IJEMD-CSAI, 3 (1) (2024), 1 – 9 https://doi.org/10.54938/ijemdcsai.2024.03.1.350

International Journal of Emerging Multidisciplinaries:
Computer Science and Artificial Intelligence

Research Paper
Journal Homepage: www.ojs.ijemd.com
ISSN (print): 2791-0164 ISSN (online): 2957-5036

Verified Views: How Blockchain-enabled Digital Identity Verification Can Combat Fake Accounts and Disinformation on Social Media

Emmanuel John Anagu [1*], Sharifatu Gago Ja'afaru [2] , Kelvin Inobemhe [2]

1. Computer Science Department, Federal University Wukari, Taraba state Nigeria.

2. Mass Communication, Glorious Vision University, Ogwa-Edo State Nigeria.

Abstract

The study was conducted to unravel the ways through which digital identity verification offered in form of blockchain technology can help combat fake accounts and disinformation across social media platforms. The researchers relied on the survey research and elicited quantitative data from respondents. The purposive sampling technique was utilized to select respondents and online link to questionnaires shared with them to complete the survey. Findings of the study showed that users have realized the importance of blockchain technology and have accepted its capacity to ensure security across online spaces. Furthermore, the researchers found that watermarking, content hashing, smart contracts, distributed ledger technology, blockchain-based content management systems, public key cryptography consensus mechanism and data encryption are some of the essential strategies and protocols utilized by media organizations to bolster information reliability. Blockchain technology was also found to be essential in curtailing the spread of disinformation and also enhancing confidence in digital content. The researcher concluded that blockchain technology holds the capacity to improve the integrity of digital identities in contemporary digitized world. Among others, the researchers recommended that media organizations and other stakeholders embark on sensitization to enlighten the public about the strength of blockchain technology.

Keywords: Blockchain; Computers; Disinformation; Fake Accounts; Social Media.

Introduction

Social media has transformed global communication, enabling instant information exchange. It allows users to engage in sharing ideas and discovering new information. However, these platforms can be exploited by malicious users who spread disinformation and manipulate public perception. Recent

Email addresses: anague@fuwukari.edu.ng (Emmanuel John Anagu), sharifatujaafaru@gmail.com (Sharifatu Gago Ja'afaru), inobemhekelvin@gmail.com (Kelvin Inobemhe).

research indicates a shift in news consumption, with many users preferring digital-based news over traditional newspapers. However, the authenticity of news on social media (digital news) is a challenging and difficult process, unlike content from radio and television, which are subjected to critical review and supervision before broadcasting[1]. Identity theft and disinformation threaten social cohesion and can influence public opinion. Despite various security measures in place: phone number verification, two-factor authentication, cloudfare and CAPTCHA tests, these approaches fell short in curtailing these challenges. Hence, blockchain technology offers a promising solution for verifying identities and enhancing social media security through its decentralized ledger.

Blockchain, or distributed ledger technology, is seen as a revolutionary advancement in data security and transparency. Initially created for Bitcoin, blockchain has evolved into a versatile tool for secure transactions and identity verification. Integrating blockchain into identity systems signifies a shift towards decentralized, user-centric models. This evolution is vital for overcoming the limitations of current identity management systems and ensuring secure digital interactions [2].

Conversely, applying blockchain for digital identity verification specifically addresses issues like fake accounts and disinformation on social media. By providing a decentralized, tamper-proof identity validation mechanism, blockchain enhances online interaction reliability. These systems leverage digital signatures and cryptographic keys to confirm user authenticity, ensuring genuine participation online [3]. Additionally, they can identify malicious actors and reduce organized disinformation efforts tied to fraudulent accounts.

Given the weaknesses of traditional identity verification, like centralized databases prone to breaches, there's a pressing need for secure solutions. Blockchain's decentralized, immutable record-keeping is ideal for improving the integrity and traceability of digital identities. It can help combat fake identities and Sybil attacks on social media. By confirming user identities, platforms can build trust and minimize disinformation. However, there's a lack of literature connecting blockchain's potential with established theories, which could enhance understanding of its impact on user behavior and trust in digital realms [4].

Brief Overview of Blockchain Technology

Blockchain technology can be traced back to the late 1970s, when computer scientist Ralph Merkle secured a patent for a data structure known as "Merkle trees" or "hash trees." These Merkle trees were created as a cryptographic method to guarantee the integrity and efficiency of data storage in digital contexts, making them essential for establishing secure links between data blocks [5].

However, it was not until the launch of Bitcoin in 2008 that blockchain gained widespread recognition as a groundbreaking technology. Bitcoin, designed by Satoshi Nakamoto, utilized blockchain as its core framework to enable a decentralized, peer-to-peer digital currency system [6]. The success of Bitcoin catalyzed the broader implementation of blockchain technology across multiple industries, including finance, healthcare, supply chain management, and digital identity verification. The evolution of blockchain is often categorized into three distinct generations, each characterized by its technological advancements and applications [7]

First Generation - Cryptocurrency Systems (2008–2013): The primary achievement of the first generation was the establishment of a d centralized financial ecosystem through Bitcoin. Nakamoto's original design employed 1 MB blocks to record and verify transactions. This foundational concept of linking blocks using cryptographic hashes and validating them through a consensus mechanism became the bedrock for

future blockchain developments. The primary focus of this generation was the creation and management of digital currencies

.

Second Generation - Smart Contracts (2013–2020): Ethereum, introduced by Buterin, Coleman & Wampler in 2015, expanded blockchain's capabilities beyond simple transactions by incorporating programmable contracts known as "smart contracts." These smart contracts facilitate the automatic enforcement of predefined rules and agreements, transforming blockchain into a versatile tool for various applications, including asset transfers, decentralized finance (DeFi), and supply chain tracking [8]. This generation marked the shift of blockchain from a basic transactional platform to one capable of supporting complex, self-executing agreements.

Third Generation - Scalability and Interoperability (2020–Present): The third generation of blockchain technology addresses the limitations of earlier versions, including challenges related to scalability, speed, and cross-chain interoperability. Innovations such as sharding, side chains, and proof-of-stake consensus algorithms have been introduced to enhance the performance and capacity of blockchain systems. These advancements are paving the way for broader acceptance in fields such as digital identity management, intellectual property protection, and public governance [9].

