNARKs.

III. Decentralised Identifiers and Self-Sovereign Identity:

Decentralised Identifiers (DIDs) are a W3C-standardised identifier format rooted in blockchain records, enabling verifiable, self-sovereign digital identities (W3C, 2022). Unlike conventional identifiers like, email addresses, usernames, national ID numbers, which are controlled by issuing organisations, DIDs are owned and controlled by their subjects. A DID resolves to a DID Document containing the subject's public keys, authentication methods, and service endpoints. Verifiable Credentials issued against a DID can attest to attributes like age, qualifications, membership, without requiring centralised identity providers. The Self-Sovereign Identity (SSI) paradigm built on DIDs gives users granular control over what they disclose and to whom, implementing the principle of data minimisation that aligns with GDPR requirements (Tobin and Reed, 2017; Kondova and Erbguth, 2020).

IV. Smart Contract-Based Access Control:

Smart contracts on programmable blockchains such as Ethereum can encode sophisticated access control policies that execute automatically, transparently, and without requiring trusted intermediaries. Role-based access control, time-locked permissions, multi-signature requirements, and token-gated access can all be implemented as self-enforcing smart contract logic (Xu, Weber and Staples, 2019). The transparency of smart contract code on public blockchains enables independent security auditing by any party, a significant advantage over proprietary centralised access control systems whose logic is opaque to external review.

C. E-Commerce Security Threats and Their Systemic Impact

E-commerce platforms operate in an adversarial environment characterised by a diverse and evolving threat landscape. Understanding the specific threat vectors that blockchain-based authentication addresses is essential for evaluating the technology's practical value.

I. Phishing and Social Engineering:

Phishing attacks have evolved from broadly distributed mass emails to highly targeted spear-phishing campaigns that leverage personal data harvested from social media and prior breaches to craft convincing impersonation attempts. Advanced variants include vishing (voice phishing using deepfake audio to impersonate known contacts or institutions) and smishing (SMS-based phishing). These attacks succeed because they exploit the weakest link in credential-based authentication: the human user who can be deceived into surrendering their credentials. (Banday and Qadri 2007) documented the early escalation of phishing as an e-commerce threat, and the sophistication of attacks has increased substantially since. Blockchain-based authentication mitigates phishing by removing the credential, meaning there is no password to steal. Even if a user is deceived into visiting a fraudulent site, the attacker cannot use that interaction to authenticate as the user on a legitimate platform, because authentication requires possession of the private key, which never leaves the user's device.

II. *Credential Stuffing:*

Credential stuffing exploits the widespread practice of password reuse. Automated bots test massive lists of username-password pairs, compiled from prior data breaches against target platforms, capitalising on the statistical likelihood that a proportion of users employ the same credentials across multiple services. Industry data indicates that some credential stuffing campaigns achieve success rates of 0.5–2%, which translates to tens of thousands of account compromises when applied to breach datasets containing hundreds of millions of records (Vissers et al., n.d.). Blockchain authentication eliminates this attack vector entirely: because authentication is performed through cryptographic signing rather than password submission, there are no reusable credentials to stuff.

III. *Man-in-the-Middle Attacks:*

Man-in-the-middle (MitM) attacks involve an adversary intercepting and potentially modifying communications between a user and a legitimate service. In e-commerce contexts, successful MitM attacks can enable session hijacking, transaction manipulation, and credential theft. Public Wi-Fi networks, which are commonly used by mobile shoppers, are particularly fertile environments for MitM attacks given their lack of encryption. Traditional TLS-based security mitigates but does not eliminate MitM risk, particularly when Certificate Authorities are compromised or when users are conditioned to accept invalid certificates (American Express, 2024). Blockchain PKI systems eliminate the Certificate Authority as a single point of trust, distributing certificate verification across the blockchain network.

