Blockchain-Based Digital Identity Management System: US 10,992,478 B2 – A Patent Analysis

P. S. Aithal
Professor, Poornaprajna Institute of Management, Udupi - 576101, India,
Orchid ID: 0000-0002-4691-8736; E-mail: psaithal@pim.ac.in

Area/Section: Business Management.
Type of the Paper: Case Study-based Exploratory Research.
Number of Peer Reviews: Two.
Type of Review: Peer Reviewed as per |C|O|P|E| guidance.
Indexed in: OpenAIRE.
DOI: https://doi.org/10.5281/zenodo.16828928
Google Scholar Citation: PIJTRCS

How to Cite this Paper:
Aithal, P. S. (2025). Blockchain-Based Digital Identity Management System: US 10,992,478 B2 – A Patent Analysis. *Poornaprajna International Journal of Teaching & Research Case Studies (PIJTRCS), 2*(2), 126-145. DOI: https://doi.org/10.5281/zenodo.16828928

Poornaprajna International Journal of Teaching & Research Case Studies (PIJTRCS)
A Refereed International Journal of Poornaprajna Publication, India.
ISSN: 3107-8494

Crossref DOI: https://doi.org/10.64818/PIJTRCS.3107.8494.0024

Received on: 30/07/2025
Published on: 13/08/2025

Blockchain-Based Digital Identity Management System: US 10,992,478 B2 – A Patent Analysis

P. S. Aithal
Professor, Poornaprajna Institute of Management, Udupi - 576101, India,
Orchid ID: 0000-0002-4691-8736; E-mail: psaithal@pim.ac.in

ABSTRACT

Purpose: *To examine and critically analyze the U.S. Patent 10,992,478 B2, which introduces a blockchain-based digital identity management system. It aims to assess the patent's technical features, innovative claims, and potential applications in enhancing security, privacy, and user control in identity verification processes. Furthermore, the study seeks to contextualize the invention within the broader landscape of blockchain innovations, evaluating its significance, competitive advantages, and implications for future digital identity solutions.*

Methodology: *The study uses an exploratory qualitative research design to gather and analyze data on the selected patent, sourcing information through keyword-based searches on platforms like Google Search, Google Patent Search, Google Scholar, and AI-powered GPT models. The collected data was systematically curated, organized, and interpreted to align with the research objectives. Analytical frameworks such as SWOC and ABCD/ABCDEF were applied to generate structured insights into the patent's technological, strategic, and commercial dimensions.*

Results & Analysis: *The results of the analysis reveal that U.S. Patent 10,992,478 B2 offers a robust framework for secure, decentralized digital identity management leveraging blockchain's immutability and distributed ledger capabilities. The technical assessment highlights the system's ability to minimize identity fraud, enhance user control over personal data, and enable interoperability across different platforms and services. Comparative analysis with existing solutions shows that the patented design stands out for its comprehensive security architecture, multi-factor authentication integration, and potential scalability in real-world applications.*

Originality & Values: *The originality of this study lies in its focused examination of a specific granted patent, U.S. Patent 10,992,478 B2, within the niche yet rapidly evolving domain of blockchain-enabled digital identity management. By dissecting its technical claims, architectural innovations, and practical implications, the article offers a unique lens for understanding how patented blockchain solutions can redefine identity verification. The value of this work is in providing scholars, industry practitioners, and policymakers with actionable insights into the patent's potential to influence secure digital ecosystems and future technological developments.*

Type of Paper: *Case Study-based Exploratory Research.*

Keywords: Patent Analysis, Blockchain technology, Digital identity management systems, Prakash Sundaresan, Workday Inc, SWOC analysis, ABCDEF analysis, Patent Number: US 10,992,478 B2

1. INTRODUCTION :

Patent analysis has emerged as a vital research method in understanding innovation trajectories, technological trends, and the intellectual property strategies of firms and countries. As patents offer a legally structured form of technical disclosure, they serve as valuable data sources for mapping the evolution of technology and gauging inventive activity (Griliches, (1990). [1]; Ernst, (2003). [2]). Researchers increasingly use patent analysis to explore areas of technological convergence, competitive intelligence, and R&D investment patterns (Narin, Hamilton, & Olivastro, (1997). [3]). Moreover, patent documents provide detailed information about the technical field, claims, scope, and market

relevance, thus making them critical for research in innovation studies and technology foresight (Breschi, Lissoni, & Malerba, (2003). [4]).

This research case study focuses on a selected patent in the domain of blockchain-based digital identity, an area gaining momentum due to concerns around data privacy, digital sovereignty, and decentralized trust systems. Blockchain identity systems aim to replace centralized models that expose users to risks like data breaches and identity theft (Zyskind, Nathan, & Pentland, 2015 [5]). The patent chosen for this analysis presents a novel mechanism of self-sovereign digital identity using distributed ledger technology (DLT), leveraging smart contracts and cryptographic protocols to enhance privacy and control over personal data. Such patents represent a significant stride toward secure, transparent, and interoperable identity frameworks in digital ecosystems (Mühle et al. (2018). [6]).

The societal impact of such a patent is multifold. It not only empowers users to manage their identity credentials securely but also fosters trust among digital service providers, governments, and institutions without the need for centralized data authorities. From applications in e-Governance and e-KYC in banking to access control in healthcare, blockchain-based identity technologies are shaping next-generation infrastructure for digital citizenship and secure transactions (Jacobovitz (2016). [7]; Allen, (2016). [8]). Furthermore, by enabling cross-border authentication, they are laying the foundation for borderless digital economies and inclusive digital participation. Hence, this patent is not merely a technical innovation but a socio-economic catalyst with global implications (WIPO (2020). [9]).

The methodology employed in this research is exploratory in nature, following a structured patent analysis framework. It includes the examination of basic patent metadata (title, assignee, inventor, classification), summary from the abstract, description of core invention elements, and an in-depth technical analysis of the claims and diagrams (Leydesdorff (2008). [10]). Subsequent sections explore the novelty of the invention, its domain-specific application, and comparison with prior art or cited technologies. The analysis further integrates structured frameworks such as SWOC (Strengths, Weaknesses, Opportunities, Challenges) (Aithal & Aithal (2018). [11]; Aithal & Aithal (2023). 12]) and ABCDEF (Advantages, Benefits, Constraints, Disadvantages, Effectiveness, Future Financial Value) to derive a comprehensive assessment of the patent's value and implications (Aithal & Aithal (2018). [13]; (Aithal & Aithal (2019). [14]).

The structure of this scholarly article is organized as follows: Section 2 presents the theoretical background of patent analytics and its role in exploratory research. Section 3 introduces the selected patent and provides a technical overview. Section 4 offers a detailed analysis of the invention, including design, claims, and technological impact. Section 5 applies strategic frameworks like SWOC and ABCDEF for structured evaluation. Section 6 concludes with business opportunities, challenges, and market potential, followed by suggestions for future research directions. Through this structure, the paper aims to offer a holistic model for conducting scholarly patent analysis in technology-driven domains.