The key attributes of blockchain technology – decentralization, immutability, and consensus distinguish it from traditional systems. Decentralization refers to the elimination of a central authority, enabling participants in a blockchain network to verify and record transactions through a distributed consensus process [10]. Immutability ensures that once a transaction is recorded in the blockchain, it cannot be altered, providing a tamper-proof ledger of all transactions. Consensus mechanisms, such as Proof of Work (PoW) and Proof of Stake (PoS), determine how transactions are verified and added to the ledger, ensuring the network's security and dependability [11].

Statement of the Problem

Social media has evolved into a vital platform for public discourse and political debate generally, resulting in proliferation of fake accounts and the swift spread of disinformation, thereby presenting a serious challenge to the integrity of digital communication. Existing identity verification systems, which primarily rely on centralized databases, not only pose a risk of data breaches but also lack the ability for real-time validation, impeding efforts to address the systematic dissemination of disinformation [12]. On social media platforms, verifying the authenticity and reliability of information is an essential security imperative. This disorder arises from the lack of a standardized verification system. In some instances, fake news can appear more appealing than authentic news. The surge in fake news has particularly arisen from an unregulated flow of information and has become an urgent concern. Social media platforms like Facebook and X have crafted their own strategies to combat fake news through the adoption of machine learning technologies. Nevertheless, the obligation to identify fake news should not be placed entirely on a single organization or platform. It ought to be decentralized, with the creation of a third-party decentralized system that provides blockchain as a service (BaaS) to effectively address the fake news dilemma [13].

Despite advancements in digital identity frameworks, traditional methods still rely on the repetitive sharing of sensitive personal information, which heightens the risk of identity theft and exploitation. Thus, the demand for a secure, transparent, and efficient solution is becoming increasingly clear. Blockchain presents a compelling alternative by guaranteeing the authenticity and traceability of digital identities without the need for a centralized authority. By leveraging its decentralized architecture, blockchain can validate

identities through cryptographic methods such as digital signatures and public keys, thereby enhancing the trustworthiness of online interactions and reducing the likelihood of identity fraud.

However, there exists a notable deficiency in the literature linking the potential of blockchain to established theories and frameworks beyond its technical dimensions. A significant amount of research has concentrated on the technological characteristics and performance assessments of blockchain, leaving an ambiguous space regarding its practical applications in digital identity management from a theoretical perspective [4,14]. [15] contends that conversations about blockchain must evolve to encompass its integration with behavioral theories and its influence on shaping digital ecosystems. This study aims to fill this void by investigating how blockchain-enabled identity solutions can tackle the issues of fake accounts and disinformation on social media, thereby providing a comprehensive understanding of blockchain's capacity to promote secure and trustworthy online interactions.

Aim and Objectives

The aim of this study is to explore the potential of blockchain technology in addressing the issues of fake accounts and disinformation on social media platforms. The study will achieve this aim through the following specific objectives:

i. Examine how blockchain's decentralized and immutable nature can improve the security and integrity of digital identities compared to traditional centralized systems.

ii. Evaluate the level of public awareness, acceptance, and trust in blockchain-based identity solutions among users.

iii. Identify essential strategies and protocols employed by media organizations utilizing blockchain technology to bolster information reliability.

iv. Assess the efficacy of these blockchain protocols in reducing the spread of disinformation and enhancing user confidence in digital content.

Hypothesis

H1: The adoption of blockchain-enabled digital identity verification significantly reduces the prevalence of fake accounts and disinformation on social media

Conceptual Review of Blockchain Technology, Digital Identity and Identity Verification

A blockchain functions as a decentralized digital ledger that records authenticated transactions, which are disseminated across a peer-to-peer network. Transactions are cryptographically grouped into blocks within a specified timeframe and subsequently appended to a permanent chain. Once these blocks are integrated into the chain, they cannot be modified, ensuring that the transaction chain remains publicly verifiable and resistant to hacking. These foster trust and transparency among blockchain participants concerning the transaction record, which is accessible to all involved parties [16]. Blockchain can be categorized into private or public, as well as permissioned or permissionless varieties. The framework of blockchain technology encompasses several layers, including networking, data, consensus, and control [17]. The network layer emphasizes the fundamental communication method known as a peer-to-peer (P2P) network, which serves as a distinct communication and storage architecture compared to the traditional client-server model. The data layer represents the essence of blockchain technology, comprising both the blocks and the blockchain itself. The consensus layer addresses the fault-tolerance challenges faced by distributed nodes through the application of consensus protocols. The control layer acts as the focal point for interaction among various applications and the ledger[17].

Consequently, blockchain technology functions as an online infrastructure that enhances security and flexibility, alleviating privacy and security concerns that arise from the growing reliance on the internet and other emerging technologies such as cyber-physical systems, the Internet of Things (IoT), cloud computing, and artificial intelligence (AI) [18]. Both blockchain technology and distributed ledger technology built on blockchain are regarded as significant disruptive innovations, marking a transformative shift in the evolution of the internet, evolving it from a platform for data transmission and exchange to one capable of transferring value as well [19].

Digital identity, also known as a digital entity or identity, can be referred to as the virtual representation of an individual, organization, or entity, composed of multiple datapoints such as an individual's email, username, password, birthdate, biometric data, social media profiles, and other credentials that identify and authenticate an entity in the digital environment. [20] defines digital identity as the personal interaction between individuals and their online presence. An online presence may encompass numerous accounts, credentials, and rights associated with an individual. Digital identities serve to represent an individual, organization, device, or application utilized for approval, verification, automation, and at times, impersonation in real-time. This suggests that a person's or entity's existence is acknowledged through digital identities within various applications, systems, networks, or cloud environments. Similarly, [21] characterizes digital identity as a collection of data regarding an individual's presence in the digital domain. When the information pertaining to an individual is aggregated, it creates a digital representation that allows them access to various services. Digital identity can be verified through database checks, biometric authentication, or document verification.

In parallel, [22] considers digital identity to be the online embodiment of a person or system, which is stored and overseen by computer systems. It comprises the specifics that allow the computer to identify an entity. The entity recognized by the computer may be another computer, a software application, an organization, or an individual. This identification relies heavily on features that are recognizable by computers, such as a person's password, the internet protocol (IP) address of another computer, or a media access control (MAC) address. [23] states that digital identity consists of a collection of data points that embody the characteristics and actions that identify an entity in the digital realm. Digital identity serves to authenticate applications, individuals, devices, or organizations. Consequently, this verification process is conducted to ensure that the evaluator is indeed the rightful possessor of the access. It is important to highlight that the digital identity of individuals represents their digital footprint.

