Digital Twins and Blockchain Fusion for Security in Metaverse-Driven Consumer Supply Chains

Pushpita Chatterjee, *Senior Member, IEEE*, Debashis Das, *Graduate Student Member, IEEE*, Danda B. Rawat, *Senior Member, IEEE*, Uttam Ghosh, *Senior Member, IEEE*, Sourav Banerjee, *Senior Member, IEEE*, and Mohammed S. Al-Numay, *Senior Member, IEEE*

***Abstract*—In the rapidly growing consumer electronics industry, continuous innovation drives increasing demand for smart devices and advanced gadgets. However, this sector faces changing demands and complex supply chains due to the management of rapid technological advancements and consumer expectations. Seamless communication between suppliers and consumers is essential to optimize production processes, minimize waste, and enhance overall customer satisfaction. In response to these demands, this paper presents a solution that combines Digital Twins (DT) and blockchain to improve security and efficiency in metaverse-inspired consumer-oriented supply chains. Herein, DT is used to represent products in virtual spaces and blockchain secures sensitive information using encryption and access controls. Our objective is to create a transparent, secure, and user-friendly system where consumers and suppliers can interact in real-time to verify product details and access important information of featured tasks like warranties and payment settlement. Smart contracts automates these tasks to make processes faster and more reliable. Through experiments, we tested how well the system maintains product integrity, authenticates transactions, and supports consumer-oriented supply chain (CSC) operations. Comparative analysis shows that our approach improves security, performance, and scalability over existing methods. Furthermore, the proposed system not only enhances security, trust, and transparency in CSC but also sets a higher standard for consumer demands and satisfaction. The findings point to the potential solution for future innovations in metaverse-driven CSC management systems.**

***Index Terms*—Blockchain, digital twins, metaverse, security, data integrity, supply chain.**

Received 19 August 2024; revised 3 October 2024; accepted 7 October 2024. Date of publication 9 October 2024; date of current version 11 December 2024. This work was supported by the National Science Foundation under Award 2401928. The work of Mohammed S. Al-Numay was supported by the Researchers Supporting Project, King Saud University, Riyadh, Saudi Arabia, under Grant RSP2024R150. The work of Danda B. Rawat was supported by MasterCard Research Impact Funds and DoD Center of Excellence in AI and Machine Learning (CoE-AIML) at Howard University with the U.S. Army Research Laboratory under Grant W911NF-20-2-0277. *(Corresponding author: Debashis Das.)*

Pushpita Chatterjee, Debashis Das, and Uttam Ghosh are with the Department of Computer Science and Data Science, Meharry Medical College, Nashville, TN 37208 USA (e-mail: pushpita.c@ieee.org; debashis.das@ieee.org; ghosh.uttam@ieee.org).

Danda B. Rawat is with the Department of Electrical Engineering and Computer Science, Howard University, Washington, DC 20059 USA (e-mail: db.rawat@ieee.org).

Sourav Banerjee is with the Department of Computer Science and Engineering, Kalyani Government Engineering College, Kalyani 741235, India (e-mail: mr.sourav.banerjee@ieee.org).

Mohammed S. Al-Numay is with the Department of Electrical Engineering and Computer Science, King Saud University, Riyadh 11451, Saudi Arabia (e-mail: alnumay@ksu.edu.sa).

Digital Object Identifier 10.1109/TCE.2024.3477297

I. Introduction

OVER the years, the consumer-oriented industry has undergone a remarkable evolution with rapid advancements in technology for changing consumer demands and an ever-accelerating pace of innovation [1]. Consumer electronics have become an integral part of modern life including a wide range of devices such as smartphones, smart home systems, wearable technology, and connected appliances. This industry's dynamism is driven by its unwavering commitment to improve product quality, increase innovation, and adapt to emerging trends. In recent times, the sector has witnessed a significant shift towards the metaverse, a virtual shared space that combines aspects of augmented reality (AR), virtual reality (VR), and the Internet [2]. The metaverse represents a convergence of virtual and physical realities, where Digital Twins (DT) [3] of consumer devices interact seamlessly within immersive environments. In this context, CSC must be able to operate fluidly across both virtual and physical spaces for the integrity, traceability, and security of data [4]. However, existing CSC systems are often centralized and vulnerable to data tampering, inefficiencies, and security breaches [5]. Therefore, deploying consumer electronics in such a metaverse environment demands a new approach to CSC management systems.

As the demand for smart and interconnected consumer products grows, CSC systems managing these products are under increasing pressure to ensure security, efficiency, and scalability. CSC face challenges related to data integrity, transparency, and real-time monitoring [6]. Traditional CSC models are often inadequate to meet the demands of highly automated, data-intensive environments, risks of data tampering, and limited visibility [7]. In addition, the emergence of the metaverse and its convergence with consumer electronics introduces new complexities, where devices must interact seamlessly across virtual and physical realms.

To address these challenges, the combination of DT and blockchain provides an innovative solution [8]. DT creates real-time digital replicas of physical consumer devices and enables continuous monitoring, predictive maintenance, and lifecycle management. On the other hand, blockchain ensures data security, traceability, and reliable access control [9]. These combined technologies can transform CSC operations for consumer electronics to enhance resilience, reduce risks, and deliver superior consumer experiences [8]. The deployment of

1558-4127 © 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: TRINITY COLLEGE LIBRARY DUBLIN. Downloaded on August 26,2025 at 10:24:37 UTC from IEEE Xplore. Restrictions apply.

this hybrid system in the metaverse involves integrating DT of consumer electronics into virtual environments where they can be monitored and managed in real-time. Smart contracts ($\mathcal{SC}_s$) automate processes like warranty management, payment settlements, and data validation within these environments [10]. For example, when a consumer interacts with a smart device within the metaverse, DT reflects its status in real-time, while the blockchain ensures secure, traceable transactions and records. This integration not only enhances security but also supports advanced scenarios like predictive analytics and autonomous device management.

Therefore, we propose an approach to integrate DT and blockchain to enhance security within metaverse-inspired CSC. The proposed system addresses key challenges such as tamper resistance, real-time monitoring, and decentralized access control for the future of consumer electronics in the metaverse. Therefore, we analyze the advantages of this approach using several critical metrics such as risk factors, real-time monitoring, transaction and execution costs, and latency. The experimental setup demonstrates the feasibility of deploying this integrated solution to provide consumer electronics in the metaverse and beyond. The main contributions of the paper are given below:

- A combined approach is proposed using DT and blockchain for a metaverse-driven CSC.
- Encryption techniques, access controls, and privacy protocols are implemented to maintain data integrity throughout the CSC management.
- An efficient communication and interaction model is designed to engage users with DT and authenticate products between various stakeholders in CSC management.
- The proposed framework automates key processes such as payment settlements, warranty management, and data validation through $\mathcal{SC}_s$.
- Performance of the proposed approach is experimentally validated using metrics such as risk factor, transaction cost, execution cost, and latency in complex CSC scenarios.
- Finally, a detailed comparative analysis of the proposed approach against traditional, blockchain-only, and DT-only solutions is presented and analyzed with its performance across multiple security and efficiency metrics.

The remainder of this paper is structured as follows: Section II provides a literature review and discusses the concepts of DT and blockchain along with their implications for CSC management. Overview and methodology of the proposed system are outlined and explained in Section III. Section IV presents the experimental results and analysis of the proposed system. Finally, Section V concludes the paper and outlines future directions.