IV. *Data Breaches and Credential Theft:*

Large-scale data breaches affecting e-commerce platforms and their authentication providers have become endemic. IBM's 2023 Cost of a Data Breach Report placed the median breach cost at $4.45 million, a figure that escalates significantly for platforms holding large volumes of payment data. The reputational damage compounds the financial impact: 81% of consumers report ceasing online engagement with breached brands (Comparitech, 2024; Ping Identity, 2019). Centralised credential databases are the primary target of most data breaches. Blockchain-based systems that store no centralised credential database eliminate this target entirely because an attacker who breaches the application server has no credential store to exfiltrate.

V. *DDoS Attacks and Availability Threats:*

Distributed Denial of Service attacks overwhelm e-commerce platforms with synthetic traffic, rendering them unavailable to legitimate users. E-commerce businesses lose an estimated £4,700 per minute of downtime, translating to £282,000 per hour (Security Brief, 2024). The availability of DDoS-for-hire services has dramatically lowered the barrier to mounting such attacks, making them an accessible tool for competitive sabotage and extortion (Jonker et al., 2017). Blockchain-based decentralised DNS and token-based request prioritisation offer structural mitigations by eliminating centralised availability bottlenecks.

D. *Existing Research on Blockchain Authentication in E-Commerce*

The application of blockchain technology to e-commerce authentication has attracted growing academic attention. (Treiblmaier and Sillaber, 2021) provide a comprehensive framework for blockchain's impact on e-commerce, identifying authentication and identity management as priority research domains and characterising scalability and regulatory compliance as the principal adoption barriers. (Dahal 2023) conducted an empirical evaluation of blockchain's effectiveness against fraudulent e-commerce transactions, finding statistically significant improvements in fraud prevention rates. (Albshaier, Almarri and Hashim, 2024) reviewed blockchain's role in e-commerce security, identifying open challenges including interoperability with legacy systems and the need for standardised DID frameworks. (Guntara, Nurfirmansyah and Ferdiansyah, 2023) demonstrated practical blockchain implementation in e-commerce transaction security, confirming measurable improvements in transaction integrity.

Several studies have specifically examined Ethereum-based authentication systems. (Umoren et al. 2022) evaluated blockchain-based authentication with improved performance for fog computing environments, achieving authentication time reductions compared to conventional 2FA. (Xu, Weber and Staples, 2019) analysed architectural patterns for blockchain applications, providing a taxonomy applicable to authentication system design. The present study builds upon this body of work by providing a complete end-to-end implementation using contemporary web development tooling (React.js, Node.js, MetaMask) and conducting a structured multi-dimensional comparative evaluation.

III. PROPOSED BLOCKCHAIN-BASED AUTHENTICATION SYSTEM

A. System Architecture Overview

The proposed system is designed around four integrated components that collectively deliver a decentralised, cryptographically secure authentication flow compatible with standard e-commerce web architectures. The design prioritises security without sacrificing usability, recognising that authentication systems that impose excessive friction on users are frequently bypassed or abandoned in favour of weaker alternatives.

The four principal components are: (1) a React.js frontend providing the user-facing interface, including login components, protected routing, and real-time MetaMask interaction prompts; (2) a Node.js and Express.js backend responsible for nonce generation, cryptographic signature verification, JWT issuance, and session management; (3) a blockchain interaction layer implemented via Web3.js and MetaMask, enabling communication between the web application and the user's Ethereum wallet; and (4) JSON Web Tokens (JWT) as the session management mechanism following successful blockchain-based verification.

This architecture deliberately preserves the familiar web application structure that e-commerce developers and operations teams are accustomed to, while inserting blockchain-based cryptographic verification as the authentication primitive. This approach minimises the integration burden for existing platforms and reduces the learning curve for development teams unfamiliar with blockchain tooling.

B. Design Principles and Rationale

The system architecture is governed by four foundational design principles, each addressing a specific requirement identified in the literature review.

I. Security by architecture:

The system eliminates the credential database entirely. There is no server-side password store to breach, hash-crack, or exfiltrate. Authentication is performed through ECDSA signatures generated on the user's device using their MetaMask-managed private key. Nonce values (unique random strings generated for each authentication session) are incorporated into the signed message to prevent replay attacks, ensuring that an intercepted signature cannot be reused. JWT tokens issued post-authentication carry a defined expiry and are transmitted exclusively over HTTPS via the Secure cookie attribute.