[24] defines identity verification as a means of establishing that an identity is authentic. This suggests that identity verification confirms the claims of an individual regarding their asserted identity. Identity verification utilizes personal information, such as date of birth and address, to validate that an identity is genuine. It fosters trust in digital transactions and protects individuals as well as businesses from cyber threats and impersonation. Therefore, identity verification refers to a process that corroborates an individual’s claimed identity by cross-referencing it with supporting documents and evidence, ensuring authenticity and affirming the person's true identity. This involves scrutinizing security passes, official records, and legal documents to verify the identity of an individual, thereby demonstrating they are who they claim to be.

In a similar manner, [25] describes identity verification as the process of confirming or denying the authenticity of a claimed identity by comparing the records of an individual seeking access with those that have been previously verified and associated with the Personal Identity Verification (PIV) card. This indicates that effective identity verification requires prior information to be provided. [26] asserts that

identity verification is a validation process aimed at establishing the authenticity, reliability, and ownership of the personal data presented by an individual. The primary goal is to mitigate fraud-related concerns such as identity theft. Moreover, [27] emphasizes that identity verification is a critical procedure that ensures individuals are accurately recognized and that their personal information is safeguarded. Identity verification protects individuals and institutions from phishing, impersonation, and other types of fraudulent activities. It may take various forms, including biometric verification, two-factor authentication, document-based verification, and knowledge-based verification. The fundamental purpose of identity verification is to prevent fraud and foster trust among individuals and systems.

Conceptualizing Fake Accounts, Disinformation and Social Media

A fake account, commonly known as a dummy account or fictitious profile, is a virtual identity frequently established on websites, social media networks, or other digital platforms using fabricated details. [28] defines a fake account as a malicious account creation process wherein bots are utilized to generate accounts that can harm or mislead others. This represents a category of automated account fraud, in which cybercriminals employ bots to create imaginary accounts to perpetrate fraudulent activities. This indicates that the generation of fake accounts constitutes a cyberthreat, involving an attacker fabricating multiple false identities to exploit vulnerabilities in platforms, mislead users, and carry out harmful actions. Fake accounts are typically generated using automated tools capable of producing hundreds or even thousands of accounts swiftly, utilizing counterfeit or stolen information.

[29] perceives fake accounts as the harmful procedure of creating accounts with fabricated or stolen information, often aided by bots. This suggests that the generation of fake accounts involves the use of misleading information about an individual, organization, or entity to deceive others. According to [30], creating fake accounts involves employing falsified and invalid email addresses, names, phone numbers, physical addresses, dates of birth, or other personal information to set up a profile on a particular platform or website. This implies that when information is unlawfully utilized to create an online profile, a fake account is established. [31] claims that fake accounts have emerged as a significant issue, as they are frequently used to automatically disseminate information or messages. Consequently, creators of fake accounts, motivated by various factors such as malicious intent and the exploitation of free resources, pose a considerable burden and financial risk to online users.

Disinformation signifies the intentional dissemination of false or misleading information designed to mislead others. [32] characterizes disinformation as incorrect and distorted information purposely aimed at deceiving the recipients of such data. In this context, facts are intentionally misrepresented to create confusion. [33] point out that disinformation extends beyond mere deception, falsehoods, and indoctrination to encompass a variety of phenomena, including inaccurate reporting, manipulative rhetoric, and ideological manipulation. This indicates that disinformation is an intentional act. It is deliberate, premeditated, calculated, and strategic, aimed at spreading misleading and false information. Thus, it represents the intentional dissemination of incorrect information to an audience eager for knowledge. The objective of disinformation is to influence individuals' opinions. In disinformation, the truth is completely absent. What is conveyed in reports consists of facts that are fabricated, manipulated, and distorted.

[34] passionately asserts that disinformation refers to the deliberate dissemination of false information aimed at causing harm. This indicates that disinformation is a recognized act, imbued with a clear malicious intent. In this context, the propagation of misleading information is intentionally orchestrated by the originator of such messages. [34] elaborates that disinformation encompasses a wide array of distinct phenomena, including rumors, hate speech, conspiracy theories, electoral meddling, state-sponsored propaganda, and medical misinformation. It is noteworthy that disinformation is rife with biased claims

designed specifically to mislead. Similarly, [33] highlights that the digital information landscape is characterized by a variety of fictitious and flawed content that can endanger individuals and disrupt societal order.

Social media can be defined as the medium through which individuals engage with one another, enabling them to create, post, share, comment, react, or interact within digital spaces and networks. These platforms include X, WhatsApp, Facebook, Instagram, YouTube, LinkedIn, TikTok, Snapchat, Pinterest, Reddit, among others. [35] describes social media as an array of technologies that facilitate the sharing of information and ideas among users. This means that social media aids in the exchange of emotions, opinions, ideas, and thoughts. Information circulated on these platforms can take the form of infographics, text, visuals, graphs, chats, and various other multimedia formats disseminated through digital networks. [36] assert that social media integrates multimedia elements in its content. Moreover, social media enables journalists, content creators, and media organizations to maintain engagement with their audiences by sharing images, text, video, as well as 2D and 3D content.

According to [37], social media has evolved into a crucial facilitator of connectivity and information sharing, leveraging the increasing adoption and utility of mediated communication. This signifies that social media connects individuals and fosters the exchange of ideas and thoughts across its various platforms. Furthermore, the real-time aspect of social media allows messages to be dispatched and received instantaneously. [33] note that the interactive nature of social media has profoundly transformed it from a conventional means of social engagement into a potent tool for shaping social interactions, public opinion, and socio-cultural behaviors. This suggests that social media plays a significant role in influencing public opinion and perceptions. Consequently, social media enables users to engage with content through likes, shares, comments, and discussions.

Opinion Review

How Blockchain Technology Improves Digital Identity Verification.

Blockchain technology presents distinct attributes that significantly enhance digital identity verification, focusing on infrastructural characteristics such as reliability, transparency, immutability, and anonymity, rather than more disruptive elements like disintermediation and decentralization [38-40].