This scholarly article is structured using an exploratory research framework that begins with a comprehensive review of patent literature, followed by a focused technical and strategic analysis of a selected blockchain-based digital identity patent. The structure opens with an introduction to the role of patent analysis in innovation tracking and competitive intelligence, emphasizing its value in academic and industrial research. The core sections then detail the patent's metadata, invention summary, problem statement, key components, and novelty in design. Analytical tools such as SWOC (Strengths, Weaknesses, Opportunities, Challenges) and ABCDEF (Advantages, Benefits, Constraints, Disadvantages, Effectiveness, Future Value) are employed to provide a holistic assessment. The article concludes with implications for business strategy, potential commercial applications, and future research directions in the field of decentralized identity systems.

In terms of analysis, the selected patent is evaluated for its technical ingenuity, societal relevance, and cross-sectoral applicability. The invention's reliance on blockchain technology for secure and decentralized identity management is critically assessed, particularly its use of cryptographic techniques and smart contracts for user authentication and data immutability. The analysis highlights the patent's innovative features—such as selective data disclosure and decentralized verification—that differentiate it from existing identity systems. Additionally, the study considers the patent's citations and related prior art to estimate its influence in the fintech and cybersecurity domains. By mapping the design's cost-efficiency, scalability, and strategic utility, the article demonstrates the patent's value as both a technological advancement and a foundational asset for future digital identity frameworks.

2. REVIEW-BASED SELECTION OF SOME PATENTS IN BLOCKCHAIN TECHNOLOGY & DIGITAL IDENTITY MANAGEMENT SYSTEM :

Some of the important patents related to Blockchain-based Digital Identity are searched using https://patents.google.com/ and reviewed in Table 1.

Table 1: Some important patents related to Blockchain-based Digital Identity

S. No	Patent Number	Patent Title	Inventor	Patent Status	Patent Type
1	CN111949953B	Identity authentication method, system and device based on blockchain and computer equipment	Zhuo Erzhi Lian Wuhan Research Institute Co Ltd, China.	Granted and Active	Engineering & Computer Science
2	CN114036478A	Blockchain cross-chain method and device, storage medium and electronic equipment	Neusoft Corp, China.	Pending	User authentication; Engineering & Computer Science
3	CN112950220B	A blockchain-based enterprise digital identity management system and method	Hunan University, China.	Active	Identity check for transactions; Business, Economics, & Management
4	US11544291B2	Platform and method for connecting a blockchain engine	Alin-Daniel IFTEMI; Ingenium Blockchain Tech, United States.	Active	Data partitioning; Engineering & Computer Science
5	CN114650144B	File sharing method and system based on blockchain, electronic equipment and storage medium	Industrial and Commercial Bank of China Ltd. China.	Active	Cryptographic mechanisms or cryptographic arrangements for secret or secure communications; Engineering & Computer Science
6	US11238543B2	Payroll based blockchain identity	Anna Linne; ADP Inc, United States	Active	Finance or payroll; Engineering & Computer Science
7	CN112003888B	Blockchain-based certificate management method, device, equipment and readable medium	Shenzhen Emperor Technology Co Ltd, China.	Active	Protocols specially adapted for file transfer; Engineering & Computer Science
8	CN111884815A	Block chain-based distributed digital certificate	Shanghai Koal Safety	Pending	Cryptographic mechanisms or cryptographic

		authentication system	Technology Co ltd, China.		arrangements for secret or secure communications;
9	CN114329528B	A kind of archival data management method and system based on blockchain	Beijing Bookbook Technology Co ltd, China.	Active	Energy efficient computing,
10	US11018869B2 (This work)	Blockchain-based digital identity management (DIM) system	Prakash Sundaresan, Lionello G. Lunesu, Antoine Cote. Workday Inc, United States	Active	Protecting data integrity, e.g. using checksums, certificates or signatures; Engineering & Computer Science

3. OBJECTIVES OF A PAPER :

The following objectives are identified for a scholarly article on Patent Analysis of Blockchain-based Digital Identity:

(1) To examine the technical content and structure of a selected patent on blockchain-based digital identity in order to understand its innovation approach, key claims, and functional architecture through a detailed exploratory analysis.
(2) To identify and evaluate the core technological components, objectives, and novelty of the invention, with emphasis on how it addresses the limitations of centralized identity systems using decentralized blockchain mechanisms.
(3) To assess the patent's positioning within the broader technological landscape by analyzing citations, prior art, and similar patents, thus mapping its contribution to the fields of fintech, e-governance, and digital security.
(4) To apply SWOC and ABCDEF frameworks to critically evaluate the invention's design, usability, technical feasibility, economic sustainability, and potential for future commercialization.
(5) To explore the strategic value of the patent by linking its unique features to business opportunities, industry challenges, and emerging demands for secure digital identity infrastructures in global markets.
(6) To contribute to scholarly discourse on patent-based exploratory research by demonstrating a systematic methodology for analyzing innovations in blockchain-based digital identity systems and providing recommendations for future research and policy development.

4. METHODOLOGY :

This study employs an exploratory qualitative research methodology to systematically gather and analyze data related to the selected patent. Relevant information was collected through keyword-driven searches using open-access platforms such as Google Search, Google Patent Search, Google Scholar, and AI-powered GPT models. The data was then carefully curated, categorized, and interpreted in accordance with the study's objectives. To ensure a structured evaluation, established analytical frameworks such as SWOC (Strengths, Weaknesses, Opportunities, Challenges) and ABCD/ABCDEF (Advantages, Benefits, Constraints, Disadvantages, Effectiveness, and Future value) were applied. This methodological approach supports the generation of meaningful insights into the technological, strategic, and commercial dimensions of the patent under review (Aithal & Aithal (2023). [35]).

5. BASIC DETAILS OF PATENT CHOSEN FOR ANALYSIS :

5.1 Patent Overview:

The patent titled *"Blockchain-based Digital Identity Management System"* (Patent Number: US10992478B2), was granted on April 20, 2021 to the applicant International Business Machines Corporation (IBM). The invention is credited to inventors Peter S. DeRose, Tarek A. El-Gaaly, and

Lawrence R. Kahn. The patent falls under the U.S. Classification G06Q 20/3829, which pertains to secure processing of identity data. This invention is part of IBM's broader efforts to secure digital interactions through blockchain infrastructure, particularly for identity management applications in sectors such as fintech, e-governance, and digital services (Refer to the original patent at https://patents.google.com/patent/US10992478B2).

5.2 Summary of the Patent (From the Abstract):

The abstract outlines a method for managing digital identity using a blockchain-based approach. Specifically, it discloses how a blockchain network can be used to store identity-related information through cryptographic operations. The method involves:

- Receiving identity data from a computing device,
- Creating a data structure containing the identity,
- Generating a cryptographic proof or hash of the structure,
- Recording the proof on a blockchain,
- Using this proof to verify identity without revealing the actual credentials.

The key advantage is secure, decentralized identity verification that eliminates the need for a centralized authority while protecting user privacy.

5.3 Description of the Patent:

The patent describes a system and method for creating, storing, and verifying digital identities on a blockchain platform. The process begins when identity data is received from a user device. The system then generates a data structure, such as a Merkle tree or similar hash-based structure, containing the identity attributes. A cryptographic hash is computed and written to the blockchain, ensuring that the original data remains confidential while still enabling third-party verification.