II. *User experience centred on existing tools:*

Rather than requiring users to adopt unfamiliar blockchain interfaces, the system integrates with MetaMask, a browser extension with over 30 million active users as of 2023 (MetaMask, 2023). For users already in possession of an Ethereum wallet (a rapidly growing demographic) the authentication experience involves a familiar wallet interaction: review and sign a message. Onboarding flows for users without MetaMask provide clear installation guidance.

III. Scalability through hybrid state management:

Blockchain interactions are confined to the authentication event itself. Post-authentication session management is handled via JWT, a stateless, computationally lightweight mechanism that does not require blockchain queries for every protected resource request. This design isolates the performance impact of blockchain consensus from the routine operation of the e-commerce platform.

IV. Interoperability with existing infrastructure:

The system is implemented using standard web technologies (React.js, Node.js, Express.js, REST

APIs) that are ubiquitous in e-commerce development. Integration with existing platforms is achievable through React component substitution or API endpoint integration, without requiring platform re-architecture.

C. User Registration and Identity Management

A distinctive feature of the proposed system is its implicit registration model, which operationalises SSI principles. Users do not register by submitting personal data to a server-side database. Instead, registration is accomplished through the user's existing Ethereum wallet: the system detects MetaMask installation upon first access, prompts the user to connect their wallet, and creates a minimal user record associated with their Ethereum address. This address serves as the user's persistent, globally unique identifier across all sessions.

This approach has significant privacy implications. The platform holds no password, no email address (unless voluntarily provided for transactional notifications), and no other personally identifying information beyond the Ethereum address, which is pseudonymous. Verifiable Credentials issued by trusted issuers (such as age verification services or loyalty programme operators) can be presented by users to prove specific attributes without revealing the underlying data, fully implementing the SSI paradigm (Tobin and Reed, 2017).

D. Authentication Protocol

The complete authentication protocol operates as follows. Upon user initiation of login, the React frontend requests the user's Ethereum address from MetaMask. The address is transmitted to the backend, which generates a unique nonce (a randomly generated alphanumeric string) and associates it with the address in a short-lived server-side store. The backend returns a structured message incorporating the nonce. The frontend passes this message to MetaMask, which prompts the user to review and sign it using their private key. The resulting ECDSA signature is transmitted to the backend. The backend uses Web3.js's ecrecover function to derive the Ethereum address from the signature and the original message. If the derived address matches the address presented at the start of the authentication flow, identity is confirmed. A signed JWT is generated and returned to the frontend, stored with the Secure and HttpOnly attributes to prevent JavaScript access and ensure HTTPS-only transmission. Subsequent requests to protected routes and API endpoints include this JWT, which is verified by backend middleware before resources are served.

This protocol achieves the three core properties of a robust authentication mechanism: authentication (verification of identity through cryptographic proof), integrity (the signed message cannot be altered without invalidating the signature), and non-repudiation (the user cannot deny having signed the authentication message without claiming compromise of their private key).

E. Access Control and Session Management

Protected routes in the React application perform client-side JWT presence and expiry checks to redirect unauthenticated users. All protected API endpoints on the backend implement JWT verification middleware that validates the token's signature, expiry, and claims before processing requests. JWT expiry is set to a configurable session duration, after which re-authentication is required. The system supports token refresh flows that extend sessions without requiring repeated wallet signing, provided the existing JWT is still within a defined refresh window. This approach aligns with established best practices for web application security (Siriwardena, 2020) while incorporating the blockchain layer only where its security advantages are decisive.

IV. PROTOTYPE IMPLEMENTATION

A. Development Environment and Technology Stack

The prototype was developed in a full-stack JavaScript environment, enabling consistent language use across frontend, backend, and blockchain interaction layers. This choice reduces cognitive switching costs for developers and simplifies dependency management. Table 1 summarises the technology stack.