Transparency in blockchain technology ensures that while transactions are publicly recorded, only pseudonymous identifiers are displayed, protecting users' real identities. This level of transparency also supports traceability and boosts confidence in data authenticity, enhancing the overall reliability of digital interactions on platforms that integrate blockchain for identity management. Additionally, blockchain's immutability means that once data is entered, it cannot be altered, ensuring records are tamper-proof and can be securely verified across the network. This is particularly beneficial for handling sensitive information, such as financial or legal records, where data integrity is crucial.

Other core blockchain features such as anonymity, disintermediation, and decentralization enhance the security of digital identity verification. Anonymity is preserved through decentralized transaction addresses, safeguarding personal information and facilitating global identity verification without central oversight. This trustless framework upholds privacy while promoting worldwide accessibility. Disintermediation minimizes intermediary involvement in transactions, resulting in more direct, cost-effective, and transparent exchanges. Ultimately, decentralization empowers users to independently verify identities, supported by smart contracts that automate agreements and payments based on predetermined

criteria. Collectively, these attributes render blockchain an efficacious mechanism for secure, transparent, and reliable digital identity verification.

Combating Fake Accounts and Disinformation with Blockchain-Enabled Verification

Social media platforms can integrate blockchain-based identity verification systems to mitigate the proliferation of fake accounts across digital platforms. By requiring social media users to authenticate their identities via a blockchain system, technology firms can ensure the integrity of each account by linking them to verifiable entities with initially submitted credentials. This validation process can significantly curtail the presence of impersonated accounts on social media that disseminate disinformation and harmful messages, potentially undermining peace and democracy.

Moreover, implementing blockchain verification methods allows social media platforms like X and Facebook to substantially reduce disinformation by confirming that users represent genuine entities rather than impersonated accounts or bots. Upon successful blockchain verification, authenticated users receive an emblem or proof of reliability visible to others. Such verification on platforms plagued by fake accounts and cybercriminal activities alleviates concerns and fosters trust in engaging in digital transactions, including business, trading, learning, or social networking. Consequently, when information providers like journalists, opinion leaders, and social media influencers authenticate their identities via blockchain systems, it enhances the credibility of their posts, enabling users to engage more comfortably with such content. This verification process markedly diminishes the spread of false reports by fraudulent opinion leaders utilizing impersonated accounts for manipulation.

In addition to curbing fake accounts in the digital realm, blockchain serves as a catalyst for validating the credibility of news and information sources. Blockchain can establish an authentic network of reliable information providers, necessitating that media organizations, journalists, influencers, and bloggers verify their identities on the blockchain before being authorized to publish and share content on websites or social media. Thus, this framework introduces an additional layer of authenticity that aids users in distinguishing between credible news and misleading information.

Key Components of Decentralized Identity Systems

The core components of decentralized identity systems – Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), Identity Hubs, and Universal Resolvers – work in synergy to establish secure, private, and user-controlled digital identities. These components support a robust framework where individuals can manage their own identities without relying on centralized authorities, ensuring greater security and autonomy in digital interactions.

Decentralized Identifiers (DIDs), enable self-sovereign, verifiable identities, allowing individuals to control their digital identities independently of centralized entities [41]. DIDs are cryptographically fortified with public-private key pairs, giving users the power to authenticate their identity and share information securely without third-party interference. Each DID is supported by a DID document on a blockchain, detailing its specifications and expanding its use across multiple platforms [42]. To further enhance security, Public Key Infrastructure (PKI) is integral to DIDs, pairing each DID with a public and private key. Public keys are shared openly, while private keys are securely held by users, allowing only the DID owner to validate transactions, thereby upholding data integrity throughout the identity verification process.

Verifiable Credentials (VCs) provide another essential layer to decentralize identity systems by offering cryptographically verified, trusted claims, like certificates or identity documents, issued by credible entities such as employers or governments. VCs, stored on distributed ledgers and linked to public DIDs, reveal only necessary information while preserving user privacy. By verifying these credentials through the issuer's public key, VCs bolster the reliability of digital identity systems, making them resilient against tampering and particularly suitable for verifying identities on social media platforms [43]. Identity Hubs further empower users by acting as secure storage systems that interact with DIDs to manage personal data. Users control their data within these hubs, enabling secure sharing with third-party services while retaining data ownership, which also allows interoperability across various platforms and applications.

Moreso, Universal Resolvers facilitate the seamless functionality of decentralized identity systems by resolving DIDs across different networks. These tools, often taking the form of digital wallets, manage private keys and VCs, supporting secure identity verification across diverse platforms. Universal Resolvers are critical to the implementation of decentralized identity management systems, giving users full control over their digital identities across applications while promoting interoperability[43]. Together, these components provide a comprehensive solution for secure, interoperable, and user-governed digital identity systems, reinforcing trust in digital interactions and addressing key challenges in identity verification on social media.

Applications of Blockchain Digital Identity in Combating Fake Accounts and Disinformation on Social Media

The incorporation of blockchain technology into the realm of digital identity verification presents an extraordinarily promising opportunity for social media platforms, as it offers a systematic and effective approach to combat the pervasive issues of counterfeit accounts and the dissemination of disinformation. By implementing robust mechanisms to authenticate user identities, blockchain systems not only promote a significant degree of transparency and trust among users but also play a crucial role in diminishing the rampant spread of disinformation that often plagues online interactions. Existing literature underscores a growing enthusiasm for leveraging the tamper-resistant characteristics inherent in blockchain technology to verify social media accounts, thereby addressing the critical challenges posed by fake news. For example, research conducted by [44] introduces an innovative architectural framework that combines Software Defined Vehicular Networks with blockchain to facilitate data verification and bolster privacy across various social platforms, while [45] delve into the application of machine learning methodologies aimed at identifying and eliminating fraudulent accounts through blockchain-based verification processes, highlighting its significant effectiveness in mitigating disinformation.

Similarly, investigations into early detection mechanisms for disinformation, as exemplified by the works of [46], illustrate the increasingly critical importance of anomaly detection techniques within the broader contexts of network security, public health, and disaster response scenarios. These advanced systems meticulously evaluate user account behaviors over extended periods to identify and flag suspicious activity patterns, thereby demonstrating blockchain's remarkable capability to meticulously track and verify user interactions within social media environments. Additionally, [47] conducted a comprehensive examination of user-centric data collection strategies, aiming to gather nuanced insights regarding account activity trends and the ramifications of disinformation, which revealed that blockchain-supported tracking methodologies significantly enhance the detection of fraudulent accounts, effectively alleviating the influence exerted by malicious actors.

