

# The Role of AI and Blockchain in Enhancing Digital Identity and Digital Wallets in Albania

PhD. Blerta Leka (Moçka)<sup>1\*</sup>, Mariana Nikolla<sup>2</sup>, Arben Kambo<sup>3</sup>

<sup>1,2,3</sup> Department of Mathematics and Informatics, Faculty of Economics and Agribusiness, Agricultural University of Tirana, Albania

\*Corresponding Author: e-mail: [bmocka@ubt.edu.al](mailto:bmocka@ubt.edu.al)

## Abstract

This paper explores the evolving role of artificial intelligence (AI) and blockchain technology in enhancing digital identity solutions, with a specific focus on Albania's readiness and challenges in adopting digital wallets aligned with European Union standards. Digital identity solutions, empowered by blockchain, provide secure, decentralized, and tamper-resistant frameworks that improve identity verification and data privacy. AI further strengthens these systems through advanced biometric authentication, fraud detection, real-time decision-making, and personalized user experiences. The integration of AI and blockchain technologies promises to address critical issues such as identity theft, secure authentication, and data protection while supporting self-sovereign identity management. The study reviews global digital wallet adoption trends, EU initiatives like the European Digital Identity Wallet, and Albania's digital governance landscape, highlighting infrastructural, regulatory, and public trust challenges. It emphasizes the need for robust legal frameworks, cybersecurity measures, and public awareness to ensure secure and efficient digital identity management. Ultimately, this research highlights how AI and blockchain can facilitate Albania's digital transformation, fostering secure, user-centric digital identity ecosystems critical for e-governance, finance, and cross-border services.

*Keywords: Digital Identity, Blockchain, Artificial Intelligence, Digital Wallet, Albania, Data Privacy, EU Digital Identity.*

## 1. Introduction

The digital transformation of public services, including digital wallets, has gained significant traction globally. Governments and private entities are increasingly integrating digital identity solutions and AI-driven technologies to enhance efficiency, security, and accessibility.

Digital identity is a digital representation of an individual's or entity's information used to authenticate and authorize access to services in online environments. It typically includes:

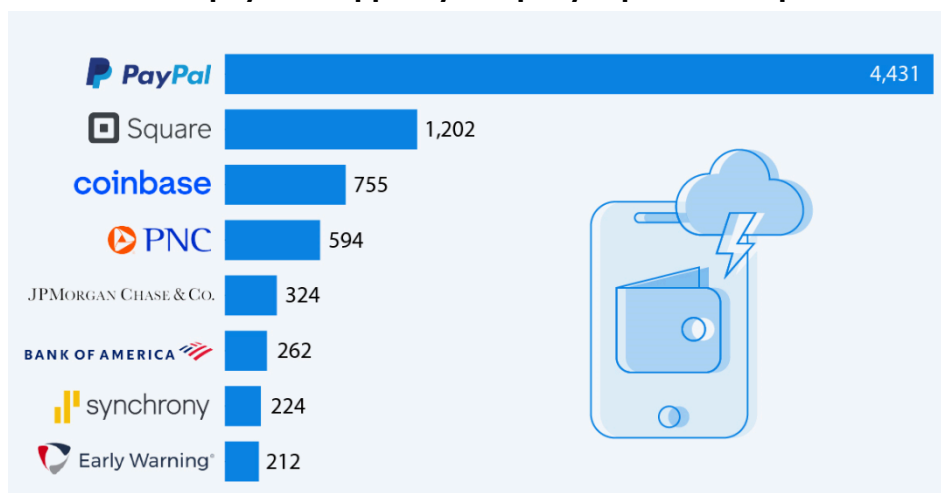
- Personally Identifiable Information (PII): name, birthdate, ID number
- Biometric data: facial recognition, fingerprints, iris scans
- Credentials: usernames, passwords, digital certificates
- Behavioral data: device usage, location patterns

Digital wallets have rapidly gained popularity due to their convenience and evolving features, with many consumers, especially Millennials and Gen-Z, seeking additional functionalities like secure information storage and international fund transfers (Fuentes, 2024). Financial institutions can enhance customer satisfaction by tailoring digital wallet features to meet specific customer needs, simplifying user experiences, and ensuring robust security measures like tokenization and biometric authentication. Partnerships with technology vendors can help smaller institutions overcome resource challenges. By prioritizing customer preferences and data protection, digital wallets can foster long-term loyalty and drive future growth in the financial sector.

Apple Pay and digital wallets represent an evolution of payment systems rather than a financial revolution, adapting traditional payment methods to the digital age. While Apple Pay introduces the next phase in the evolution of money, it is the strong brand image and strategic marketing of Apple Inc. that have played a crucial role in its adoption. The lack of a proper regulatory framework for mobile and digital wallets is a key challenge, with existing laws failing to address their unique characteristics. Legal definitions and clearer guidelines are needed to establish the rights and obligations surrounding these Technologies (Salazar, 2017). Moreover, the rapid pace of technological innovation in digital payments outstrips the law's ability to regulate, raising concerns about security and the potential risks of unregulated electronic transactions. As such, authorities must carefully balance regulation with innovation, understanding the trade-offs involved in ensuring both security and progress in this fast-evolving sector.