Component	Technology / Library
Frontend UI	React.js, React Router v6, Fetch API
Backend Server	Node.js v18, Express.js v4
Authentication Tokens	jsonwebtoken (JWT), bcryptjs
Cross-Origin Management	CORS middleware (Express)
Blockchain Interaction	Web3.js v1.10, MetaMask browser extension

Blockchain Network	Ethereum (Sepolia testnet for developmen
Development Environment	Visual Studio Code, Git, npm
Testing	Postman (API), Chrome DevTools (fronte

Table 1. Prototype Development Environment and Technology Stack

B. *Frontend Implementation*

The React.js frontend was structured around three primary components: an authentication context provider managing global authentication state; a login page implementing the MetaMask interaction flow; and a higher-order protected route component that redirects unauthenticated users. Upon mounting, the application checks for MetaMask availability using window.ethereum and prompts installation if absent. The login function is implemented as an asynchronous operation that first requests the user's Ethereum accounts array from MetaMask via ethereum.request({ method: 'eth_requestAccounts' }), extracts the first account, submits it to the backend to retrieve a session-specific nonce, constructs the message to be signed, invokes ethereum.request with the eth_sign method to obtain the ECDSA signature, and submits both the address and signature to the backend verification endpoint. On successful verification, the returned JWT is stored as a Secure cookie, and the application router redirects to the protected dashboard. Error handling covers MetaMask non-installation, user rejection of the signing request, and backend verification failure, providing contextually appropriate user feedback in each case.

C. *Backend Implementation*

The Node.js/Express.js backend exposes four API endpoints: GET /nonce/:address for nonce generation and retrieval; POST /authenticate for signature verification and JWT issuance; GET /protected-resource for demonstrating JWT-protected resource access; and POST /logout for session termination. Nonce generation produces a cryptographically random 32-byte hex string per session, stored in a server-side Map with a 10-minute expiry to prevent long-lived replay attack windows. Signature verification employs Web3.js's web3.eth.accounts.recover(message, signature) function, which implements the Ethereum personal sign message recovery algorithm. The recovered address is compared case-insensitively against the submitted address. On successful verification, the nonce is invalidated preventing reuse, and a JWT is signed using a server-side secret key with a configurable expiry. The JWT payload includes the Ethereum address as the subject claim, an issued-at timestamp, and an expiry timestamp.

D. *Implementation Challenges and Adaptations*

The original implementation plan called for smart contract-based credential management using Solidity contracts deployed via Truffle to a local Ganache development blockchain. During implementation, Truffle was announced as deprecated, with ConsenSys directing developers to alternative tooling. The transition to Hardhat and Foundry as successor frameworks required navigating incomplete migration documentation and breaking API changes, experiences consistent with the broader challenge of rapid tooling evolution in the blockchain ecosystem documented by (Marr, 2023) and (Tripathi, Ahad and Casalino, 2023).

Following an architectural reassessment, the smart contract layer was replaced by MetaMask wallet-based authentication, which proved architecturally superior for the e-commerce use case: it does not require on-chain transactions (eliminating gas costs and transaction confirmation latency), integrates directly with users' existing Ethereum wallets, and reduces the attack surface by removing smart contract code as a potential vulnerability vector. The revised architecture is consistent with the wallet-based authentication pattern described by (Dahal, 2023) and (Umoren et al., 2022).

A secondary challenge involved supporting alternative wallet clients beyond MetaMask, which was identified as important for accessibility to users unfamiliar with MetaMask. Implementation of WalletConnect integration which enables connection with over 300 wallet applications was planned but could not be completed within the project timeframe. This remains an identified improvement for future iterations.

V. COMPARATIVE ANALYSIS: RESULTS AND DISCUSSION

A. *Evaluation Framework*

The comparative evaluation was conducted across eleven dimensions derived from the literature, spanning security architecture, data management, usability, economic considerations, and technological compatibility. For each dimension, the behaviour of the proposed blockchain-based system was contrasted with that of conventional authentication methods specifically, username-password authentication with optional 2FA, drawing on both the prototype implementation experience and the academic literature. Table 2 presents the structured comparison.