The vast potential for blockchain-enabled identity verification is not confined solely to individual user accounts but also extends to sophisticated federated identity management systems. As articulated by [3], users are afforded the ability to manage their digital identities across a multitude of social platforms, thereby fostering a high degree of interoperability between diverse service providers while simultaneously safeguarding user privacy in an increasingly interconnected digital landscape. This functionality is particularly beneficial as it supports the implementation of single-sign-on (SSO) services across trusted domains, with blockchain technology facilitating seamless identity verification processes and ensuring the portability of user profiles across various online service providers.

Decentralized identity systems, underpinned by blockchain technology, present a revolutionary paradigm shift in the management of digital identities, empowering individuals with self-sovereignty, enhanced security, and seamless interoperability. Essential components such as Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), and Identity Hubs collectively contribute to the establishment of robust identity verification frameworks, which serve to protect users and guarantee their accurate representation on social media platforms. As an increasing number of social media platforms begin to adopt blockchain technology for the purpose of digital identity verification, the field is poised to hold substantial promise in its efforts to combat disinformation and nurture a more secure, user-controlled online ecosystem.

Blockchain Challenges and the Criteria for Assessing its Solutions

Despite the potential benefits, several challenges hinder the widespread adoption of blockchain-based digital identities:

1. Technological hurdles: Are blockchain interoperability, security and privacy, quantum resilience, artificial intelligence, lack of governance, standards, and regulations [39]. The most prominent concerns for practitioners relate to maturity and scalability[38]. Other blockchain technology-related issues are efficiency, energy consumption, and transaction cost. Efficiency and energy consumption are related as the "proof-of-work" model currently consumes inordinate amounts of electricity, and consequently affects the transaction cost. These issues are of a technical nature and reflect the growth of diverse applications from the basic blockchain technology [48].
2. Regulatory challenges: Legal frameworks must adapt to accommodate decentralized identity systems. Thus, the criteria to be considered when deciding if a blockchain solution is feasible are: usability, functionality, performance, platform support, security, privacy, network topology, modularity, interoperability, and cost [49]. Consideration of these criteria results in the possible conclusions of 'traditional ledger database blockchain not needed', or 'public permissionless blockchain platform needed', 'public permissioned blockchain needed', 'private permissionless blockchain platform needed', or 'private permissioned blockchain platform needed'[50].

Theoretical Framework

The Technology Acceptance Model (TAM) is the theory upon which this study is anchored. The Technology Acceptance Model (TAM) is a theoretical framework that aims to understand and predict an individual's acceptance and use of technology. It was first proposed by [51] and has since become one of the most widely studied models in the field of information systems. The core elements of the Technology Acceptance Model are:

Perceived Usefulness (PU): This refers to the degree to which a person believes that using a particular technology will enhance their job performance or facilitate achieving specific goals. Perceived usefulness

is influenced by factors such as the perceived impact of the technology on productivity, efficiency, and effectiveness. Perceived Ease of Use (PEOU): This refers to the degree to which a person believes that using a particular technology will be free from effort. It encompasses aspects such as the ease of learning, ease of navigation, and simplicity of interface design. Perceived ease of use directly affects the intention to use a technology. Since the respondents are students who are majorly young people, it is believed that young people have positive attitudes towards technology. Therefore, Technology Acceptance Model is relevant to this study's positive attitudes of users and media house towards acceptance and adoption of blockchain in combating fake accounts and disinformation on social media.

Method

The study employed quantitative survey to investigate user perceptions and acceptance of blockchain-enabled digital identity solutions. The study concentrated on social media users and media organizations, employing a purposive sampling method to choose participants with experience in digital identity management and blockchain. The Google Form indicates the total number of respondents and the percentage of questionnaires completed. A total of 208 completed e-copies of questionnaires were deemed appropriate for analysis. Table 1 details the scale items used in this study. The questionnaire form consisted of two main sections. The first section requested the respondents to provide their demographic information (see Table 1). The second section consisted of 21 measurement items to measure the various constructs in the research objectives. Items were rated on a 5-point Likert scale from 1 (strongly disagree) to 5 (strongly agree), with a higher score indicating a higher level of the variable. The collected data was coded into SPSS 26, for data screening, statistical analysis and correlations while the hypothesis was analyzed using regression analysis.

Data Presentation and Analysis

The study conducted descriptive statistics and correlation analysis on all studied variables. Table 2-5 presents the means and standard deviations of the variables along with the correlations between them. The research findings provide comprehensive insights on verified views about how adoption of blockchain-enabled digital identity verification significantly reduces the prevalence of fake accounts and disinformation on social media.

Table 1: Respondents' demographic information

Variables	**Category**	**Frequency**	**Percentage**
Gender	Male	147	70.9
	Female	61	29.1
Age	18–30 years	126	60.5
	31–45 years	71	34.2
	Above 45 years	11	5.3
	FSLC	20	9.5

Educational qualification	BSc/HND	139	67.2
	MSc & Above	49	23.3

Source: Field Survey, 2024

Table 2: Examine how blockchain's decentralized and immutable nature can improve the security and integrity of digital identities compared to traditional centralized systems

Statements	SA	A	D	SD	Mean	Stand Dev
I believe that blockchain's decentralized nature offers more security for digital identity verification compared to traditional centralized systems.	78 (37.5%)	61 (29.2%)	43 (20.8%)	26 (12.5%)	3.73	1.36
I feel that verified digital identities are important in reducing disinformation on social media	84 (40.3%)	62 (29.7%)	38 (18.3%)	24 (11.7%)	3.67	1.31
I believe blockchain technology can provide better privacy protection for my personal data compared to current systems	132 (63.5%)	57 (27.3%)	19 (9.2%)	0.00	4.21	0.85

Source: Field Survey, 2024

Table 2 indicates that a majority of respondents perceive blockchain's decentralized nature as offering enhanced security for digital identity verification over traditional systems. Moreover, a significant number agree that verified digital identities play a crucial role in mitigating disinformation on social media. Furthermore, a substantial portion believes that blockchain technology can improve personal data privacy, thereby reducing fake accounts and misinformation.