II. Background and Literature Review

A. Digital Twins: Fundamentals and Applications

Digital Twins (DT) represent a powerful concept that has transcended its origins in manufacturing and emerged as a transformative force across diverse industries [11]. This virtual representation is not static, it continuously collects real-time data from its physical counterpart by facilitating monitoring, analysis, and simulation [12]. In the consumer electronics sectors, DT enables designers and engineers to create virtual prototypes of products. They can simulate how a product will behave under various conditions and make necessary design adjustments early in the development process. DT helps monitor the condition of consumer-oriented devices in real-time. By analyzing sensor data, they can predict when maintenance or repairs are required [13]. DT allows manufacturers to create virtual versions of products that users can customize to their preferences. Reputed smartphone manufacturers employ DT to simulate and optimize device performance, such as battery life, thermal management, and camera functionality [14]. The integration of DT in consumer electronics not only enhances user experiences and product quality but also informs strategic decisions in the market. This leads to improved user experiences and product quality. Companies producing wearables like smartwatches and fitness trackers utilize DT to model user interactions and test various scenarios. This approach assists in refining product designs and enhancing sensor accuracy. In the realm of smart home devices, DT plays a role in simulating user interactions and ensuring seamless integration with other IoT devices. In parallel, effective stock ranking is crucial for investment strategies in the consumer electronics sector [15]. The Time-Aware Balanced multi-view Learning (TABLE) method [16] can improve stock ranking by using multiple data sources such as price and social media sentiment. The results show that TABLE performs better than existing methods and is a valuable tool for consumer electronics companies to optimize their investment strategies and make better stock trading decisions.

To optimize data transmission and minimize energy consumption, manufacturing factories are deploying servers at the edge of the network to cache services. However, due to the dynamic nature of edge networks and the unpredictability of service requests, the optimal caching strategy for IoT devices remains a significant challenge. Authors [17] addressed this issue by employing DT to create dynamic digital models of IoT devices and edge servers. They proposed a service caching scheme called SCRD, which utilizes deep reinforcement learning (DRL) enabled by DT to derive optimal caching strategies for IoT devices. However, there are scalability concerns as the number of IoT devices increases to manage dynamic digital models and caching strategies. The development of smart cities is increasingly facilitated by consumer electronics-grade DT. The authors in [18] have shown the integration of sophisticated AI algorithms for network security and threat detection effectively mitigates potential network attacks and data breaches for the safety and reliability of DT systems. However, the implementation of AI-driven digital twins may involve significant complexity and resource requirements.

B. Blockchain in CSC

Blockchain is a distributed ledger system that underpins cryptocurrencies like Bitcoin but extends its utility far beyond digital currencies [8]. At its core, a blockchain is a chain

Authorized licensed use limited to: TRINITY COLLEGE LIBRARY DUBLIN. Downloaded on August 26,2025 at 10:24:37 UTC from IEEE Xplore. Restrictions apply.

of blocks, each containing a list of transactions or data records. These blocks are linked together in a chronological and immutable sequence [19]. Consumer electronics are often targeted by counterfeiters. Blockchain enables the creation of a digital fingerprint for each genuine product. This reduces the circulation of counterfeit goods. Companies in the consumer-oriented sector can utilize blockchain to gain end-to-end visibility into their CSC [20]. They can track the movement of components and finished products across multiple suppliers, manufacturers, and distributors in real-time. If a component or product fails quality standards, it can be flagged, and its journey through the CSC can be traced back to identify the source of the issue. Blockchain can also streamline warranty management by recording product information and warranty details on an immutable ledger. In a recall, companies can quickly identify affected products and notify customers.

Numerous schemes have been developed using blockchain, Mobile Edge Computing (MEC), and consumer electronic devices for efficient Electronic Medical Record (EMR) exchange. However, these schemes face critical challenges, including data security, automation, and scalability. Authors in [21] proposed a novel blockchain-based EMR sharing scheme to safeguard the Health Information Exchange (HIE) process between patients and doctors. The proposed scheme employs advanced security techniques encryption method and digital signatures along with the Inter-Planetary File System (IPFS) for secure storage of EMRs. However, it still faces limitations related to implementation complexity and potential integration challenges with existing healthcare systems. Another study [22] investigated the synergistic integration of blockchain with 6G networks to create secure and decentralized connectivity specifically designed for consumer electronics. A multi-party, dependable framework was proposed that includes intelligent edge servers, blockchain consensus mechanisms, and resource-constrained electronic devices. However, resource-constrained electronic devices may struggle to handle the computational demands of blockchain transactions and consensus mechanisms. These limitations need to be addressed to realize the full potential of 6G communication and consumer electronics.

C. The Metaverse Era and Its Implications

The metaverse is a concept that has gained significant traction in recent years and represents a convergence of digital technologies and virtual experiences. It can be defined as a collective virtual shared space by merging AR, VR, and the Internet into an interconnected environment [23]. In the metaverse, individuals can interact with each other and digital objects. It is not limited to a single platform or technology but encompasses a spectrum of digital experiences and spaces. Fig. 1 shows the advent of the metaverse is fundamentally reshaping consumer behavior and expectations using DT. Consumers expect highly personalized experiences within the metaverse. They anticipate products and services tailored to their preferences, and DT plays a pivotal role in delivering this personalization. Furthermore, DT enables more customized & immersive interactions and experiences that align with individual consumer needs by creating real-time and dynamic virtual replicas of physical products.

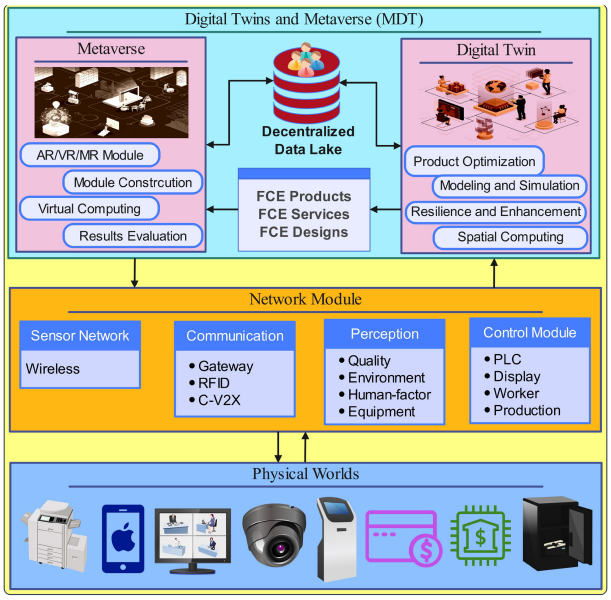


Fig. 1. Digital-twin and metaverse linked with blockchain for consumer-oriented products.

D. DT and Blockchain in CSC

Case Study 1: DT and blockchain have reshaped the consumer-oriented industry by providing innovative solutions to long-standing challenges. Leading consumer-oriented manufacturers faced challenges in managing their complex CSC [24]. Delays, quality issues, and inefficiencies were common. Therefore, they implemented DT in its entire CSC. Each component, product, and logistics node was represented in a digital twin. Sensors and IoT devices were integrated to capture real-time data on inventory levels, shipment status, and product condition.