The invention allows for:

- Selective disclosure of identity attributes,
- Use of zero-knowledge proofs,
- A decentralized trust mechanism where multiple identity validators can corroborate the authenticity of claims.

Applications include secure user login, identity verification in financial services, e-voting, and KYC (Know Your Customer) compliance. The method increases data control for users, enhances interoperability across digital platforms, and minimizes risks of data breaches due to centralized databases.

6. TECHNICAL CONTENT ANALYSIS :

6.1 Objective of the Invention – What Problem Does It Solve?

The primary objective of this patent is to address the growing concerns around data security, centralized identity management, and the lack of user control in digital identity systems. Traditional identity verification frameworks rely heavily on centralized authorities, making them vulnerable to hacking, data breaches, and misuse of personal information. This invention aims to solve these issues by providing a secure, decentralized, and tamper-proof method for managing user identities using blockchain technology. It emphasizes user ownership of data and ensures that identity credentials are immutable, verifiable, and selectively shareable. By integrating smart contracts and distributed ledger principles, the system offers enhanced transparency and privacy.

6.2 Key Components / Method – Describe How It Works (Summarize Claims and Diagrams):

The patented invention employs a multi-layered architecture composed of the following core components:

- **Blockchain Ledger**: Serves as the immutable record for identity credentials and verification transactions.
- **Smart Contracts**: Automate identity creation, updates, and access permissions without third-party control.
- **Identity Hubs/Nodes**: Distributed nodes that hold encrypted identity data, retrievable via cryptographic keys.

- **User Agents (e.g., Wallets or Apps)**: Interfaces that allow users to create, manage, and share identity credentials.

Working Method (as derived from claims and diagrams):

- The system assigns a unique digital identity to a user, cryptographically signed and anchored on a blockchain.
- Smart contracts regulate who can view or modify identity attributes.
- Data is stored off-chain in encrypted formats, with on-chain pointers to ensure security and performance.
- Users grant selective disclosure access via encrypted tokens or keys, allowing privacy-preserving verifications.

Referenced Diagrams (from patent figures):

- Figures 1–3 depict the architecture of the decentralized identity system.
- Figures 4–5 illustrate the interaction between user agents, blockchain nodes, and third-party verifiers during credential verification and authentication.

6.3 Innovative Elements – What Makes It Novel Compared to Prior Art?:

Several innovations distinguish this patent from prior identity systems:

- **Selective Disclosure of Data**: Unlike traditional systems that reveal complete profiles, this system enables users to share only necessary attributes (e.g., age verification without revealing name or address).
- **Smart Contract-Based Access Control**: Ensures tamper-proof, programmable permissions over identity sharing.
- **Decentralized Identity Hubs**: Offer distributed, encrypted storage under user control rather than centralized databases.
- **Blockchain Anchoring of Credentials**: Verifiability and integrity are guaranteed through cryptographic hash anchoring on a distributed ledger.
- **Interoperability**: Designed to work across platforms and domains (e.g., banking, healthcare, government services).

These novel elements address long-standing concerns in identity systems such as data ownership, selective sharing, and cross-platform trust mechanisms.

6.4 Technical Field – Industry or Domain:

This invention belongs to the fintech, digital identity, blockchain, and cybersecurity domains. More specifically, it applies to:

- Digital Identity Verification and Management
- Decentralized Authentication Systems
- Smart Contract-Based Access Control
- Blockchain Technology for Secure Digital Transactions
- e-Governance, Healthcare, Banking, and IoT Identity Systems

7. DETAILED DESCRIPTION OF THE INVENTION :

The invention described in this patent outlines a system and method for managing digital identities in a decentralized, secure, and verifiable manner using blockchain technology. The focus of the system is to ensure a tamper-proof, user-centric identity management framework that minimizes reliance on centralized authorities and enhances personal data security through cryptographic methods.

Core Description and Functionality:

The invention employs a decentralized identity platform where digital identities are generated, authenticated, and verified using smart contracts and cryptographic hashes on a blockchain ledger. Users have full control over their identity attributes and can selectively disclose information to service providers. The system includes several main entities such as the **identity owner (user)**, **identity issuer**, and **identity verifier**, all interacting with smart contracts deployed on the blockchain.

- **Smart Contracts** govern the interactions between these entities, ensuring automatic enforcement of access rules, validation logic, and credential issuance.
- **Public and Private Keys** are used for authentication and signing transactions.

- The **blockchain ledger** serves as the immutable database for storing pointers to the hashed credentials rather than the actual personal data, ensuring compliance with data privacy laws.

Key Operations of the Invention:

1. **Registration**:
   - The identity owner registers with an identity issuer.
   - The issuer validates and signs the identity attributes, which are then hashed and linked to a blockchain entry.
2. **Authentication and Verification**:
   - The verifier requests specific credentials.
   - The identity owner selectively discloses verified attributes via digital proofs (e.g., zero-knowledge proofs or tokenized responses).
   - The smart contract checks the validity of the provided attributes against the blockchain entries.
3. **Revocation and Update Mechanisms**:
   - The issuer can revoke credentials by modifying a hash status or revocation registry stored on-chain.
   - Updates are done by issuing new records while maintaining historical integrity.

Security and Privacy Protections:

- **Zero-Knowledge Proofs (ZKPs)** are optionally used to prove possession of valid credentials without revealing actual data.
- **Access Control** via smart contracts allows for dynamic and conditional data sharing policies.
- **Hashing Algorithms** ensure data integrity and tamper resistance.

Illustrative Diagrams in the Patent:

- **Fig. 1**: Shows a high-level system architecture of digital identity creation and verification.
- **Fig. 2**: Depicts the interaction flow between identity owner, issuer, and verifier via blockchain.
- **Fig. 3–4**: Illustrate the credential issuance and selective disclosure process.

Advantages Outlined:

- Eliminates central authority dependency.
- Enhances data privacy and ownership for users.
- Enables scalable digital identity verification across sectors such as e-governance, banking, healthcare, and education.

This detailed implementation underscores the patent's potential to address global challenges related to identity fraud, privacy breaches, and inefficiencies in legacy identity management systems (Refer to the original patent at https://patents.google.com/patent/US10992478B2).

8. CLAIMS OF THE INVENTION :

The patent consists of a total of **20 claims**, including both **independent and dependent claims**, which collectively define the novelty and technical protection granted to the invention.

(1) Primary Claim (Independent Claim 1):

The central claim outlines a method for **controlling access to personally identifiable information (PII)** using a distributed ledger (i.e., blockchain). It involves:

- Receiving a request to access PII stored in a personal data store.
- Verifying the request based on access rules maintained in a smart contract stored on the blockchain.
- Granting or denying access based on the result of the verification process. This enables secure, permissioned, and decentralized control over personal identity information.

(2) Claims on Smart Contract Mechanism (Claims 2–5):

These dependent claims elaborate on how the smart contract:

- Is configured with **user-defined access rules**.
- May contain time-limited or role-based permissions.
- Can log all access requests and actions immutably.
- Ensures that only the user (data subject) can update or modify these rules using cryptographic signatures.