Dimension	Traditional Authentication	Blockchain-Based Authentication
Centralisation	Single authoritative server holds credentials; single point of failure	Trust distributed across blockchain nodes; no central credential store
Data Integrity	Server-side databases susceptible to tampering, injection, and unauthorised modification	Immutable ledger prevents retroactive alteration; cryptographic linking ensures chain integrity
Identity Management	Centralised, provider-controlled; users have no sovereignty over their data	User-controlled SSI via DIDs; selective disclosure without revealing underlying data
Scalability	Mature, high-throughput at scale; latency typically sub-100ms per authentication	Consensus mechanisms limit throughput; mainnet Ethereum ~15–30 TPS; latency depends on network congestion
Cross-Domain Auth	Requires separate credentials and verification per platform; fragmented user experience	Unified Ethereum address as portable identity; reduces re-verification friction across platforms
Flexibility	Customisation limited to server-side logic; policy changes require server redeployment	Smart contract logic can encode complex, automated policies; updates governed by contract versioning
Trust Model	Requires trust in centralised authority; CA compromise undermines entire PKI	Distributed trust; no single party can unilaterally corrupt the authentication record
Auditability	Log integrity depends on server security; logs can be deleted or modified	On-chain authentication events are immutable and publicly auditable
MFA Support	Centralised MFA; credential compromise may bypass secondary factor	Decentralised MFA; each factor independently cryptographically secured
Emerging Tech Fit	Limited native compatibility with IoT and smart contract ecosystems	Native compatibility; Ethereum addresses serve as universal device and contract identifiers
Long-Term Economics	Lower initial deployment cost; higher ongoing infrastructure, compliance, and breach recovery costs	Higher initial implementation cost; lower ongoing infrastructure; breach costs minimised by eliminating credential stores

Table 2. Comparative Analysis: Traditional vs. Blockchain-Based Authentication Across Eleven Dimensions

B. *Security Architecture: Elimination of the Credential Database*

The most consequential security advantage of the proposed system is structural: it eliminates the centralised credential database that is the primary target of the vast majority of e-commerce data breaches. In conventional systems, even well-implemented password storage, using bcrypt or Argon2 hashing with appropriate cost factors creates a recoverable asset: a large enough breach provides attackers with a dataset that can be subjected to offline dictionary and rainbow-table attacks indefinitely. The blockchain-based system stores no password. The Ethereum address is public by design; possessing it, grants no authentication capability without the private key that generated it. An attacker who breaches the application server obtains only JWT secrets (which can be rotated immediately) and Ethereum addresses (which are already public). This represents a qualitative improvement in breach consequence, consistent with the findings of (Dahal, 2023) and (Albshaier, Almarri and Hashim, 2024).

C. *Privacy and Regulatory Alignment*

The SSI model implemented through the proposed system is well-aligned with GDPR's core principles, particularly data minimisation and purpose limitation. The platform collects no personal data beyond the pseudonymous Ethereum address, and verification of user attributes (age, region, membership status) can be performed through Verifiable Credentials that attest to the attribute without transmitting the underlying data. This contrasts sharply with conventional authentication systems that typically collect and retain substantial personal data, like email addresses, phone numbers, security question answers, that is irrelevant to authentication but creates GDPR compliance obligations and breach exposure.

A tension does exist between blockchain immutability and GDPR's right to erasure (Article 17). Authentication events recorded on a public blockchain cannot be deleted. This tension is mitigated in the proposed architecture by minimising what is recorded on-chain: the prototype does not record authentication events on the Ethereum mainnet, it uses Ethereum's cryptographic primitives for signing and verification without writing authentication records to the public ledger. This design choice preserves compliance while leveraging the cryptographic security of Ethereum's infrastructure.

D. Scalability Analysis

Scalability is the most significant limitation of the proposed system in its current form. Ethereum mainnet processes approximately 15–30 transactions per second under normal network conditions, orders of magnitude below the authentication throughput requirements of large-scale e-commerce platforms during peak periods such as Black Friday or seasonal sales events. However, the prototype's architecture mitigates this constraint through its hybrid design: the blockchain is invoked only for the initial authentication event, while subsequent session management relies on JWT verification, which is computationally trivial and adds negligible latency to resource requests.