Table 3: Evaluate the level of public awareness, acceptance, and trust in blockchain-based identity solutions among users

Statements	SA	A	D	SD	Mean	Stand Dev.
I am aware that blockchain technology is being used for digital identity verification	105 (50.3%)	78 (37.8%)	25 (11.9%)	-	3.23	1.34

I feel familiar with the concept of blockchain technology.	96 (46.2%)	48 (22.9%)	44 (21.2%)	20 (9.7%)	3.60	1.16
I trust blockchain technology for securing my digital identity compared to current methods.	103 (49.5%)	73 (35.2%)	2 (15.3%)	-	4.13	1.00
I would feel safer using social media platforms if they adopted blockchain-based identity verification for all users.	82 (39.5%)	91 (43.7%)	31 (14.9%)	4 (1.9%)	4.13	0.98

Source: Field Survey, 2024

Table 3 reveals that many respondents recognize the application of blockchain technology in digital identity verification, highlighting the necessity for sufficient funding to convey its advantages. Additionally, a notable percentage identifies the lack of technical expertise as a considerable obstacle to promoting blockchain-based identity solutions, emphasizing the need for increased technical knowledge among media organizations and users. Furthermore, respondents express concern that inadequate governmental policy frameworks may impede the promotion of blockchain identity verification systems, underscoring the significance of supportive policies for user adoption and awareness. Consequently, a majority believes that implementing blockchain-based identity verification could enhance safety on social media platforms.

Table 4: Identify essential strategies and protocols employed by media organizations utilizing blockchain technology to bolster information reliability

Statements	**SA**	**A**	**D**	**SD**	**Mean**	**Stand Dev.**
Digital watermarking is an effective strategy for enhancing information reliability	134 (64.5%)	48 (22.9%)	26 (12.6%)	-	4.48	0.85
Content hashing helps improve the reliability of information	156 (75.0%)	41 (19.5%)	-	11 (5.5%)	4.48	1.11
Smart contracts contribute to ensuring reliable information	121 (57.8%)	53 (25.7%)	34 (16.5%)	-	4.15	1.13
Distributed ledger technology enhances the reliability of information in media organizations.	113 (54.3%)	61 (29.5%)	21 (10.2%)	13 (6.0%)	4.00	1.22

Blockchain-based content management systems support reliable information sharing	137 (65.8%)	47 (22.9%)	24 (11.3%)	-	4.48	0.85
Public key cryptography is an effective protocol for securing reliable information	120 (57.9%)	68 (32.5%)	20 (9.6%)	-	4.48	1.11
Consensus mechanisms contribute to the reliability of information	109 (52.8%)	64 (30.6%)	26 (12.5%)	8.5 (4.1%)	4.15	1.13
Data encryption enhances the reliability of information	124 (59.8%)	62 (29.7%)	22 (10.5%)	-	4.00	1.22

Source: Field Survey, 2024

Table 4 demonstrates that most respondents strongly agree that watermarking is an effective measure to curb disinformation on social media, reflecting a favorable view of blockchain technology's role in bolstering online information credibility. Additionally, a significant majority concurs that the application of blockchain protocols, like content hashing and digital watermarking, fosters user confidence in digital content reliability, suggesting that awareness of these technological safeguards increases trust in online information.

Table 5: Assess the efficacy of these blockchain protocols in reducing the spread of disinformation and enhancing user confidence in digital content

Statements	**SA**	**A**	**D**	**SD**	**Mean**	**Stand Dev.**
I frequently encounter fake accounts or disinformation on social media platforms.	103 (49.7%)	99 (47.5%)	-	6 (2.8%)	4.21	0.87
I think current identity verification methods on social media are effective in preventing fake accounts.	77 (37.2%)	72 (34.4%)	59 (28.4%)	-	4.08	0.92
I feel that verified digital identities are important in reducing disinformation on social media.	100 (48.2%)	86 (41.1%)	22 (10.7%)	-	4.08	0.85
I think blockchain-based identity verification could be effective in reducing the spread of fake news on social media.	71 (34.3%)	108 (51.6%)	29 (14.1%)	-	3.96	1.01

I see increased security as a primary benefit of using blockchain for digital identity verification on social media	115 (55.3%)	84 (40.2%)	9 (4.5%)	-	3.98	1.00
I view user privacy concerns as a significant challenge in implementing blockchain-based identity verification on social media.	65 (31.4%)	90 (43.7%)	32 (14.8%)	21 (10.1%)	3.92	1.03

Source: Field Survey, 2024

Table 5 reveals that a substantial portion of participants acknowledge the prevalence of fake accounts and misinformation on social media. Many agree on the effectiveness of current identity verification methods in limiting fake accounts. There is also significant support for the role of digital identities in combating disinformation, with over half of respondents recognizing that identity verification could curb fake news. The majority view enhanced security as a major benefit of using blockchain for digital identity verification, and a notable portion believes that consensus mechanisms bolster information reliability, highlighting the value of technological safeguards in fostering trust online.

Table 6: Model Summary

Mo del	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.649[a]	.421	.363	2.46011

a. Predictors: (Constant), Blockchain-enabled Digital Identity Verification

Table 7: ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	244.011	1	244.01	64.448	.000[b]
	Residual	560.355	148	3.786		
	Total	804.367	149			

a. Dependent Variable: Prevalence of fake accounts and disinformation on social media

b. Predictors: (Constant) Adoption of blockchain-enabled digital identity verification

Table 8: Coefficients

	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	9.473	2.342		7.093	.000
Adoption of blockchain-enabled digital identity verification	.661	.104	.471	3.618	.000

a. Dependent Variable: Sustainable Urban Development

Discussion of Findings

This research examines the effect of blockchain-based digital identity verification in the fight against fake accounts and misinformation on social media. The results indicate that the decentralized and unchangeable characteristics of blockchain greatly enhance the security and authenticity of digital identities when compared to conventional centralized systems (X = 3.39, SD = 1.73). This highlights the critical role of decentralized identity management in mitigating the risks of identity theft and data breaches. Additionally, the research uncovered a strong level of public awareness, acceptance, and trust in blockchain-driven identity solutions among users (X = 4.18, SD = 2.81). This suggests that users are progressively acknowledging the capacity of blockchain technology to bolster their online security and promote trust in digital engagements.