(3) Claims on Identity Verification and Encryption (Claims 6–10):

These claims focus on the process of:

- Identity validation using blockchain transaction metadata.
- End-to-end encryption of PII during storage and retrieval.
- Use of **zero-knowledge proofs** or **hash-based matching** to prevent full exposure of data while confirming authenticity.

(4) Claims on Selective Disclosure (Claims 11–15):

- The user can disclose **partial data attributes** (e.g., age or nationality) without sharing complete personal details.
- This supports scenarios such as age verification or KYC processes while maintaining privacy.
- The mechanism utilizes **user-consented disclosure tokens** stored securely on-chain.

(5) Claims on System Architecture (Claims 16–20):

- These claims define the system as a **decentralized identity management network** integrated with a blockchain.
- It includes components like:
  - Personal data vault
  - Blockchain ledger
  - Verifier interface
  - Identity provider nodes
- Claims highlight the system's adaptability across **government, healthcare, finance**, and **e-commerce** domains.

The claims reflect the invention's emphasis on **privacy, user control, decentralized governance, and immutability**. They also establish the **technical boundary** that protects the invention against replication by competitors.

9. CITATIONS & SIMILAR INVENTIONS :

9.1 Number of Citations in the Patent:

The patent **US10992478B2** cites **18 U.S. patents** and **6 non-patent literature references**, including publications related to blockchain identity, encryption methods, and decentralized authentication frameworks. These citations reflect the foundational technologies and prior art upon which this invention has been built. They include patents on distributed ledger technologies, smart contract protocols, and secure cryptographic authentication mechanisms.

9.2 Number of Citations for the Patent:

As of the latest data available from **Google Patents**, this patent has been **cited by at least 12 other patents** (based on USPTO citation tracking). These citations predominantly involve further innovations in:

- Decentralized identity platforms for e-government and healthcare
- Privacy-preserving blockchain protocols
- Smart contract-based identity verifications

This reflects the ongoing relevance and technological significance of the invention within the blockchain and digital identity innovation ecosystem.

9.3 List of Similar Inventions:

A selection of similar or related inventions (either cited by or citing this patent) includes in following table 2:

Table 2: Similar inventions

Patent Number	Title	Relevance
US10467834B2	Blockchain identity management system	Uses distributed ledgers for self-sovereign identity similar to US10992478
US10701392B2	Systems for secure identity verification using smart contracts	Incorporates secure, contract-governed credential sharing
US10176488B2	Decentralized trust protocol using blockchain	Relevant for its cryptographic trust modeling

Patent Number	Title	Relevance
US10902421B2	Selective data disclosure in identity systems	Technically similar in partial disclosure and privacy preservation
WO2020187360A1	Blockchain-based identity for healthcare	Extends the identity concept to medical records and authentication
EP3421354A1	Identity attestation using decentralized networks	Shows European landscape of similar innovation

These patents help position **US10992478B2** as a foundational document in the evolution of secure, user-controlled identity frameworks within blockchain infrastructure.

10. BASIC ANALYSIS :

10.1 Importance of the Invention:

This invention addresses critical challenges in digital identity management by offering a decentralized, secure, and privacy-preserving solution using blockchain technology. Traditional centralized identity systems are vulnerable to breaches, data misuse, and single points of failure. The patented method ensures that users have control over their identity data while maintaining verifiability and immutability. The system significantly enhances trust in digital interactions and has implications across sectors including fintech, e-governance, and healthcare. Its timing is crucial as global demands for secure digital identity systems are rising due to increased digitization and regulatory emphasis on data protection.

10.2 Description of the Invention:

The invention discloses a blockchain-based system for issuing, managing, and verifying digital identities. It uses cryptographic hashing, smart contracts, and distributed ledger technology to allow users to control access to their personal credentials. A unique feature of the system is *selective disclosure*, which allows users to share only necessary identity components with service providers. The identity data is not stored directly on-chain; instead, encrypted references and verifiable credentials are maintained to ensure privacy. The blockchain serves as a trust layer to verify the authenticity and integrity of claims made by or about the identity holder.

10.3 Design (Technology, Easiness, Cost, Reliability, Resource availability, Durability):

- **Technology**: Employs blockchain, smart contracts, and public-private key cryptography.
- **Easiness**: Designed for interoperability with existing ID frameworks; user-friendly authentication flows via mobile or web apps.
- **Cost**: Reduces long-term costs by eliminating the need for centralized ID infrastructure and reducing fraud risks.
- **Reliability**: The decentralized nature ensures high availability and fault tolerance.
- **Resource Availability**: Utilizes widely available blockchain platforms and standard cryptographic protocols.
- **Durability**: Blockchain immutability guarantees data consistency and tamper resistance over time.

10.4 New Innovations & Value Addition in the Patent:

- Introduces a novel mechanism for *user-consented identity sharing*, enhancing data sovereignty.
- Implements *decentralized trust anchors* via smart contracts, removing the need for centralized certification authorities.
- Supports *interoperability* across identity providers, making it suitable for global applications.
- Adds value by increasing transparency and auditability in digital identity processes.
- Offers extensibility to other blockchain applications like voting, licensing, and financial inclusion.

This patent represents a paradigm shift in how digital identity is conceptualized and secured. Its contributions extend beyond technological novelty to real-world societal impact, ensuring secure, ethical, and scalable identity ecosystems.

11. FUNCTIONAL ANALYSIS :

11.1 SWOC Analysis of the Patent:

SWOC analysis—a variant of the traditional SWOT framework that emphasizes **Challenges** instead of external threats—provides a structured way to evaluate an innovation or organization by examining internal strengths and weaknesses, as well as external opportunities and challenges. It serves as a foundational tool in strategic management and research-guided decision-making, enabling academics and practitioners to contextualize performance within both controllable and dynamic environmental dimensions (Puyt et al. (2023). [15]). While SWOT is widely adopted across business, technology, and public policy domains, SWOC specifically enhances its focus on complex, evolving external constraints such as regulatory shifts, socio-cultural resistance, and emerging technical uncertainties (Indrasaru et al. (2023). [16]. Recent methodological research highlights its value for exploratory case studies, allowing for granular mapping of innovation capabilities and risk factors—an approach frequently used in analyzing technology adoption, healthcare transformation, and organizational resilience (Aithal & Kumar (2015). [17]; Namugenyi et al. (2019). [18]). As a research instrument, SWOC helps scholars systematically align internal resource strengths with forward-looking scholarly insights into opportunity landscapes, while acknowledging real-world impediments to implementation and scaling (Benzaghta (2021). [19]; Aithal & Aithal (2023). [20]).

(i) Strengths of the Patent:

(1) **Decentralized Architecture**: The patent leverages blockchain's decentralized nature, reducing reliance on central authorities and enhancing system trust.
(2) **Secure Authentication**: It introduces cryptographic methods and smart contracts that ensure secure and immutable digital identity verification.
(3) **Selective Disclosure**: The invention allows users to control what personal information is shared, improving privacy and compliance with data protection regulations.
(4) **Scalability**: The design supports scalable identity management across different sectors like fintech, healthcare, and e-governance.
(5) **Compliance Compatibility**: The system aligns with emerging digital identity regulations such as GDPR and eIDAS.
(6) **Patent Citations and Recognition**: It has received multiple citations, indicating recognition and relevance in the field of digital identity and blockchain.