Case Study 2: A manufacturer of high-end smartphones faced significant challenges with counterfeit products entering the market [25]. This not only impacted revenues but also eroded customer trust. The company implemented DT for each smartphone model. The digital twin contained detailed specifications and unique identifiers linked to the physical product. Customers could verify product authenticity by scanning a QR code on the product, which is linked to the digital twin.

Case Study 3: A consumer electronics retailer faced challenges in verifying the authenticity of products it sourced from various suppliers, which resulted in product returns and customer dissatisfaction [26]. The retailer implemented a blockchain-based product authentication system. Each product's manufacturing and distribution data were recorded on the blockchain, accessible via a QR code on the product. Customers appreciated the transparent authentication process. And, Suppliers were held accountable for the authenticity of their products.

E. DT and Blockchain Within the Metaverse

The metaverse era has brought about a profound transformation in the consumer-oriented industry. DT can

Authorized licensed use limited to: TRINITY COLLEGE LIBRARY DUBLIN. Downloaded on August 26,2025 at 10:24:37 UTC from IEEE Xplore. Restrictions apply.

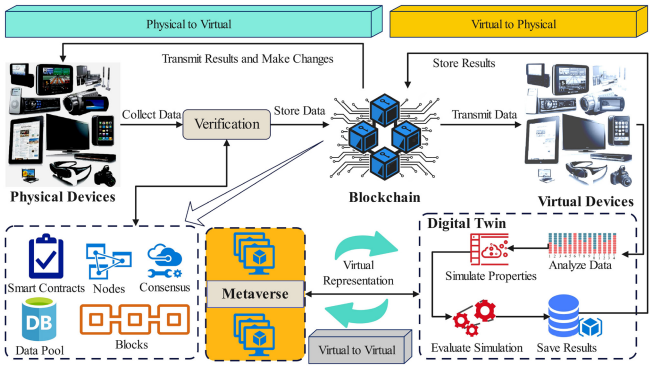


Fig. 2. Proposed system model.

create virtual replicas of consumer-oriented products within the metaverse that allow users to interact with them before making a purchase decision [11]. On the other hand, blockchain can secure ownership records of these virtual products, which enables users to verify authenticity and provenance. Users can customize these virtual products and preferences, which can be stored on a blockchain for future interactions. Blockchain records can verify the authenticity and quality of virtual representations of products within the metaverse [27]. DT can simulate user interactions and collect data on preferences and behavior within the metaverse. DT and blockchain can facilitate the seamless transfer of virtual assets and identities across different metaverse environments. This integration is facilitated by technologies such as blockchain, which has become a cornerstone for secure and transparent financial transactions related to consumer electronics. Consumer electronics are increasingly used for digital payments and transactions within the metaverse [28]. Smartphones serve as digital wallets for users to make purchases, conduct financial transactions, and interact with virtual currencies seamlessly. With the metaverse blurring the lines between physical and digital assets, consumer electronics enables users to own and manage virtual assets [29]. Blockchain's transparent CSC records can facilitate it financing for consumer-oriented manufacturers.

III. System Overview and Methodology

A. System Model

The proposed system model integrates DT, sensors, analytics, blockchain, and ($\mathcal{SC}_s$) to optimize CSC processes for consumer-oriented applications. Fig. 2 shows the proposed system model. These technologies work together to create a robust system that enhances transparency, traceability, and security throughout for CSC management system. Each component of the proposed system is defined and described their roles below:

Physical Entity: This component represents the tangible consumer-oriented device, and it plays a foundational role in the entire system. The physical entity serves as the anchor for the digital twin, which is a virtual representation of it. The physical attributes of the device, such as its hardware specifications, components, and physical condition, are recorded and monitored in real-time. For instance, if it's a smartphone, data can include details about its processor, storage, battery status, and even physical damage or wear.

Virtual Model: The digital twin's virtual model is a detailed and dynamic 3D or 2D representation of the physical entity. It encapsulates every aspect of the device, including its physical structure, components, firmware, and relevant attributes. This model is updated continuously and in real-time based on the data collected from sensors embedded within the physical entity.

Sensor Integration: Sensors embedded within the consumer-oriented device serve as the eyes and ears of the digital twin. These sensors continuously collect data on various aspects of the device, including its state, performance, usage patterns, and environmental conditions. For instance, sensors can monitor temperature, battery voltage, screen usage, GPS location, and more, providing a comprehensive view of the device's behavior and surroundings.

Blockchain Network: The blockchain network is a fundamental element of the system's infrastructure. It serves as a distributed ledger that records critical data related to consumer-oriented devices as they move through the CSC. The choice of blockchain network can vary, depending on factors such as security requirements and the need for transparency. We choose a private blockchain that may restrict access to authorized participants. This blockchain ledger provides an immutable and tamper-proof record of the device's journey, manufacturing history, ownership transfers, and CSC events.

Smart Contracts ($\mathcal{SC}_s$): $\mathcal{SC}_s$ are self-executing agreements with predefined rules and conditions that automate various aspects of the CSC and financial transactions. In this context, $\mathcal{SC}_s$ plays a pivotal role in ensuring trust and efficiency. $\mathcal{SC}_s$ can automate payment settlements as devices move through the CSC. Warranty terms and conditions can be encoded into $\mathcal{SC}_s$. When a device's digital twin detects a malfunction, the smart contract can automatically initiate the warranty claim process. $\mathcal{SC}_s$ can validate the integrity and authenticity of data recorded on the blockchain. If any data inconsistencies or anomalies are detected, $\mathcal{SC}_s$ trigger alerts or corrective actions and ensure transparency and efficiency throughout the process.

B. Data Integration and Analytics

In this step, data collected by sensors from the physical entity (consumer-oriented device) is integrated into the digital twin's virtual model. This integration process involves updating the virtual model in real-time based on sensor data. The process of integrating sensor data into the virtual model is represented in *Equation* (1).

$$\mathcal{V}_t = \mathcal{V}_{t-1} + \Delta\mathcal{V}_t \tag{1}$$

Here, $\Delta\mathcal{V}_t$ represents the change in the virtual model due to new sensor data at time t. Each sensor's data integration (integrating $\mathcal{T}_t$ into the virtual model) is represented as *Equation* (2) based on its respective data type.

$$\Delta\mathcal{V}_t = \mathcal{F}(\mathcal{T}_t) \tag{2}$$

where: $\mathcal{F}(\mathcal{T}_t)$ is the virtual model based on temperature data. Advanced analytics are applied to the integrated data

Authorized licensed use limited to: TRINITY COLLEGE LIBRARY DUBLIN. Downloaded on August 26,2025 at 10:24:37 UTC from IEEE Xplore. Restrictions apply.