The study also pinpointed vital strategies and protocols adopted by media organizations that leverage blockchain technology to enhance information reliability (X = 3.61, SD = 1.71). These strategies are essential in tackling the issues presented by fake accounts and misinformation on social media platforms. The effectiveness of these blockchain protocols in curbing the spread of misinformation and boosting user confidence in digital content was further validated by a mean score of (X = 3.91, SD = 1.86), indicating that users feel increasingly secure and assured when interacting with blockchain-supported systems.

The outcomes of the hypothesis testing indicated that the implementation of blockchain-enabled digital identity verification had a significant effect on the prevalence of fake accounts and misinformation on social media, accounting for around 42.1% of the observed variance. This result is consistent with [52], who outlined how blockchain's decentralized structure decreases the likelihood of identity theft and data breaches, making it more difficult for malicious entities to alter identity records and thus lowering the occurrence of fake accounts. This transition diminishes dependence on centralized authorities, emphasizing the significance of decentralized identity management in establishing a more secure digital identity framework.

Conclusion

The results of this research present strong evidence that the use of blockchain-based digital identity verification significantly contributes to the fight against fake accounts and misinformation on social media platforms. The regression analysis indicated that blockchain technology explains approximately 42.1% of

the variance in the occurrence of fake accounts and misinformation, highlighting its potential as a powerful solution for improving the integrity of digital identities. The positive correlation discovered between blockchain-based identity verification and the decrease of misinformation stresses the critical role of decentralized and immutable systems in building trust among users. By alleviating the risks associated with identity fraud and refining the verification processes, blockchain technology can effectively reduce the spread of misleading information while boosting user confidence in the content they encounter online. Moreover, the study emphasizes that media organizations utilizing blockchain protocols such as content hashing, digital watermarking, and smart contracts can significantly improve the reliability of information shared through digital channels. These strategies not only tackle the issues brought about by fake accounts and misinformation but also bolster user confidence in digital content. Consequently, the integration of blockchain technology in digital identity verification can be crucial in fostering a more trustworthy online environment.

Recommendations

The findings of the study proffered some recommendations to enhance the effectiveness of blockchain-based digital identity verification in addressing fake accounts and misinformation on social media:

i. Awareness campaigns must be intensified by all stakeholders. Consequently, media organizations and stakeholders should initiate extensive awareness campaigns to inform the public about the advantages and functionalities of blockchain technology in digital identity verification. Increased awareness can nurture greater acceptance and trust among users.

ii. There should be collaboration with tech developers. As such, media organizations ought to partner with technology developers to design user-friendly blockchain solutions for digital identity verification. Streamlining the user experience can motivate more individuals to embrace these technologies. Policy Development: Governments should formulate and enforce policies that encourage the adoption of blockchain technology for identity verification on social media platforms. These policies could encompass guidelines for data privacy, security measures, and the obligations of platforms in addressing fake accounts and misinformation.

iii. Partnerships for implementation should also be leveraged as one of the ways forward. Stakeholders, including social media platforms and regulatory bodies, should establish partnerships to effectively implement blockchain-based identity verification systems. Collaboration can aid in overcoming implementation barriers and foster standardized practices.

References

[1] Agudelo, G. E. R., Parra, O. J. S., & Velandia, J. B. (2018). Raising a model for fake news detection using machine learning in Python. Challenges and opportunities in the digital era: 17th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2018, Kuwait City, Kuwait, October 30–November 1, 2018, Proceedings 17, 596–604.

[2] Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & information systems engineering*, *59*, 183-187.

[3] Zhu, X., He, D., Bao, Z., Luo, M., & Peng, C. (2023). An efficient decentralised identity management system based on range proof for social networks. *IEEE Open Journal of the Computer Society*, *4*, 84-96.

[4] Monrat, A. A., Schelén, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. *Ieee Access*, *7*, 117134-117151.
[5] Merkle, R. C. (1979). *Secrecy, authentication, and public key systems*. Stanford university.
[6] Nakamoto, S., & Bitcoin, A. (2008). A peer-to-peer electronic cash system. *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf*, *4*(2), 15.
[7] Herold, D. M., Saberi, S., Kouhizadeh, M., & Wilde, S. (2022). Categorising transaction costs outcomes under uncertainty: a blockchain perspective for government organisations. *Journal of Global Operations and Strategic Sourcing*, *15*(3), 431-448.
[8] Buterin, V., Coleman, J., & Wampler-Doty, M. (2015). Notes on scalable blockchain protocols (version 0.3. 2). Retrieved from https://vitalik.ca/files/scalable_blockchain_protocols.pdf
[9] Christodoulou, I., Rizomyliotis, I., Konstantoulaki, K., Nazarian, A., & Binh, D. (2024). Transforming the remittance industry: Harnessing the power of blockchain technology. *Journal of Enterprise Information Management*, *37*(5), 1551-1577.
[10] Naseer, I. (2023). AWS cloud computing solutions: optimising implementation for businesses. *Statistics, Computing and Interdisciplinary Research*, *5*(2), 121-132.
[11] Materwala, H., & Ismail, L. (2022). Performance and energy-aware bi-objective tasks scheduling for cloud data centers. *Procedia Computer Science*, *197*, 238-246.
[12] Sharma, A., Bahl, S., Bagha, A. K., Javaid, M., Shukla, D. K., & Haleem, A. (2020). Blockchain technology and its applications to combat COVID-19 pandemic. *Research on Biomedical Engineering*, 1-8.
[13] Ush Shahid, I., Anjum, M. T., Hossain Miah Shohan, M. S., Tasnim, R., & Al-Amin, M. (2021). Authentic facts: A blockchain based solution for reducing fake news in social media. In *Proceedings of the 2021 4th International Conference on Blockchain Technology and Applications* (pp. 121-127).
[14] Pelt, R. V., Jansen, S., Baars, D., & Overbeek, S. (2021). Defining blockchain governance: a framework for analysis and comparison. *Information Systems Management*, *38*(1), 21-41.
[15] Hughes, H. (2020). Blockchain and the future of secured transactions law. *Stan. J. Blockchain L. & Pol'y*, *3*, 21
[16] Matei, G. (2020). Blockchain technology: support for collaborative systems. *Informatica Economica*, 24(2/2020), 15-26.
[17] Zeng, S. -Q., Huo, R., Huang, T., Liu, J., Wang, S., & Feng, W. (2020). Survey of blockchain: principle, progress and application', *Journal on Communications*, 41(1), 134-151.
[18] Tavera Romero, C. A., Castro, D. F., Ortiz, J. H., Khalaf, O. I., & Vargas, M. A. (2021). Synergy between circular economy and industry 4.0: a literature review. *Sustainability*, 13(8):4331.
[19] Truong, N. B., Um, T. -W., Zhou, B., & Lee, G. M. (2018). Strengthening the blockchain-based internet of value with trust' *2018 IEEE International Conference on Communications (ICC)*.
[20] BeyondTrust. (2024). Digital identity. https://www.beyondtrust.com/resources/glossary/digital-identity.
[21] Bowyer, C. (2024). What is digital identity? Your guide to digital identity. https://onfido.com/blog/digital-identity/
[22] Cloudfare. (2024) What is digital identity? https://www.cloudflare.com/learning/access-management/what-is-identity/
[23] Garey, L. (2024). What is digital identity? https://www.oracle.com/ng/security/identity-management/digital-identity.
[24] Tomlinson, G. (2024). What is identity verification and how does it work? https://www.gbgplc.com/en/blog/what-is-identity-verification-and-how-does-it-work.