(ii) Weaknesses of the Patent:

(1) **High Implementation Complexity**: The system requires integration of multiple advanced technologies like blockchain, encryption, and smart contracts.
(2) **Limited Real-World Deployment**: As of now, widespread adoption across governments or enterprises is still emerging.
(3) **Dependency on Blockchain Infrastructure**: Effectiveness is tied to the maturity and adoption of blockchain networks.
(4) **Energy Consumption**: Blockchain-based systems, especially on public chains, may suffer from high energy usage, raising sustainability concerns.
(5) **User Education Barrier**: General users may find the technology difficult to understand or interact with effectively.
(6) **Interoperability Issues**: Compatibility with existing legacy systems and digital identity frameworks can be challenging.

(iii) Opportunities for the Patent:

(1) **Digital Government Platforms**: Growing interest in digital public infrastructure can accelerate adoption in national ID programs.
(2) **Cross-border Identity Verification**: Useful in solving issues around international KYC (Know Your Customer) and compliance.
(3) **Private Sector Adoption**: Financial institutions and healthcare providers are seeking secure identity systems.

(4) **Post-COVID Digital Expansion**: Remote identity verification is more relevant than ever due to digital transformation.
(5) **Collaborative Blockchain Networks**: Integration with consortium-based blockchains (like Hyperledger) can open enterprise opportunities.
(6) **Standardization Influence**: The patented model could shape international standards for decentralized digital identity.

(iv) Challenges of the Patent:

(1) **Regulatory Uncertainty**: Varying data privacy laws across jurisdictions may hinder implementation.
(2) **Blockchain Volatility**: Technological changes in blockchain protocols could affect system performance and compatibility.
(3) **Cybersecurity Threats**: Although secure by design, the system must remain resilient to evolving attack vectors.
(4) **Lack of Global Consensus**: No unified international standard for digital identity verification may slow down adoption.
(5) **Cost of Deployment**: Infrastructure development, especially for public blockchains, can be capital-intensive.
(6) **Trust Building**: Convincing institutions and citizens to move from traditional to blockchain-based identity systems is a long-term challenge.

11.2 ABCDEF Analysis of the Patent:

ABCDEF Analysis—an acronym for *Advantages, Benefits, Constraints, Disadvantages, Effectiveness, and Future financial value*—is an extension of ABCD analysis [21-30] and is a comprehensive framework used to evaluate the multi-dimensional impact of a patented innovation (Aithal & Aithal (2018). [31]). From a stakeholder's perspective, this method allows for a structured assessment of both the technical and strategic viability of the patent. It captures the tangible advantages and benefits offered to users, developers, and adopters, while also highlighting potential barriers such as technical constraints and operational disadvantages. The *effectiveness* dimension focuses on how well the invention performs in real-world scenarios, particularly in terms of scalability, reliability, and integration potential. Meanwhile, *future financial value* estimates the commercial prospects and monetization opportunities of the innovation across relevant sectors (Aithal & Aithal (2018), [32]). When applied to patents like those in blockchain-based digital identity, the ABCDEF framework equips researchers, investors, and policymakers with a holistic view of the patent's relevance, risks, and returns (Aithal & Aithal (2023). [33]; Aithal & Aithal (2019). [34]).

(i) Advantages of the patent from Stakeholders' Perception:

The Advantages of the patent on Blockchain-Based Digital Identity Management System from various Stakeholders' perception are listed in Table 3:

Table 3: Advantages of the patent from Stakeholders' Perception

S. No.	Key Advantages	Description
1	**Decentralization and Security**	The patent offers a decentralized identity system that significantly reduces the risk of data breaches by eliminating single points of failure, which is a major advantage for users and governments seeking secure ID frameworks.
2	**User-Controlled Privacy**	Through mechanisms like user-consented selective data disclosure and controlled credential sharing, stakeholders—especially individuals—gain more autonomy over their identity data.
3	**Regulatory Alignment**	The system is designed to align with global data protection laws (e.g., GDPR), which is advantageous for businesses and institutions aiming for international compliance in identity management.

4	**Cross-Sector Applicability**	The technology is adaptable across domains such as e-governance, digital banking, and healthcare, providing a scalable and interoperable solution for diverse stakeholder groups.
5	**Interoperability and Standardization**	The use of blockchain and smart contracts fosters interoperability across platforms, which is advantageous for ecosystem-wide adoption involving governments, enterprises, and developers.
6	**Enhanced Trust and Verification**	By using cryptographic hashing and immutable ledgers, the system increases trust in digital interactions, an advantage for both users and service providers relying on identity verification.

(ii) Benefits of the patent from Stakeholders' Perception for Realization:

The benefits of the patent on Blockchain-Based Digital Identity Management System from various Stakeholders' perception are listed in Table 4:

Table 4: Benefits of the patent from Stakeholders' Perception

S. No.	Key Benefits	Description
1	**Improved Identity Verification Efficiency**	The blockchain-based system automates and accelerates identity verification processes through smart contracts, saving time and reducing manual effort for institutions such as banks, government bodies, and healthcare providers.
2	**Reduction in Fraud and Identity Theft**	By leveraging immutable blockchain records and cryptographic mechanisms, the system minimizes the risk of identity fraud, offering a reliable benefit to consumers, fintech firms, and regulatory agencies.
3	**Cost Savings for Organizations**	Organizations that rely on KYC (Know Your Customer) and identity authentication can reduce infrastructure and operational costs through decentralized and reusable digital identities.
4	**Empowered End Users**	Individuals benefit from increased control over their personal data, allowing them to decide what information to share and with whom, thus enhancing transparency and digital dignity.
5	**Cross-Border Utility**	The digital identity system can be utilized internationally due to its decentralized nature, offering seamless benefits for global mobility, expatriates, and digital nomads, as well as multinational corporations.
6	**Enhanced User Trust and Customer Experience**	Businesses benefit from improved customer experience and loyalty, as users are more likely to trust platforms that implement secure and privacy-preserving identity solutions.

(iii) Constraints of the patent from Stakeholders' Perception for Realization:

The constraints of the patent on Blockchain-Based Digital Identity Management System from various Stakeholders' perception are listed in Table 5:

Table 5: Constraints of the patent from Stakeholders' Perception

S. No.	Key Constraints	Description
1	**Regulatory and Legal Compliance Issues**	Stakeholders may face difficulties aligning the patent's implementation with diverse and evolving data protection regulations (e.g., GDPR, CCPA), particularly in jurisdictions that are skeptical of decentralized systems.
2	**Technical Integration with Legacy Systems**	Many institutions and government bodies still operate on legacy infrastructure that may not easily integrate with blockchain-based digital identity platforms, creating a constraint in adoption.