TABLE I
USEFUL NOTATIONS AND THEIR DEFINITION

Symbol	Description
D	The data to be validated (e.g., device specifications, manufacturing records, or performance data).
$\mathcal{V}$	Virtual model.
$\mathcal{V}_{t-1}$	virtual model at time t-1.
$\mathcal{V}_t$	virtual model at time t.
$\mathcal{T}_t$	Temperature data into the $\mathcal{V}$.
$\mathcal{H}(\mathcal{D})$	Hash of D.
Ω	Encrypted form of $\mathcal{H}(\mathcal{D})$
$\mathcal{E}()$	Encryption function.
$\mathcal{D}()$	Encryption function.
ε	EncryptionKey / Private key
δ	DecryptionKey / Public key
Υ	The digital signature associated with χ.
γ	Binary variable (1 for device delivered & 0 for not delivered).
ζ	A binary variable (1 for device malfunction, 0 for device functioning correctly).
χ	The seller's account or wallet address.
ψ	The buyer's account or wallet address.
$\Im$	Transactions.
τ	Timestamps
φ	The amount of funds to be transferred.
ϱ	The unique identifier of the device.
ρ	The manufacturer's account (ID) or wallet address.
X	Sensor data value
α	Standard deviation of X.
μ	Mean of X.
λ	Execution cost of $\mathcal{SC}_s$.
κ	Transaction cost of $\mathcal{SC}_s$.

to generate insights and predictions. Here, linear regression for predicting device performance based on usage patterns is presented in *Equation* (3).

$$Y = \beta 0 + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_n X_n \tag{3}$$

where: Y represents the predicted performance metric. $\beta_0, \beta_1, \ldots, \beta_n$ are the regression coefficients. $X_1, X_2, \ldots, X_n$ are the relevant features (sensor data) used for prediction.

Anomaly detection using statistical methods (using a Z-score for identifying outliers in sensor data) is represented in *Equation* (4), where: Z is the Z-score.

$$Z = \frac{X - \mu}{\alpha} \tag{4}$$

C. Data Anchoring on the Blockchain

In this step, critical data points from the digital twin, such as product specifications, manufacturing records, and performance data, are anchored onto the blockchain. These data points are time-stamped and immutable. When anchoring data onto the blockchain, cryptographic hashing is typically used to create a unique fingerprint hash of the data, as shown in *Equation* (5).

$$\mathcal{H}(\mathcal{D}) = SHA256(\mathcal{D}) \tag{5}$$

SHA-256 is the Secure Hash Algorithm 256-bit cryptographic hash function. To ensure immutability, a timestamp is added to $\mathcal{H}(\mathcal{D})$ by creating a digital signature (Υ) using *Equation* (6).

$$\Upsilon = SHA256(\mathcal{D} + \tau) \tag{6}$$

Each device is associated with a unique identifier ϱ (generated using *Equation* (7)) recorded on the blockchain ledger.

Algorithm 1: Payment Settlements

Input: χ, ψ, φ;
Output: TransactionStatus;
γ: A binary variable (1 for device delivered successfully, 0 for not delivered);
if (γ *is equal to 1)* **then**
  Execute the smart contract action:;
  TransactionStatus = TransferFunds(φ, χ, ψ);
else
  TransactionStatus =ϱ not delivered, payment settlement failed;
end
Return TransactionStatus: A status indicating the success of the payment settlement;

This identifier is linked to the device's digital twin and its associated data hashes.

$$\varrho = UniqueIdentifier(\mathcal{D}, \Upsilon) \tag{7}$$

To ensure transparency in the CSC, the blockchain ledger records each device's ϱ and its corresponding transactions (see *Equation* (8)) as it moves through the CSC.

$$\Im = Transaction(\varrho, \chi, \psi, \tau) \tag{8}$$

D. $\mathcal{SC}_s$ for CSC Automation

$\mathcal{SC}_s$ are self-executing agreements with predefined rules and conditions that automate various aspects of the CSC, such as payment settlements, warranty management, and data validation. The payment settlement is described in Algorithm 1, which handles the conditional transfer of funds based on predefined delivery conditions. A key parameter in this process is represented by γ, which signifies the successful delivery of a device or product. It first checks if the delivery condition γ is met. This could be confirmed through delivery tracking systems, digital signatures, or IoT-enabled devices. If γ is true (delivery is successful), the smart contract automatically triggers the release of funds to the supplier or vendor. If the delivery condition is not met, the transaction is flagged as unsuccessful, and the payment process is terminated. The funds remain unreleased, which is critical in decentralized systems that require trustless execution. After the payment process is completed, the warranty of consumer-oriented devices or products becomes essential to ensure ongoing product support and customer satisfaction. Warranty management is crucial in a CSC because it upholds the commitment to product quality and reliability. Therefore, the warranty algorithm (described in Algorithm 2) is proposed to provide a mechanism for managing malfunctions or defects. This monitors for device malfunctions. A key variable ζ is used to determine whether a malfunction has occurred ($\zeta = 1$) or not ($\zeta = 0$). If $\zeta = 1$, it initiates a warranty validation process, validates the claim, notifies the relevant parties, and initiates corrective actions or replacements. If $\zeta = 0$, the warranty validation process is bypassed and confirms that no action is needed. Furthermore, the overall process is trustless, autonomous, and decentralized and ideal for blockchain networks that underpin many modern CSC systems.

Authorized licensed use limited to: TRINITY COLLEGE LIBRARY DUBLIN. Downloaded on August 26,2025 at 10:24:37 UTC from IEEE Xplore. Restrictions apply.

Algorithm 2: Warranty Management

Input: ϱ, ρ, ζ;
Output: WarrantyValidationStatus;
if (ζ *is equal to 1)* **then**
  Execute the smart contract action: WarrantyValidationStatus = ValidateWarranty(ϱ, ρ);
else
  WarrantyValidationStatus = "No device malfunction reported, warranty validation not required";
end
Return TransactionStatus: A status indicating the success of warranty validation;

Algorithm 3: Data Integrity Validation

Input: ϱ;
Output: ValidationResult, ErrorMessage;
if (Υ *is valid)* **then**
  Calculate the hash of the provided data ($\mathcal{H}'(\mathcal{D})$);
  if (($\mathcal{H}'(\mathcal{D})$) == ($\mathcal{H}(\mathcal{D})$)) **then**
    Check τ of the data and ensure it falls within an acceptable time frame;
    Obtain the current τ;
    if (τ *is valid)* **then**
      Set **ValidationResult** to "Validation Successful";
    else
      ErrorMessage set to "Invalid τ";
    end
  else
    Set **ValidationResult** to "Validation Failed";
  end
else
  Set **ErrorMessage** to "Υ verification failed;
end
if *(Algorithm 1 && Algorithm 2 is executed successfully)* **then**
  End the data validation process;
  Return **ValidationResult** as the final result of data validation;
else
  ErrorMessage to provide details on the validation failure;
end

E. Data Integrity Assurance

Cryptographic hash functions are essential tools for ensuring data integrity on the blockchain. These functions take an input (data) and produce a fixed-size output (hash) that is unique to the input data. Any change in the input data, even a small one, results in a significantly different hash. This property makes cryptographic hashes suitable for detecting tampering or data corruption. To verify data integrity, *Equation* (9) is represented to compare the calculated hash with the stored hash on the blockchain. Algorithm 3 is designed to validate the integrity of data by verifying its authenticity and ensuring that it meets the required temporal constraints. The validation process includes hashing the data, comparing it to a reference hash, checking its timestamp, and confirming that related algorithms (Algorithms 1 and 2) have been executed successfully. It ensures that the integrity and validity of data are verified before it is accepted as trustworthy.

$$\mathcal{H}'(\mathcal{D}) = StoredHash \tag{9}$$

where: StoredHash is the hash $\mathcal{H}(\mathcal{D})$ previously recorded on the blockchain. If $\mathcal{H}'(\mathcal{D})$ matches with $\mathcal{H}(\mathcal{D})$, the data is considered intact. Any modification to D would result in a different hash, indicating potential data tampering. When a new block is proposed by a miner, it undergoes validation by the network. The network nodes independently verify the transactions and the nonce to ensure that the block's content is accurate and that the Proof of Work (PoW) puzzle was correctly solved. If a majority of nodes agree, the block is added to the blockchain and provides consensus on the data's integrity.