[25] NIST. (2024). Identity verification. htps://csrc.nist.gov/glossary/term/identity_verification

[26] Stepnov, J. (2023). What is identity verification & how is it done? An explainer. https://regulaforensics.com/blog/identity-verification.

[27] Tookitaki. (2024). Identity verification: importance, methods and online solutions. https://www.tookitaki.com/glossary/identity-verification.

[28] DataDome. (2022). What is fake account creation? how to prevent fake account creation. https://datadome.co/guides/account-takeover/how-to-detect-prevent-fake-account-creation-websites-apps.

[29] Human. (2024). What is fake account creation? How to prevent it. https://www.humansecurity.com/learn/topics/what-is-fake-account-creation

[30] IPQS. (2024). How to prevent fake account creation fraud. https://www.ipqualityscore.com/articles/view/107/prevent-fake-account-creation-fraud.

[31] Keil, M. (2022). What are fake accounts and how can they be worth $44 Billion? https://cequencestage.wpengine.com/blog/cq-prime-threat-research/what-are-fake-accounts-and-how-can-they-be-worth-44-billion.

[32] APA. (2023). Misinformation and disinformation. https://www.apa.org/topics/journalism-facts/misinformation-disinformation.

[33] Ja'afaru, S. G. & Asemah, E. S. (2024). How social media shape public opinion through propaganda and the spread of disinformation. In E. S. Asemah (Ed.), *Communication and Media Dynamics* (pp. 26-41). Enugu: Franklead Printing and Publishing Company.

[34] Leidel, S. (2024). Disinformation: current definitions and examples. https://akademie.dw.com/en/disinformation-current-definitions-and-examples/a-67786912.

[35] Dollarhide, M. (2024). Social media: definition, importance, top websites and apps. https://www.investopedia.com/terms/s/social-media.asp

[36] Inobemhe, K. & Santas T. (2021). Adoption and use of social media in the newsroom operations of selected television stations in Nigeria. *Styles of Communication.* 13(1), 43-59.

[37] Santas, T., & Inobemhe, K. (2021). Social media regulation in a democratic Nigeria: challenges and implications. *Media & Communication Current*, 5(1), 71-88.

[38] Flovik S., Moudnib R. A, & Vassilakopoulou, P. (2021). Determinants of blockchain technology introduction in organisations: an empirical study among experienced practitioners', *Procedia Computer Science*, 181, 664-670.

[39] Gad, A. G., Mosa, D. T., Abualigah, L., & Abohany, A. A.s (2022). Emerging trends in blockchain technology and applications: a review and outlook', *Journal of King Saud University - Computer and Information Sciences*, 34(9):6719-6742, doi:10.1016/j.jksuci.2022.03.007.

[40] Rajasekaran, A. S., Azees, M. & Al-Turjman, F. (2022). A comprehensive survey on blockchain technology. *Sustainable Energy Technologies and Assessments*, 52, https://doi.org/10.1016/j.seta.2022.102039.

[41] Alzahrani, B. (2020). An information-centric networking based registry for decentralised identifiers and verifiable credentials. *IEEE Access*, *8*, 137198-137208.

[42] Van Bokkem, D., Hageman, R., Koning, G., Nguyen, L., & Zarin, N. (2019). Self-sovereign identity solutions: the necessity of blockchain technology. *arXiv preprint arXiv:1904.12816*.

[43] Patil, A. S., Belhekar, S. P., Burkul, R. S., Sambare, M. V., & Reddy, P. K. T. V. (2019). Review Paper on – Smart Wallet. *International Research Journal of Engineering and Technology (IRJET)*, *6*(10), 1258-1260.

[44] Yahiatene, Y., & Rachedi, A. (2018). Towards a blockchain and software-defined vehicular networks approaches to secure vehicular social network. In *2018 IEEE Conference on Standards for Communications and Networking (CSCN)* (pp. 1-7).

[45] Kantartopoulos, P., Pitropakis, N., Mylonas, A., & Kylilis, N. (2020). Exploring adversarial attacks and defences for fake twitter account detection. *Technologies*, *8*(4), 64.

[46] Averza, A., Slhoub, K., & Bhattacharyya, S. (2022). Evaluating the influence of twitter bots via agent-based social simulation. *IEEE Access*, *10*, 129394-129407.

[47] Cola, G., Mazza, M., & Tesconi, M. (2023). Twitter newcomers: uncovering the behaviour and fate of new accounts through early detection and monitoring. *IEEE Access*, *11*, 55223-55232.

[48] Khan, D., Jung, L. T., & Hashmani, M. A. (2021). Systematic literature review of challenges in blockchain scalability. *Applied Sciences*, 11(20):9372.

[49] Kim, H., & Kim, D. (2024). Methodological advancements in standardising blockchain assessment', *IEEE Access*. 12, 35552-35570. https://doi.org/10.1109/ACCESS.2024.1234567

[50] Almeshal, T. A, & Alhogail, A. A. (2021). Blockchain for businesses: a scoping review of suitability evaluations frameworks', *IEEE Access*, 9:155425-155442.

[51] Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, *35*(8), 982–1003. https://doi.org/10.1287/mnsc.35.8.982

[52] Aydar, M., Ayvaz, S., & Cetin, S. C. (2019). Towards a Blockchain based digital identity verification, record attestation and record sharing system. *arXiv preprint arXiv:1906.09791*.