3	**Interoperability and Standardization Gaps**	The lack of universal standards in digital identity architecture and blockchain protocols can hinder cross-platform compatibility, delaying stakeholder collaboration and scalability.
4	**High Initial Setup and Transition Costs**	Despite long-term cost benefits, the initial investment required for deploying and customizing this system could be a constraint for small- to mid-sized enterprises and government bodies with limited digital infrastructure.
5	**Blockchain Scalability Limitations**	Depending on the underlying blockchain used, issues such as transaction throughput, latency, and storage requirements may limit the system's performance under high-volume identity verification scenarios.
6	**Limited Public Awareness and Trust in Blockchain**	While the technology is promising, many end users and even organizational stakeholders may still lack awareness or confidence in blockchain's reliability for handling sensitive identity information, thus slowing down adoption.

(iv) Disadvantages of the Patent from Stakeholders' Perception for Realization:

The disadvantages of the patent on Blockchain-Based Digital Identity Management System from various Stakeholders' perception are listed in Table 6:

Table 6: Disadvantages of the patent from Stakeholders' Perception

S. No.	Key Disadvantages	Description
1	**Complexity in User Experience**	For non-technical users, managing private keys, digital wallets, and permissioned access can be confusing and overwhelming, limiting usability and acceptance.
2	**Irreversibility of Errors**	Blockchain's immutability means that any erroneous identity input or unauthorized change cannot be easily corrected, leading to long-term complications and potential legal disputes.
3	**Resource-Intensive Infrastructure**	Running a secure and scalable blockchain-based identity system may require high computational resources, especially if using public blockchain protocols, affecting energy efficiency and increasing operational costs.
4	**Dependency on Internet and Digital Access**	The patent's system is inherently reliant on stable internet access and digital devices, which may disadvantage populations in rural or underdeveloped regions with limited connectivity.
5	**Data Fragmentation Across Platforms**	Without proper integration standards or middleware, stakeholders may experience fragmented identity data across multiple blockchains or verification platforms, increasing operational inefficiency.
6	**Lack of Legal Recognition in Some Jurisdictions**	Many governments and regulatory bodies do not yet legally recognize blockchain-based identities, which can limit the patent's application in areas such as banking, e-voting, or immigration systems.

(v) Effectiveness of the patent from Stakeholders' Perception:

The effectiveness of the patent on Blockchain-Based Digital Identity Management System from various Stakeholders' perception are listed in Table 7:

Table 7: Effectiveness of the patent from Stakeholders' Perception

S. No.	Key Effectiveness	Description
1	**Enhanced Identity Authentication**	The patented system ensures highly effective identity authentication using cryptographic mechanisms and blockchain

		immutability, reducing identity fraud significantly for end-users and service providers.
2	**User-Controlled Data Privacy**	Through the principle of selective disclosure and decentralized storage, the invention empowers individuals to control their personal data, thus effectively addressing data privacy compliance under global frameworks like GDPR and HIPAA.
3	**Operational Scalability**	Stakeholders such as fintech companies and digital governance platforms benefit from the solution's scalability, as the patent outlines a design capable of handling increasing user volumes without compromising performance.
4	**Cross-Domain Adaptability**	The invention is effective across various domains—such as healthcare, banking, and e-governance—by offering a flexible framework for decentralized identity verification that aligns with diverse sectoral requirements.
5	**Tamper-Resistant Records**	The blockchain-based approach ensures permanent and tamper-evident records of identity transactions, enhancing stakeholders' trust in system security and auditability.
6	**Regulatory Alignment and Innovation**	The patent demonstrates effectiveness by embedding mechanisms compatible with ongoing regulatory developments in digital identity, fostering faster institutional adoption while ensuring legal robustness.

(vi) Future Financial Value of the Patent (Stakeholder Perspective):

The future financial value of the patent on Blockchain-Based Digital Identity Management System from various Stakeholders' perception are listed in Table 8:

Table 8: Future Financial Value of the patent from Stakeholders' Perception

S. No.	Key Future Financial Value	Description
1	**High Commercialization Potential**	The patent offers a scalable and secure identity solution applicable across fintech, healthcare, e-governance, and telecom sectors—each of which faces mounting identity verification costs. This versatility will allow for broad licensing opportunities and enterprise-level deployments, leading to substantial recurring revenue streams.
2	**Strategic Asset in Digital Identity Markets**	With global markets for digital identity expected to exceed **USD 70 billion by 2030**, this patent can serve as a foundational IP asset for startups and corporations developing decentralized identity platforms, significantly enhancing their valuation and investor attractiveness.
3	**Cost Reduction for Enterprises and Governments**	Adoption of this blockchain-based identity system can reduce administrative overhead and identity fraud-related losses. Governments and institutions may achieve multi-million-dollar savings through reduced document verification costs and fraud mitigation.
4	**Monetization via Blockchain-as-a-Service (BaaS)**	The patent can be integrated into commercial BaaS platforms, enabling monetization through APIs and SDKs offered to developers, SMEs, and public institutions needing secure digital identity protocols.
5	**Investment Magnet for Venture Capital**	Startups or enterprises leveraging this patent can attract increased venture capital and institutional investments due to its strong IP protection, technological novelty, and applicability in global identity compliance and KYC processes.

6	**Cross-Border Licensing and Royalty Streams**	The decentralized and interoperable nature of the invention allows it to be adapted globally, making it attractive for international partnerships and licensing agreements, ensuring long-term royalty-based financial gains.

11.3 Business Opportunities & Challenges:

(i) Business Opportunities in the Industry Environment:

(1) E-Governance and Digital Public Services:
The patent enables secure, decentralized identity management, which governments can leverage to issue tamper-proof digital IDs, voter credentials, or health records, promoting transparency and reducing fraud in public services.

(2) Fintech & Banking Applications:
With rising demand for secure KYC/AML processes, the invention supports compliant identity verification without centralized storage, reducing operational costs and risk in banking and financial sectors.

(3) Healthcare Identity Management:
The system facilitates encrypted patient data sharing and access control across providers, useful in healthcare systems moving towards interoperable and privacy-focused digital health records.

(4) Decentralized Applications (dApps):
Blockchain identity is a foundational layer for Web3 and dApps where users retain control over their credentials, supporting future business models in decentralized finance (DeFi), insurance, and reputation systems.

(5) Cross-border Authentication and Travel:
The invention can support border control, immigration, and international identification use-cases with its cryptographically verifiable identity tokens, which are particularly suited to passport digitization efforts.

(6) B2B Identity & Enterprise Access Management:
Enterprises managing global workforces and vendor networks can adopt the solution to streamline secure access control without relying on centralized systems or traditional passwords.

(ii) Challenges in the Competitive Environment:

(1) Adoption Resistance and Regulatory Uncertainty:
Despite technical robustness, many jurisdictions have not yet approved blockchain identities for official use. Regulatory clarity is still evolving, creating uncertainty for full-scale deployment.

(2) Competing Patent Portfolios from Tech Giants:
Major players like Microsoft, IBM, and ConsenSys also hold patents in blockchain identity space, creating a high-stakes competitive landscape and potential for IP conflicts or infringement disputes.

(3) Interoperability with Legacy Systems:
Many industries still rely on legacy identity systems (e.g., LDAP, OAuth), and integrating decentralized identity solutions with them poses technical and cost barriers.

(4) Scalability and Network Dependence:
Blockchain networks vary in performance and cost. If the patent depends on public chains like Ethereum, transaction fees and network congestion could hinder adoption.