F. CSC Processes

During manufacturing, DT generates data $\mathcal{H}$ that represents the specifications of each device. The resulting $\mathcal{H}(\mathcal{D})$ is unique to the device's specifications. The hash $\mathcal{H}(\mathcal{D})$ is recorded on the blockchain as part of the device's manufacturing record. This creates a digital trail of the device's origin ensuring data integrity and traceability.

At each step of the distribution phase (e.g., shipping, storage, quality checks), relevant information is logged on the blockchain. Blockchain records a series of these $\Im$ transactions. Consumers can verify the authenticity of a device by scanning a QR code or using a mobile app, which retrieves the device's unique identifier ϱ, which is the identifier that has been pre-recorded on the blockchain during an earlier transaction or at the time of product registration. The blockchain stores ϱ in a tamper-proof and decentralized manner and makes it a reliable source for verification. The verification process includes querying the blockchain using ϱ' and comparing it against ϱ (i.e., $\varrho' = \varrho$) where ϱ' is the identifier provided during the verification process. The goal of the verification is to check whether the current ϱ' matches the stored ϱ on the blockchain. If the ϱ' matches the recorded identifier ϱ, the device is considered authentic. This comparison ensures that only genuine devices are validated to protect the integrity of the CSC.

G. Encryption and Access Controls

End-to-end encryption protects sensitive data as it travels through the CSC. Encryption ensures that only authorized parties can decrypt and access the data. Encryption and Decryption processes are shown in *Equations* (10) and (11).

$$\Omega = \mathcal{E}(\mathcal{H}(\mathcal{D}), \varepsilon) \tag{10}$$

$$\mathcal{HD} = \mathcal{D}(\Omega, \delta) \tag{11}$$

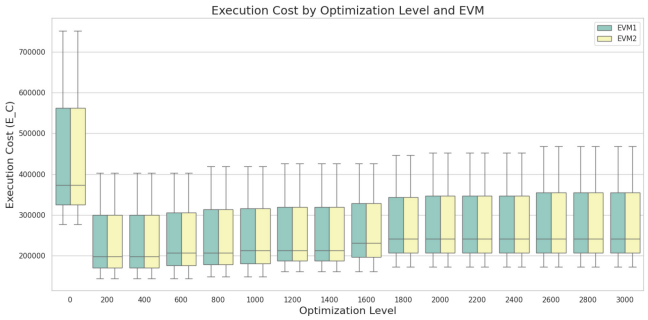
To ensure that only authorized parties can view or modify data on the blockchain, granular access controls can be established. Access control policies are defined based on roles and permissions. Let's consider an example with two roles: "Manufacturer" and "Retailer."

Access Control Policy for Manufacturer: 1) Manufacturers can write manufacturing data to the blockchain but cannot modify distribution data. 2) Manufacturer has read access to distribution data related to their products.

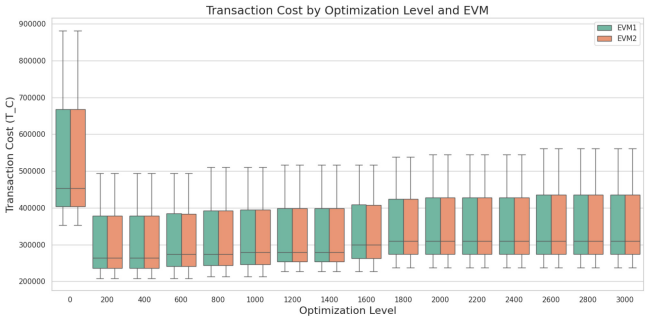
Access Control Policy for Retailer: Retailers can read distribution data and verify product authenticity but cannot modify manufacturing data.

However, Access control policies can be enforced using cryptographic methods and digital signatures. For example,

Authorized licensed use limited to: TRINITY COLLEGE LIBRARY DUBLIN. Downloaded on August 26,2025 at 10:24:37 UTC from IEEE Xplore. Restrictions apply.



(a) λ of two EVMs.



(b) κ of two EVMs.

Fig. 3. λ and κ analysis based on optimization levels of two different EVMs.

a manufacturer can sign their manufacturing data with their private key, and a retailer can verify the signature using the manufacturer's public key.

IV. Experiment Results and Analysis

In our experimentation, we developed three distinct $\mathcal{SC}_s$ tailored to specific algorithms: payment settlement, warranty management, and data integrity validation. These contracts were implemented within the Ethereum Remix IDE [30] using the Solidity programming language. Remix IDE served as our primary development and testing environment. It provides an Ethereum Virtual Machine (EVM) for cost analysis during contract deployment and execution, as shown in Fig. 3 for our case. The EVM is a decentralized system that powers the Ethereum blockchain. It's a virtual computer that runs $\mathcal{SC}_s$ and decentralized apps (dApps). The EVM consists of multiple connected computers working together to process tasks and execute instructions.