However, just as we acknowledge the advantages of digital wallets, it is essential to address the challenges and user dissatisfaction that accompany their widespread adoption. As illustrated in Figure 1, most consumer complaints reported to U.S. federal regulators between April 2017 and April 2021 were directed at a few major providers. PayPal received the highest number of complaints (4,431), followed by Square (1,202) and Coinbase (755), highlighting recurring issues related to account management and unauthorized transactions (McCarthy, 2021).

**Figure 2. Consumer complaints submitted to U.S. federal regulators about digital wallets and payment apps, by company (April 2017–April 2021).**



Source: U.S. Public Interest Research Group, as cited in McCarthy (2021).

CFPB has finalized a rule to supervise Big Tech companies like Apple, Google, and Amazon, which together process over 13 billion transactions annually through digital wallets and payment apps (Gillison, 2024). This rule brings these services under regulatory scrutiny like those faced by banks, aiming to protect consumer privacy, prevent fraud, and stop the illegal closure of accounts. The rule applies to companies processing at least 50 million transactions per year and will focus on U.S. dollar transactions. Set to take effect 30 days after publication, the rule marks a significant step in regulating the growing digital payments sector.

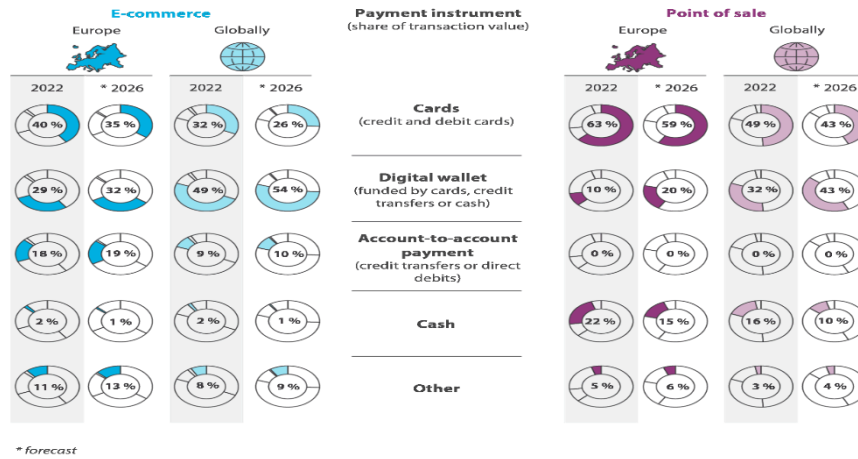
According to the European Court of Auditors (2025), while card payments have traditionally dominated retail transactions in Europe, the value of payments via digital wallets is growing dynamically, signaling a shift away from cash, which is steadily losing its importance (Figure 2).

While this trend suggests progress, it also underscores key structural and ethical challenges:

- The need for robust legal and regulatory frameworks aligned with EU digital finance and AI governance standards.
- Significant investment in technological infrastructure and cybersecurity, particularly in cross-border contexts.
- Enhanced public awareness and education to address digital identity, privacy, and fraud risks.
- The challenge of ensuring interoperability and cross-border acceptance of digital payment systems.
- Ongoing ethical concerns regarding data usage, algorithmic bias, and AI-driven decision-making in financial services.

Addressing these challenges will be essential not only for protecting consumers but also for ensuring the safe and inclusive digital transformation of the financial ecosystem.

**Figure 3.** Share of transaction value by payment instrument (European Court of Auditors, 2025)



## 2. Digital Wallet

### 2.1 How Digital Wallets Work

A digital wallet is a secure, software-based system that stores payment information, identification credentials, and other personal data electronically. It enables users to make transactions, access services, and verify their identities without physical documents or cash. The EU Digital Identity Wallet is designed to be highly secure, using advanced encryption and giving users full control over which data they share and with whom. It follows European data protection standards such as the GDPR and is built to ensure that only the user can manage and share their official credentials.

However, security is not absolute. It depends on:

- The quality of technical implementation.
- User education and awareness.
- The state’s preparedness to deal with cyber threats

Key Components of Digital Wallets (Figure 3):

**Figure 4.** Key Components of Digital Wallets (Source: OpenAI, 2025)



- User Authentication – Digital wallets require secure authentication methods such as PIN codes, biometrics (fingerprint, facial recognition), or multi-factor authentication to ensure only authorized users can access their accounts.