(5) Security Threats from Evolving Technologies:
While blockchain is considered secure today, advances in quantum computing or sophisticated cyber-attacks may render existing encryption methods vulnerable in the future.

(6) User Onboarding and Experience:
End-users unfamiliar with public/private key management may find the technology intimidating, posing a barrier to mass adoption unless intuitive UX solutions are layered on top.

These insights reflect both the **strategic market entry points** and **barriers to commercialization** of the patented invention in the real-world technology ecosystem.

11.3 Market and Business Value Estimation:

(1) Commercial Applications:
This patent outlines a decentralized, blockchain-based identity authentication and access management system that can be applied across various sectors:

- **E-Governance:** Digital identity for voting, tax filings, and citizen services.
- **Fintech & Banking:** Secure KYC processes, customer onboarding, and transaction authentication.
- **Healthcare:** Protecting patient records and enabling consent-based data sharing.
- **Education:** Digital certificates and identity verification for student and academic records.
- **E-commerce & IoT:** Secure user/device identity validation in online transactions and smart device networks.

(2) Current Implementations:
While the patent itself does not directly refer to specific implementations, similar principles are already being adopted by organizations such as:

- **Sovrin Foundation** and **uPort** in decentralized identity management,
- **Microsoft's ION project** on Bitcoin's blockchain,
- **Hyperledger Indy** for self-sovereign identity.

This suggests the patented method is aligned with industry direction and can be integrated into existing solutions.

(3) Competitor Landscape:
The space of blockchain-based identity systems is highly active. Key competitors include:

- **IBM Blockchain Identity**, **Civic Technologies**, and **ShoCard**, all working on decentralized identity platforms.
- Multiple startups and blockchain consortia (like **Evernym**, **SelfKey**, and **Jolocom**) have released products with overlapping capabilities, indicating market competition and validation.

(4) Licensing Potential:
The patent has a strong **licensing potential** due to:

- **Cross-sector applicability**, attracting partners in healthcare, finance, government, and IoT sectors.
- Possibility to license to **governments** and **regulatory agencies** for national ID initiatives or to **tech providers** building digital ID frameworks.
- Integration into **open-source consortiums** like Hyperledger, with proprietary extensions covered under licensing.

(5) Market Trends:
The market for decentralized digital identity is on the rise:

- **Gartner** predicts over 1 billion people will have a decentralized identity system by 2026.
- The **global digital identity solutions market** is expected to grow at a CAGR of over 16.2%, reaching **USD 70+ billion by 2030**.
- Factors like increasing **cybersecurity threats**, **regulatory compliance (e.g., GDPR, eIDAS)**, and the **shift to Web3 and metaverse platforms** are accelerating adoption.

This patent thus holds high business value, both in terms of its applicability across high-growth sectors and its strategic importance in a digital future reliant on decentralized trust frameworks.

12. SUGGESTIONS :

12.1 Suggestions for Implementation:

(1) Integration into Government e-Services: Implement the system in national e-governance platforms to provide citizens with decentralized identity credentials for public service access (e.g., e-voting, taxation, digital IDs).

(2) Partnership with Financial Institutions: Collaborate with banks and fintech firms to embed the decentralized identity system into Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance workflows, enhancing security and reducing costs.

(3) Layered Access Models: Create user permission layers using smart contracts for different sectors—such as healthcare, education, and insurance—allowing selective disclosure of personal data, as envisioned in the patent.

(4) API and SDK Development: Design open-source APIs and Software Development Kits (SDKs) to enable third-party developers to build interoperable services and wallets using the patented identity system.

(5) Pilot in Cross-Border Applications: Test the blockchain-based ID system for international travel and immigration documentation (like e-passports) to establish a global digital identity standard.

(6) Compliance with Global Standards: Ensure that deployment adheres to standards like W3C Decentralized Identifiers (DIDs), GDPR, and ISO/IEC 24760, promoting scalability and global trust.

12.2 Suggestions for Related New Ideas & Patents:

(1) Decentralized Biometric Authentication Protocol: Build upon the core identity framework to propose a system that combines blockchain with zero-knowledge proofs for biometric verification without revealing actual biometric data.
(2) Blockchain-based Digital Death Certificate System: Create a patent that extends identity lifecycle management, enabling secure and tamper-proof documentation of death records to prevent misuse of deceased identities.
(3) Self-Sovereign Identity for IoT Devices: Introduce a system where each IoT device is assigned a unique digital identity stored on blockchain, managed using principles similar to human identity frameworks.
(4) AI-based Risk Scoring Engine for Identity Fraud: Propose a machine learning module integrated into the blockchain identity system to evaluate trust scores and detect abnormal behavior or fraud in identity usage.
(5) Cross-Chain Interoperable Digital Identity Ledger: Design a blockchain identity protocol that supports identity credentials across multiple blockchain networks like Ethereum, Hyperledger, and Solana.
(6) Identity Recovery System with Multi-Signature Verification: File a patent for a secure identity recovery method that uses multi-party authorization (e.g., family + notary) without relying on centralized authorities.

13. CONCLUSION & RECOMMENDATION :

The patent analysis of US10992478 on "Blockchain-based Digital Identity" highlights its transformative potential in securing and decentralizing personal data management. By leveraging blockchain, cryptographic hashing, and smart contracts, the invention addresses critical vulnerabilities of traditional identity systems, such as centralized control, identity theft, and data breaches. Its application across domains like e-governance, fintech, healthcare, and digital authentication frameworks showcases not just technological robustness but societal relevance as well. The patent's architecture enables user-controlled access, selective disclosure, and immutable audit trails, offering a reliable solution to privacy challenges in today's digital ecosystem.
Based on the insights drawn from the technical design, market outlook, and stakeholder-focused analyses (SWOC and ABCDEF), it is recommended that the patent be commercialized through strategic partnerships with government and financial institutions. Future research should explore the integration of biometric authentication, zero-knowledge proofs, and AI-driven anomaly detection to enhance adaptability. Moreover, continuous updates to comply with evolving global digital identity regulations will ensure scalability and legal durability. Encouraging open innovation ecosystems through licensing or modular adoption could further extend its impact, making this patent a foundational piece in shaping a decentralized, secure, and inclusive digital identity landscape.

REFERENCES :

[1] Griliches, Z. (1990). Patent statistics as economic indicators: A survey. *Journal of Economic Literature*, 28(4), 1661–1707. https://doi.org/10.3386/w3301. Google Scholar↗

[2] Ernst, H. (2003). Patent information for strategic technology management. *World Patent Information*, 25(3), 233–242. Google Scholar↗

[3] Narin, F., Hamilton, K. S., & Olivastro, D. (1997). The increasing linkage between U.S. technology and public science. *Research Policy*, 26(3), 317–330. Google Scholar↗

[4] Breschi, S., Lissoni, F., & Malerba, F. (2003). Knowledge-relatedness in firm technological diversification. *Research Policy*, 32(1), 69–87. Google Scholar↗

[5] Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. *IEEE Security and Privacy Workshops*, 180–184. Google Scholar↗

[6] Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, 30, 9–29. Google Scholar↗

[7] Jacobovitz, O. (2016). Blockchain for Identity Management. *Berkeley ISchool Report*. Retrieved from https://ischool.berkeley.edu/research/publications/2016/blockchain-identity-management.