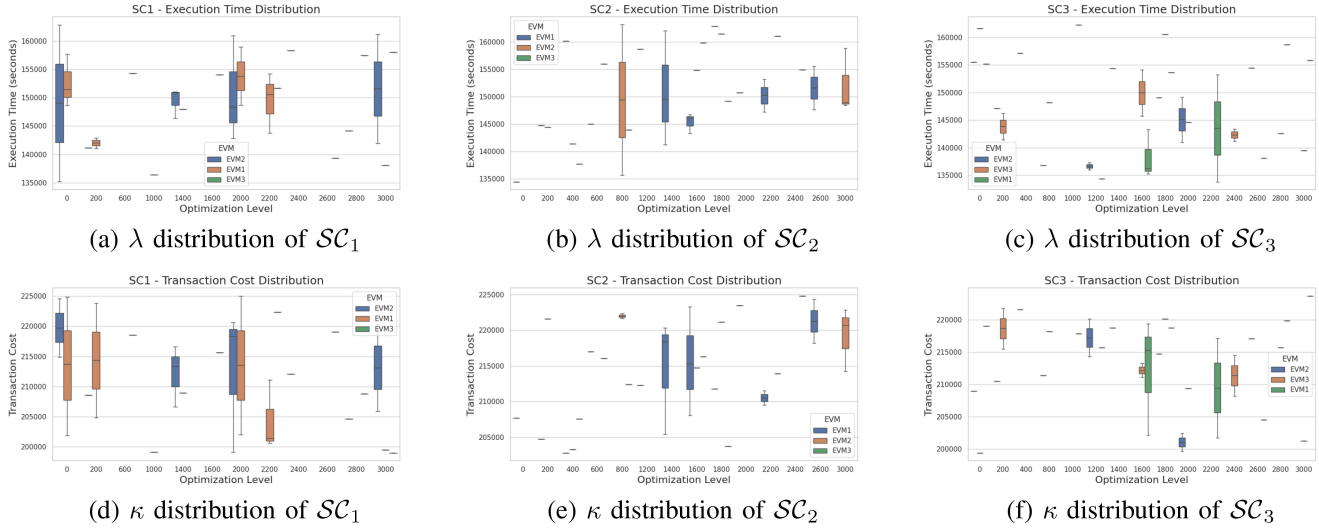
A. Experiment Results

1) $\mathcal{SC}_s$ for CSC Automation: $\mathcal{SC}_1$ PaymentSettlement, facilitates payment settlement between χ and ψ. The contract includes two modifiers, *onlyBuyer* and *onlySeller*, which restrict certain functions to be callable only by the respective parties. *settlePayment* function is intended to be called by the ψ and requires two parameters: *deviceDelivered*, indicating whether the purchased device was delivered, and *paymentAmount*, specifying the amount to be settled. If the device was not delivered, the contract transfers the payment amount to the χ using the *send* function for the payment settlement to be executed. $\mathcal{SC}_2$ for *WarrantyManagement* is designed for managing warranties associated with devices. It includes functionality for manufacturers to validate warranties and for users to check the validity of their warranties. The contract is initialized with the manufacturer's address and a specified warranty duration in seconds. The main functions are protected by a modifier called *onlyManufacturer*, which ensures only the manufacturer can call certain functions. The overall cost of $\mathcal{SC}_1$ and $\mathcal{SC}_2$ are shown in Fig. 4(a), 4(b), 4(d), and 4(e), which are calculated in several optimization levels at different environments. Optimization level is a feature that simplifies complex expressions in Solidity code, which can reduce the size of the code and the cost of execution. Specific optimizations aim to reduce transaction and execution costs, improve speed, or optimize resource usage within the Ethereum environment.

2) Data Integrity Assurance: $\mathcal{SC}_3$ for *DataIntegrity Validation* smart contract serves the purpose of validating data integrity on the Ethereum blockchain. It stores essential data attributes, including the data itself, original and current hash values, a timestamp, the validator's address, and the validation result status. The contract's constructor initializes these parameters and sets the initial validation status to *Pending*. A *onlyValidator* modifier ensures that only the designated validator can invoke certain functions. The core function *validateData* facilitates data validation by comparing the provided current hash with the original hash, verifying the timestamp, and updating the validation result accordingly. If successful, it marks the validation as *Successful*; otherwise, it flags it as *Failed* with an appropriate error message. The proposed algorithms consistently demonstrated their ability to maintain the integrity of data products, authenticate sellers, and verify buyers securely and efficiently. Our testing and validation process has provided strong evidence that these algorithms are robust and reliable setting a solid foundation for the secure operation of our metaverse-driven CSC ecosystem. λ and κ of $\mathcal{SC}_3$ without applying optimization is shown in Fig. 4(c) and applying optimization on cost are shown in Fig. 4(f). Furthermore, increasing optimization levels generally reduces transaction costs but may slightly impact execution times.

3) Comparison Analysis: In our experiment, $\mathcal{SC}_1$ (*payment settlement*) shows consistent cost reductions with higher optimization. As optimization levels increase, the cost consistently decreases. This indicates that optimizing the smart contract reduces the expense associated with executing payment transactions, which makes it more efficient. $\mathcal{SC}_2$ (*warranty management*) benefits from moderate optimization as it balances the cost and execution time for managing warranties and validations. Moderate levels of optimization work best here. This smart contract benefits from some optimization, but too much optimization might compromise the balance between cost and how fast it executes. Therefore, finding the right middle ground is a key challenge. Finally, $\mathcal{SC}_3$ (*data integrity validation*) shows the highest sensitivity to optimization levels due to its complexity. This smart contract is more complex, so its costs and performance are highly affected by the level of optimization. Small changes in optimization can have a big impact that makes this smart contract sensitive to

Authorized licensed use limited to: TRINITY COLLEGE LIBRARY DUBLIN. Downloaded on August 26,2025 at 10:24:37 UTC from IEEE Xplore. Restrictions apply.



(a) λ distribution of $\mathcal{SC}_1$ (b) λ distribution of $\mathcal{SC}_2$ (c) λ distribution of $\mathcal{SC}_3$

(d) κ distribution of $\mathcal{SC}_1$ (e) κ distribution of $\mathcal{SC}_2$ (f) κ distribution of $\mathcal{SC}_3$

Fig. 4. λ and κ analysis results.

achieve the best results. Overall, each smart contract behaves differently under various optimization levels due to differences in complexity and function. And, these contracts achieve the best cost and performance through balancing the cost and execution in different optimization levels. Here in this paper, the proposed method applies a balanced level of optimization specifically tuned for each smart contract. This ensures that cost is minimized without compromising execution speed or security, which makes it particularly effective for the diverse requirements of $\mathcal{SC}_1$, $\mathcal{SC}_2$, and $\mathcal{SC}_3$. Across all scenarios, the proposed approach works best because it intelligently adapts and optimizes each smart contract's execution based on its unique requirements.

Therefore, DT enables real-time monitoring and tracking of warranty-related data and blockchain ensures the integrity and transparency of this data. This integration improves decision-making in the CSC by providing accurate and real-time warranty validation. The experiment highlights that with the proposed integration, $\mathcal{SC}_3$ becomes more efficient and reliable with the need for high security in CSC transactions. $\mathcal{SC}_1$ shows consistent cost reductions as optimization levels increase which can automate and secure payment processes for the consumer electronics's CSC management. As shown in Fig. 5, the proposed integration of DT and blockchain outperforms other schemes across a wide range of security parameters. It is particularly well-suited for environments where real-time monitoring, proactive threat detection, and decentralized control are essential, such as metaverse-inspired CSC.

The proposed approach positions as a robust, scalable, and future-ready solution compared to traditional or less integrated systems, as described in Table II. It provides key benefits for evaluating the proposed integration of DT and blockchain against various existing approaches in the context of CSC management. The proposed approach **1**) Achieves high data integrity through the combination of blockchain's immutable ledger and real-time validation by digital twins, where DT-enabled/traditional methods have low integrity due to data manipulation risks. **2**) Demonstrates high tamper resistance due to the immutability of blockchain and alerts

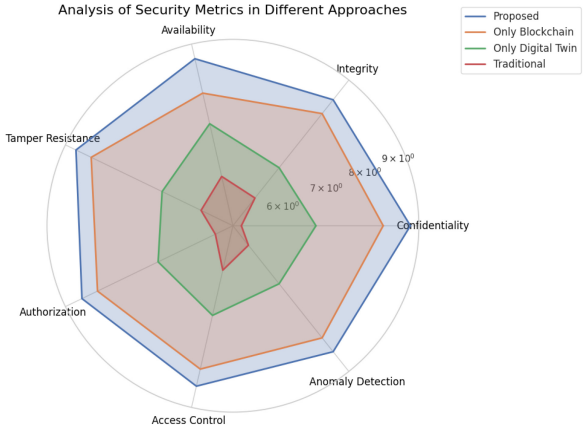


Fig. 5. Analysis of security metrics in different approaches.

generated from digital twins to make it far superior to DT-enabled/traditional systems. **3**) Utilizes $\mathcal{SC}_s$ and DT access control policies for robust access control compared to the basic or manual access controls found in DT-enabled/traditional systems. **4**) Enhances resilience through decentralized and twin-based anomaly detection and makes it significantly more robust against attacks compared to DT-enabled/traditional systems. **5**) The integration is designed to be compatible with metaverse standards for its applicability in future environments, while DT-enabled/traditional systems face significant interoperability challenges. **6**) Finally, high fault tolerance in the proposed scheme is achieved through redundant twin and blockchain nodes, whereas DT-enabled/traditional systems often struggle with single points of failure. Overall, the proposed integration of DT and blockchain stands out as the superior solution due to its advantages across these critical metrics. It not only enhances security and efficiency in CSC management but also positions itself as a future-ready system capable of meeting the demands of increasingly complex and interconnected environments, such as metaverse-inspired CSC.