Looking ahead, Layer 2 scaling solutions, including Optimistic Rollups and ZK-Rollups deployed on networks such as Arbitrum, Optimism, and zkSync, offer throughput improvements of 100–1000x compared to Ethereum mainnet while preserving security guarantees through periodic settlement to mainnet (TokenMinds, 2024). Adoption of these solutions for the authentication layer would substantially reduce the scalability gap. Additionally, the system could be deployed on Ethereum's Sepolia or Polygon network for cost efficiency, or on permissioned enterprise blockchains such as Hyperledger Fabric for organisations requiring higher throughput and lower latency.

E. User Experience Considerations

User experience is a critical determinant of authentication system adoption. The MetaMask integration introduces a prerequisite, wallet installation and account creation, that represents a non-trivial onboarding burden for users unfamiliar with blockchain technology. However, this burden is a one-time cost; subsequent authentication interactions are comparable in friction to standard login flows. The signing prompt presented by MetaMask is clear and readable, displaying the message to be signed and requiring explicit user confirmation.

The shift of responsibility to the user specifically, the imperative to safeguard the private key, represents a double-edged aspect of SSI. Users who lose access to their private key lose access to their identity on the system, with no password reset mechanism available. This is mitigated in practice through social recovery mechanisms (Ethereum's ERC-4337 account abstraction standard enables guardian-based recovery) and hardware wallet backup procedures, but requires explicit user education. This finding aligns with (Dahal's, 2023) observation that user empowerment and user responsibility are inversely related in SSI systems.

F. Economic Analysis

Initial deployment costs for blockchain-based authentication are higher than for conventional systems, principally due to the need for developer expertise spanning both web application and blockchain domains, a relatively scarce skill combination that commands premium compensation. Ongoing operational costs, however, are structured differently: the proposed system has no centralised authentication server infrastructure to maintain (beyond the existing application backend), no licensing costs for authentication-as-a-service providers, and dramatically reduced breach-related costs. IBM's 2023 breach cost analysis suggests that eliminating the credential database could reduce the average e-commerce breach cost by a substantial proportion, since credential exfiltration and its downstream consequences account for a major share of breach-related losses. Over a 5-to-7-year horizon, the economics of blockchain authentication are likely to favour adoption, particularly as developer tooling matures and reduces implementation complexity.

VI. LIMITATIONS AND FUTURE RESEARCH DIRECTIONS

A. Limitations of the Present Study

This research acknowledges several limitations that qualify the generalisability of its findings. First, the prototype was evaluated in a controlled development environment using the Ethereum Sepolia testnet, which does not replicate the performance characteristics of mainnet deployment or the throughput demands of production e-commerce platforms. Formal performance benchmarking under simulated peak load conditions was outside the scope of this study and represents a priority for future work.

Second, the evaluation was conducted by the system's author without independent peer assessment of the prototype implementation or external user testing. A formal usability study with representative end users, including both technically sophisticated users and those with no prior blockchain experience, would provide more robust evidence on user experience outcomes. Third, the system was evaluated against a stylised representation of 'traditional authentication' rather than specific commercial implementations, which vary considerably in their security configurations. Finally, the scope was limited to Ethereum as the blockchain platform; comparative evaluation across multiple platforms (Hyperledger Fabric, Polygon, Cardano) would provide richer guidance for practitioners selecting platforms for deployment.

B. Future Research Directions

Several avenues for future research emerge from this study. Performance benchmarking under realistic e-commerce loads, including authentication throughput, latency distribution, and behaviour under Layer 2 scaling, would provide empirically grounded guidance for deployment decisions. Formal usability evaluation through controlled user studies would quantify onboarding friction and identify specific UX improvements. Integration with WalletConnect to support multiple wallet clients beyond MetaMask would improve accessibility. Investigation of ERC-4337 account abstraction for social recovery mechanisms would address the private key management challenge. Research into privacy-preserving Verifiable Credential frameworks, specifically ZKP-based selective disclosure would strengthen the regulatory compliance proposition of SSI-based e-commerce identity. Finally, longitudinal deployment studies in production environments would provide real-world validation of the security and economic claims advanced in this paper.