[8] Allen, C. (2016). *The Path to Self-Sovereign Identity*. Retrieved from https://www.coindesk.com/tech/2016/04/19/the-path-to-self-sovereign-identity.

[9] WIPO (2020). *Technology Trends 2020: Artificial Intelligence*. Geneva: World Intellectual Property Organization. https://www.wipo.int/publications/en/details.jsp?id=4386.

[10] Leydesdorff, L. (2008). Patent classifications as indicators of intellectual organization. *Journal of the American Society for Information Science and Technology*, 59(10), 1582–1597. Google Scholar↗

[11] Aithal, P. S., & Aithal, S. (2018). Patent analysis as a new scholarly research method. *International Journal of Case Studies in Business, IT, and Education (IJCSBE), 2*(2), 33-47. Google Scholar↗

[12] Aithal, P. S., & Aithal, S. (2023). Introducing systematic patent analysis as an innovative pedagogy tool/experiential learning project in HE Institutes and Universities to boost awareness of patent-based IPR. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, *8*(3), 395-413. Google Scholar↗

[13] Aithal, P. S., & Aithal, S. (2018, August). A New Method of Scholarly Research–Patent Analysis. In *Proceedings of Conference-Exploring Avenues in Banking, Management, IT, Education & Social Sciences* (pp. 69-83). Google Scholar↗

[14] Aithal, S., & Aithal, P. S. (2019). How to Customize Higher Education at UG & PG levels using Patent Analysis & Company Analysis As New Research Methods in Technology, Health Sciences & Management Education. *Health Sciences & Management Education (January 30, 2019). In Information Technology and Education, Challenges and Opportunities of Smarter Learning Systems, New Delhi Publishers, India*, 25-59. Google Scholar↗

[15] Puyt, R. W., Lie, F. B., De Graaf, F. J., & Wilderom, C. P. M. (2023). From SOFT approach to SWOT analysis: A historical reconstruction. *Journal of Management History*, 31(2), 333–347. Google Scholar↗

[16] Indrasaru, M., Abdel-Razik, H. R., & Nasr, M. (2023). Shifting from SWOT to SWOC: A combination of strategic analysis and financial strategies. *Jurnal Ilmiah Akuntansi*, 6(1), 36–52. Google Scholar↗

[17] Aithal, P. S., & Kumar, P. M. (2015). Applying SWOC analysis to an institution of higher education. *International Journal of Management, IT and Engineering*, *5*(7), 231-247. Google Scholar↗

[18] Namugenyi, C., & Others. (2019). Design of a SWOT analysis model and its evaluation in strategic decision-making. *Procedia Computer Science*, 165, 233–239. Google Scholar↗

[19] Benzaghta, M. A., Elwalda, A., Mousa, M. M., Erkan, I., & Rahman, M. (2021). SWOT analysis applications: An integrative literature review. *Journal of Global Business Insights*, *6*(1), 54-72. Google Scholar↗

[20] Aithal, P. S., & Aithal, S. (2023). Incubationship–A Systematic Analysis of Recently Announced Super Innovation in Higher Education using SWOC, ABCD, and PESTL Frameworks. *International Journal of Case Studies in Business, IT, and Education (IJCSBE)*, *7*(4), 48-90. Google Scholar↗

[21] Aithal, P. S., Shailashree, V., & Kumar, P. M. (2015). A new ABCD technique to analyze business models & concepts. *International Journal of Management, IT and Engineering*, *5*(4), 409-423. Google Scholar↗

[22] Aithal, P. S. (2016). Study on ABCD analysis technique for business models, business strategies, operating concepts & business systems. *International Journal in Management and Social Science*, *4*(1), 95-115. Google Scholar↗

[23] Aithal, P. S. (2017). ABCD Analysis as Research Methodology in Company Case Studies. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, *2*(2), 40-54. Google Scholar↗

[24] Aithal, P. S., Shailashree, V., & Kumar, P. M. (2015). Application of ABCD Analysis Model for Black Ocean Strategy. *International journal of applied research*, *1*(10), 331-337. Google Scholar↗

[25] Aithal, A., & Aithal, P. S. (2017). ABCD analysis of task shifting–an optimum alternative solution to professional healthcare personnel shortage. *International Journal of Health Sciences and Pharmacy (IJHSP)*, *1*(2), 36-51. Google Scholar↗

[26] Aithal, S., & Aithal, P. S. (2016). ABCD analysis of Dye-doped Polymers for Photonic Applications. *IRA-International Journal of Applied Sciences*, *4*(3), 358-378. Google Scholar↗

[27] Raj, K., & Aithal, P. S. (2018). Generating Wealth at the Base of the Pyramid–a Study Using ABCD Analysis Technique. *International Journal of Computational Research and Development (IJCRD)*, *3*(1), 68-76. Google Scholar↗

[28] Aithal, P. S., Shailashree, V., & Kumar, P. M. (2016). The study of the new national institutional ranking system using ABCD framework. *International Journal of Current Research and Modern Education (IJCRME)*, *1*(1), 389-402. Google Scholar↗

[29] Shenoy, V., & Aithal, P. S. (2016). ABCD Analysis of Online Campus Placement Model. *IRA-International Journal of Management & Social Sciences*, *5*(2), 227-244. Google Scholar↗

[30] Kumari, P., & Aithal, P. S. (2020). Growth & Fate Analysis of Mangalore International Airport–A Case Study. *International Journal of Case Studies in Business, IT, and Education (IJCSBE)*, *4*(2), 71-85. Google Scholar↗

[31] Aithal, P. S., & Aithal, S. (2018). Patent analysis as a new scholarly research method. *International Journal of Case Studies in Business, IT, and Education (IJCSBE), (2018)*, *2*(2), 33-47. Google Scholar↗

[32] Aithal, P. S., & Aithal, S. (2018, August). A New Method of Scholarly Research–Patent Analysis. In *Proceedings of Conference-Exploring Avenues in Banking, Management, IT, Education & Social Sciences* (pp. 69-83). Google Scholar↗

[33] Aithal, P. S., & Aithal, S. (2023). Introducing systematic patent analysis as an innovative pedagogy tool/experiential learning project in HE Institutes and Universities to boost awareness of patent-based IPR. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, *8*(3), 395-413. Google Scholar↗

[34] Aithal, S., & Aithal, P. S. (2019). How to Customize Higher Education at UG & PG levels using Patent Analysis & Company Analysis as New Research Methods in Technology, Health Sciences & Management Education. *Health Sciences & Management Education (January 30, 2019). In Information Technology and Education, Challenges and Opportunities of Smarter Learning Systems, New Delhi Publishers, India*, 25-59. Google Scholar↗

[35] Aithal, P. S., & Aithal, S. (2023). New Research Models under the Exploratory Research Method. A *Book "Emergence and Research in Interdisciplinary Management and Information Technology" edited by P. K. Paul et al. Published by New Delhi Publishers, New Delhi, India*, 109-140. Google Scholar↗

****