B. Analysis of Consumer Apps and Metaverse Interfaces

Consumer apps are developed to provide a user-friendly interface for consumers to interact with the digital twin of

Authorized licensed use limited to: TRINITY COLLEGE LIBRARY DUBLIN. Downloaded on August 26,2025 at 10:24:37 UTC from IEEE Xplore. Restrictions apply.

TABLE II
COMPARISON OF SECURITY METRICS ACROSS VARIOUS APPROACHES

Metrics/Approach	Proposed (DT + Blockchain)	Blockchain [21], [22]	DT [17], [18], [32]	Traditional [33], [34], [35]
Data Integrity	High (Blockchain + real-time twin validation)	High (Immutable blockchain ledger)	Moderate (Centralized data)	Low (Easily manipulated data)
Tamper Resistance	High (Blockchain immutability + alerts from twins)	High (Blockchain immutability)	Low (Vulnerable centralized control)	Low (Manual processes prone to tampering)
Traceability and Auditability	High (Blockchain + twin logs)	High (Blockchain audit trails)	Moderate (Limited by centralized logging)	Low (Basic traceability with manual records)
Real-time Monitoring	High (Twin-driven continuous monitoring)	Low (Blockchain lacks real-time capabilities)	High (Twins provide real-time insights)	Low (Traditional systems are reactive)
Decentralization	High (Blockchain distributed network)	High (Decentralized blockchain)	Low (Centralized twin systems)	Low (Single points of failure)
Access Control and Authorization	High ($\mathcal{SC}_s$ + twin access control policies)	High ($\mathcal{SC}_s$ enforce rules)	Low (Limited by centralized control)	Low (Manual or basic access controls)
Privacy Protection	High (Encryption + selective data sharing)	Moderate (Depends on blockchain design)	Low (Privacy vulnerable in centralized systems)	Low (Minimal privacy controls)
Resilience Against Attacks	High (Decentralized, twin-based anomaly detection)	Moderate (Resistant but not proactive)	Low (Single points of failure)	Low (Vulnerable to various attacks)
Interoperability and Standards Compliance	High (Compatible with metaverse standards)	Moderate (Interoperability limited to blockchain protocols)	Low (Custom solutions for twin platforms)	Low (Legacy systems with limited compliance)
Anomaly Detection and Predictive Analytics	High (Twins offer real-time analytics)	Low (Reactive monitoring only)	High (Predictive twin analytics)	Low (Manual and reactive incident response)
Fault Tolerance	High (Redundant twin and blockchain nodes)	Moderate (Depends on blockchain network redundancy)	Moderate (Fault tolerance limited by centralization)	Low (Single points of failure)

their consumer-oriented devices. Users can access real-time information about their devices, such as performance metrics, usage data, and maintenance recommendations from the digital twin. Consumers can easily view and manage warranty-related information, including coverage details, expiration dates, and the process for warranty claims. Some consumer-oriented devices, such as smartphones, offer customization options. Users can personalize their devices through the app, and the changes are reflected in the digital twin.

Metaverse Interfaces for Blockchain-Enabled Interaction: In the metaverse era, blockchain integration enhances user engagement by enabling secure and transparent interactions beyond traditional mobile apps [35]. These interfaces provide immersive experiences where users can explore virtual showrooms and verify the authenticity of consumer-oriented devices through blockchain-backed digital certificates. They can interact with $\mathcal{SC}_s$ to automatically handle transactions like payments, warranties, and product ownership transfers within the virtual environment. Blockchain-driven AI avatars or virtual representatives assist users with inquiries and provide decentralized support for troubleshooting and technical issues. Users can participate in shared experiences in product launches or community events. Gamification features can add value by rewarding users with blockchain tokens or digital assets for engaging in activities of the metaverse. This blockchain integration not only secures interactions but also empowers users to verify device authenticity and ownership within the metaverse ecosystem.

V. CONCLUSION

The integration of DT and blockchain presents a paradigm shift for addressing the challenges of security, transparency, & trust and ensuring data integrity in metaverse-driven CSC and products. This innovative approach brings together the physical and virtual worlds, where manufacturers can gain real-time insights into product performance by creating DT of consumer-oriented devices. This DT serve as the bridge between the physical devices and the virtual metaverse to facilitate seamless interaction. Meanwhile, blockchain ensures the security and immutability of critical data points, such as product specifications and CSC records and establishes trust in the authenticity of consumer-oriented products and provides transparency throughout the CSC. In the metaverse, users can engage in virtual shopping and trade digital representations of consumer-oriented products. And, blockchain-based tokens enable secure transactions and ownership transfers. Furthermore, the proposed approach not only ensures the authenticity of products but also enhances user trust, engagement, and the overall consumer-oriented experience in the metaverse-driven era. The application of the integrated approach beyond consumer electronics to other sectors, such as healthcare, manufacturing, and logistics, can be expanded to validate its versatility and effectiveness in various contexts. Continuous research into new security protocols and frameworks will be necessary and focused on adapting to emerging threats and vulnerabilities using advanced encryption methods and real-time threat detection algorithms for future digital twin environments.

REFERENCES

[1] D. Javeed, M. S. Saeed, I. Ahmad, P. Kumar, A. Jolfaei, and M. Tahir, "An intelligent intrusion detection system for smart consumer electronics network," *IEEE Trans. Consum. Electron.*, vol. 69, no. 4, pp. 906–913, Nov. 2023.

[2] H. Dong and Y. Liu, "Metaverse meets consumer electronics," *IEEE Consum. Electron. Mag.*, vol. 12, no. 3, pp. 17–19, May 2023.

[3] P. Chatterjee, D. Das, and D. B. Rawat, "Digital twin for credit card fraud detection: Opportunities, challenges, and fraud detection advancements," *Future Gener. Comput. Syst.*, vol. 158, pp. 410–426, Sep. 2024.

Authorized licensed use limited to: TRINITY COLLEGE LIBRARY DUBLIN. Downloaded on August 26,2025 at 10:24:37 UTC from IEEE Xplore. Restrictions apply.