VII. CONCLUSION

This paper has presented a comprehensive investigation of blockchain-based authentication as a structural response to the endemic security vulnerabilities of conventional e-commerce authentication architectures. Through a review of the relevant literature, the design and implementation of a proof-of-concept prototype on the Ethereum blockchain, and a structured comparative evaluation across eleven analytical dimensions, the study has demonstrated that blockchain-based authentication offers meaningful and qualitatively distinct security improvements over traditional centralised methods.

The central security advantage is architectural: the elimination of the centralised credential database removes the primary target of the vast majority of e-commerce data breaches. Authentication through ECDSA cryptographic signing provides non-repudiable, replay-resistant identity verification without transmitting or storing any secret. Zero-Knowledge Proof compatibility and Decentralised Identifier support enable privacy-preserving verification aligned with data minimisation principles. The Self-Sovereign Identity model returns data ownership to users and reduces the platform's GDPR exposure.

These advantages come with substantive constraints. Blockchain consensus mechanisms limit authentication throughput below the requirements of large-scale platforms. MetaMask dependency introduces onboarding friction. Private key management places new responsibilities on users accustomed to password reset flows. The rapidly evolving blockchain tooling ecosystem creates implementation complexity and requires ongoing maintenance vigilance.

The practical recommendation emerging from this study is a phased, hybrid adoption strategy: deploy blockchain-based authentication for high-value transactions, account recovery events, and cross-platform identity federation, while retaining conventional authentication for routine low-stakes interactions. As Layer 2 scaling solutions mature, developer tooling stabilises, and user familiarity with blockchain wallets increases, the case for broader deployment strengthens. The trajectory of blockchain technology and the escalating costs of conventional authentication failures point toward a future in which decentralised cryptographic authentication becomes the norm rather than the exception for digital commerce security.

This research contributes to the empirical foundation of that transition, providing both a worked implementation reference and a structured evaluation framework for practitioners and researchers advancing the state of e-commerce security.

REFERENCES

[1] Albshaier, L., Almarri, S. and Hashim, M.M. (2024) 'A Review of Blockchain's Role in E-Commerce Transactions: Open Challenges, and Future Research Directions', Computers, 13(1). Available at: https://doi.org/10.3390/computers13010027.

[2] American Express (2024) Security Solutions and Best Practices to Protect Against E-Commerce Threats. Available at: https://www.americanexpress.com/en-us/business/trends-and-insights/articles/security-solutions-and-best-practices-to-protect-against-e-commerce-threats/ (Accessed: 11 July 2024).

[3] Banday, M.T. and Qadri, J.A. (2007) 'Phishing-A Growing Threat to E-Commerce', The Business Review, 12(2), pp. 76–83.

[4] Buterin, V. (2014) 'A next-generation smart contract and decentralized application platform'. Ethereum Foundation. Available at: https://ethereum.org/en/whitepaper/ (Accessed: 15 July 2024).

[5] Comparitech (2024) 30+ Data Breach Statistics and Facts: Frequency, Impact & More. Available at: https://www.comparitech.com/blog/vpn-privacy/data-breach-statistics-facts/ (Accessed: 12 July 2024).

[6] Dahal, S.B. (2023) 'Enhancing E-commerce Security: The Effectiveness of Blockchain Technology in Protecting Against Fraudulent Transactions', International Journal of Intelligent Computing, 1(1). Available at: https://publications.dlpress.org/index.php/ijic/article/view/1/1 (Accessed: 19 July 2024).

[7] Jonker, M. et al. (2017) 'Millions of Targets Under Attack: a Macroscopic Characterization of the DoS Ecosystem', in Proceedings of the 2017 Internet Measurement Conference. New York: ACM, pp. 100–113.