[4] Z. Lv, W.-L. Shang, and M. Guizani, "Impact of digital twins and metaverse on cities: History, current situation, and application perspectives," *Appl. Sci.*, vol. 12, no. 24, 2022, Art. no. 12820.
[5] S. Zahran, "Optimizing supply chain management of fresh E-commerce agri-consumer products using energy-efficient vehicle routing," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 1685–1693, Feb. 2024.
[6] B. Hammi, S. Zeadally, and J. Nebhen, "Security threats, countermeasures, and challenges of digital supply chains," *ACM Comput. Surv.*, vol. 55, no. 14, pp. 1–10, Jul. 2023.
[7] S. Sai, D. Goyal, V. Chamola, and B. Sikdar, "Consumer electronics technologies for enabling an immersive metaverse experience," *IEEE Consum. Electron. Mag.*, vol. 13, no. 3, pp. 16–24, May 2024.
[8] S. Banerjee, D. Das, P. Chatterjee, and U. Ghosh, "Blockchain-enabled digital twin technology for next-generation transportation systems," in *Proc. IEEE 26th Int. Symp. Real-Time Distrib. Comput. (ISORC)*, 2023, pp. 224–229.
[9] D. Das, S. Banerjee, P. Chatterjee, U. Ghosh, W. Mansoor, and U. Biswas, "Design of an automated blockchain-enabled vehicle data management system," in *Proc. 5th Int. Conf. Signal Process. Inf. Secur. (ICSPIS)*, 2022, pp. 22–25.
[10] D. Das, K. Dasgupta, and U. Biswas, "A secure blockchain-enabled vehicle identity management framework for intelligent transportation systems," *Comput. Elect. Eng.*, vol. 105, Jan. 2023, Art. no. 108535.
[11] A. Rasheed, O. San, and T. Kvamsdal, "Digital twin: Values, challenges and enablers from a modeling perspective," *IEEE Access*, vol. 8, pp. 21980–22012, 2020.
[12] J.-F. Yao, Y. Yang, X.-C. Wang, and X.-P. Zhang, "Systematic review of digital twin technology and applications," *Vis. Comput. Industry, Biomed., Art*, vol. 6, no. 1, p. 10, 2023.
[13] Z. Lv, S. Xie, Y. Li, M. S. Hossain, and A. El Saddik, "Building the metaverse by digital twins at all scales, state, relation," *Virtual Reality Intell. Hardw.*, vol. 4, no. 6, pp. 459–470, 2022.
[14] A. E. Onile, R. Machlev, E. Petlenkov, Y. Levron, and J. Belikov, "Uses of the digital twins concept for energy services, intelligent recommendation systems, and demand side management: A review," *Energy Rep.*, vol. 7, pp. 997–1015, Nov. 2021.
[15] P. Chatterjee, D. Das, and D. B. Rawat, "Federated learning empowered recommendation model for financial consumer services," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 2508–2516, Feb. 2024.
[16] Y. Liu, C. Xu, L. Chen, M. Yan, W. Zhao, and Z. Guan, "TABLE: Time-aware balanced multi-view learning for stock ranking," *Knowl.-Based Syst.*, vol. 303, Nov. 2024, Art. no. 112424.
[17] W. Liu et al., "Digital twin-assisted edge service caching for consumer electronics manufacturing," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 3141–3151, Feb. 2024.
[18] T. Wang, J. Tian, K. Fang, T. R. Gadekallu, and W. Wang, "AI and digital twin for consumer electronics in smart cities," *IEEE Consum. Electron. Mag.*, early access, Aug. 15, 2024, doi: 10.1109/MCE.2024.3444312.
[19] D. Das, S. Banerjee, P. Chatterjee, U. Ghosh, W. Mansoor, and U. Biswas, "Design of a trust-based authentication scheme for blockchain-enabled IoV system," in *Proc. Adv. Sci. Eng. Technol. Int. Conf. (ASET)*, 2023, pp. 1–6.
[20] K. Gai, Y. Zhang, M. Qiu, and B. Thuraisingham, "Blockchain-enabled service optimizations in supply chain digital twin," *IEEE Trans. Services Comput.*, vol. 16, no. 3, pp. 1673–1685, Jun. 2023.
[21] S. Datta and S. Namasudra, "Blockchain-based smart contract model for securing Healthcare transactions by using consumer electronics and mobile-edge computing," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 4026–4036, Feb. 2024.
[22] X. Wang, A. Shankar, K. Li, B. D. Parameshachari, and J. Lv, "Blockchain-enabled decentralized edge intelligence for trustworthy 6G consumer electronics," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 1214–1225, Feb. 2024.
[23] M. A. Babu and P. Mohan, "Impact of the metaverse on the digital future: People's perspective," in *Proc. 7th Int. Conf. Commun. Electron. Syst. (ICCES)*, 2022, pp. 1576–1581.
[24] M. E. Latino, M. Menegoli, M. Lazoi, and A. Corallo, "Voluntary traceability in food supply chain: A framework leading its implementation in agriculture 4.0," *Technol. Forecast. Soc. Change*, vol. 178, May 2022, Art. no. 121564.
[25] Y. Qin, L. Song, L. H. Shi, and K. Tan, "A global perspective on combating Shanzhai products: Cross-cultural solutions," *Thunderbird Int. Bus. Rev.*, vol. 65, no. 4, pp. 409–421, 2023.
[26] S. Cuc, "Unlocking the potential of blockchain technology in the textile and fashion industry," *FinTech*, vol. 2, no. 2, pp. 311–326, 2023.
[27] P. Chatterjee, D. Das, and D. B. Rawat, "Next generation financial services: Role of blockchain enabled federated learning and metaverse," in *Proc. IEEE/ACM 23rd Int. Symp. Cluster, Cloud Internet Comput. Workshops (CCGridW)*, 2023, pp. 69–74.
[28] R. K. Marjerison, C. Chae, and S. Li, "Investor activity in Chinese financial institutions: A precursor to economic sustainability," *Sustainability*, vol. 13, no. 21, 2021, Art.no. 12267.
[29] A. Zatevakhina, N. Dedyukhina, and O. Klioutchnikov, "Recommender systems-the foundation of an intelligent financial platform: Prospects of development," in *Proc. Int. Conf. Artif. Intell., Appl. Innovat. (IC-AIAI)*, 2019, pp. 104–1046.
[30] "The native ide for Web3 development IDEv0.29.0." Accessed: Aug. 18, 2024. [Online]. Available: https://remix.ethereum.org/
[31] S. Sai, M. Prasad, A. Upadhyay, V. Chamola, and N. Herencsar, "Confluence of digital twins and Metaverse for consumer electronics: Real world case studies," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 3194–3203, Feb. 2024.
[32] Y. Li, J. Shen, P. Vijayakumar, C.-F. Lai, A. Sivaraman, and P. K. Sharma, "Next-generation consumer electronics data auditing scheme toward cloud–edge distributed and resilient machine learning," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 2244–2256, Feb. 2024.
[33] Z. Li, Z. Yang, and S. Xie, "Computing resource trading for edge-cloud-assisted Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3661–3669, Jun. 2019.
[34] W. Z. Khan, M. Y. Aalsalem, M. K. Khan, and Q. Arshad, "Data and privacy: Getting consumers to trust products enabled by the Internet of Things," *IEEE Consum. Electron. Mag.*, vol. 8, no. 2, pp. 35–38, Mar. 2019.
[35] T. Huynh-The et al., "Blockchain for the metaverse: A review," *Future Gener. Comput. Syst.*, vol. 143, pp. 401–419, Jun. 2023.

Authorized licensed use limited to: TRINITY COLLEGE LIBRARY DUBLIN. Downloaded on August 26,2025 at 10:24:37 UTC from IEEE Xplore. Restrictions apply.