[8] Kondova, G. and Erbguth, J. (2020) 'Self-Sovereign Identity on Public Blockchains and the GDPR', in Proceedings of the 35th ACM/SIGAPP Symposium on Applied Computing. New York: ACM. Available at: https://doi.org/10.1145/3341105.3374066.

[9] Marr, B. (2023) 'The 5 Biggest Problems With Blockchain Technology Everyone Must Know About', Forbes, 14 April. Available at: https://www.forbes.com/sites/bernardmarr/2023/04/14/the-5-biggest-problems-with-blockchain-technology-everyone-must-know-about/ (Accessed: 23 July 2024).

[10] MetaMask (2023) MetaMask Monthly Active Users. ConsenSys. Available at: https://metamask.io (Accessed: 18 July 2024).

[11] Nakamoto, S. (2008) 'Bitcoin: A Peer-to-Peer Electronic Cash System'. Available at: https://bitcoin.org/bitcoin.pdf (Accessed: 15 July 2024).

[12] Ping Identity (2019) 2019 Consumer Survey: Data Misuse & Trust. Available at: https://www.pingidentity.com/en/resources/content-library/misc/3464-2019-consumer-survey-trust-accountability.html (Accessed: 13 July 2024).

[13] Security Brief (2024) Global surge in DDoS attacks causes dire financial consequences. Available at: https://securitybrief.in/story/global-surge-in-ddos-attacks-causes-dire-financial-consequences (Accessed: 13 July 2024).

[14] Siriwardena, P. (2020) Advanced API Security: OAuth 2.0 and Beyond. 2nd edn. Berkeley: Apress. Available at: https://doi.org/10.1007/978-1-4842-2050-4.

[15] Statista (2024) E-commerce worldwide – statistics & facts. Hamburg: Statista Research Department.

[16] Tobin, A. and Reed, D. (2017) 'The Inevitable Rise of Self-Sovereign Identity', Sovrin Foundation White Paper. Available at: https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf (Accessed: 17 July 2024).

[17] TokenMinds (2024) Unlocking Speed with Layer 2 Solutions: TokenMinds' Comprehensive Guide. Available at: https://tokenminds.co/blog/blockchain-development/layer-2-solutions (Accessed: 16 July 2024).

[18] Treiblmaier, H. and Sillaber, C. (2021) 'The impact of blockchain on e-commerce: A framework for salient research topics', Electronic Commerce Research and Applications, 48, Article 101054. Available at: https://doi.org/10.1016/j.elerap.2021.101054.

[19] Tripathi, G., Ahad, M.A. and Casalino, G. (2023) 'A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges', Decision Analytics Journal. Available at: https://doi.org/10.1016/j.dajour.2023.100344.

[20] Umoren, O. et al. (2022) 'Blockchain-Based Secure Authentication with Improved Performance for Fog Computing', Sensors, 22(22). Available at: https://doi.org/10.3390/s22228969.

[21] Voshmgir, S. and Zargham, M. (2020) 'Foundations of Cryptoeconomic Systems', Research Institute for Cryptoeconomics Working Paper Series, No. 1.

[22] W3C (2022) Decentralized Identifiers (DIDs) v1.0: Core Architecture, Data Model, and Representations. W3C Recommendation. Available at: https://www.w3.org/TR/did-core/ (Accessed: 17 July 2024).

[23] Wilson, D. and Ateniese, G. (2015) 'From Pretty Good to Great: Enhancing PGP Using Bitcoin and the Blockchain', in Qiu, M. et al. (eds) Network and System Security. Lecture Notes in Computer Science, vol 9408. Cham: Springer.

[24] Xu, X., Weber, I. and Staples, M. (2019) Architecture for Blockchain Applications. Cham: Springer.

[25] Zheng, Z. et al. (2018) 'Blockchain challenges and opportunities: A survey', International Journal of Web and Grid Services, 14(4), pp. 352–375. Available at: https://doi.org/10.1504/IJWGS.2018.095647