- Data Storage & Encryption – Payment details, personal identity documents, and credentials are securely stored using encryption to prevent unauthorized access and data breaches.
- Payment Integration – Digital wallets support various payment methods, including credit/debit cards, bank accounts, and cryptocurrencies, enabling seamless transactions.
- Near Field Communication (NFC) & QR Codes – Digital wallets facilitate contactless payments via NFC technology and QR codes, allowing users to make purchases with a simple tap or scan.
- AI and Fraud Detection – Many digital wallets use artificial intelligence to detect fraudulent activities, analyze transaction patterns, and enhance security measures.
- What should citizens be careful about?
- Not sharing more information than necessary. The wallet allows selective sharing—this feature should be used wisely.
- Always verifying official apps and platforms to avoid scams or phishing attacks.
- Using strong passwords and enabling two-factor authentication.
- Staying informed about their privacy rights and data protection policies.
- How Transactions Work (TchTarget,2022):
- Adding Funds & Credentials – Users link their bank accounts, credit cards, or other payment methods to their digital wallets. They can also store digital IDs, travel documents, or health records.
- Making Payments – At a checkout terminal, users can pay using their smartphones, smartwatches, or other digital wallet-enabled devices via NFC, QR codes, or online authentication.
- Receiving & Sending Money – Digital wallets allow peer-to-peer (P2P) transactions, enabling users to send and receive money instantly through secure platforms.
- Identity Verification & Access – In government and enterprise settings, digital wallets are used for verifying identities, signing documents electronically, and accessing services securely.

By integrating AI and blockchain technology, digital wallets are becoming more secure, efficient, and widely accepted across different industries and public services.

## 2.2 Digital Identity Connected with Digital Wallets

Digital wallets increasingly rely on digital identity frameworks to ensure secure, personalized, and legally valid transactions. Here's how they are connected:

**Table 6.** How is Digital Identity Connected with Digital Wallets

Digital Identity Function	Role in Digital Wallets
Authentication	Digital IDs verify the user before granting wallet access (e.g., via biometric login or eID verification).
Authorization	Only users with verified digital identities can perform financial operations.
KYC Compliance	Wallet providers use digital identity to fulfill Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements.
Interoperability	A verified digital identity allows users to access various services (e.g., banking, healthcare, tax) through the same wallet.
Security	Digital identity reduces fraud by linking wallet access to biometric or multi-factor authenticated profiles.

*Example: In the EU, digital identity systems like eIDAS (Electronic Identification and Trust Services) are linked to digital wallets, allowing citizens to use the same identity for e-government and financial services.*

### 3.1 Adoption Worldwide

Digital wallets serve as a means of storing identification credentials, financial data, and other important documents electronically. Various countries have implemented or are in the process of implementing digital identity wallets.

#### European Union

European Union: The EU is leading this transition through the development of the European Digital Identity Wallet (EUDI Wallet), which is expected to be available to all citizens, residents, and businesses by the end of 2026 (European Commission, 2024). The EUDI Wallet allows users to store, manage, and share identity credentials and official documents, such as diplomas, health records, and income statements, while enabling features like electronic signatures, secure authentication, and selective data disclosure. One of the core principles of the initiative is user control over personal data, ensuring individuals can decide what information to share, with whom, and for how long.

Announced in June 2021, the project was partly catalyzed by the COVID-19 pandemic, which accelerated the demand for digital public services and secure online identity solutions (Reuters, 2021). Additionally, the initiative aims to reduce dependency on commercial digital wallets provided by tech giants such as Apple, Google, and Thales, which often raise concerns around privacy, surveillance, and data commodification. The European Digital Identity Framework (eIDAS 2.0) and its Architecture and Reference Framework (ARF) provide the technical and legal foundation for the wallet's interoperability across all

Member States. To support implementation, the EU is conducting large-scale pilot projects involving over 350 public and private stakeholders across 26 countries.

The European Commission estimates that widespread adoption of the EUDI Wallet could yield economic benefits of up to €9.6 billion and create approximately 27,000 jobs over five years. The wallet is also expected to improve cybersecurity, reduce administrative costs, and foster cross-border trust in the digital single market.

Some other countries that have made progress in using digital wallets are:

- **United States:** Several states, including Arizona, Georgia, and Maryland, have introduced digital driver's licenses, integrating them into Apple Wallet and Google Wallet (Smith et al., 2022).
- **China:** The Chinese government has promoted digital identification and mobile payment systems, with platforms like Alipay and WeChat Pay dominating the digital transaction landscape (Li & Zhang, 2020).
- **India:** The Aadhaar-based digital identity system allows citizens to access financial and government services seamlessly (Kumar et al., 2021).
- **Estonia:** A leader in e-governance, Estonia's digital ID system facilitates secure transactions, voting, and access to various public and private services (Mets et al., 2019).

### 2.3 Digital Wallet Feasibility in Albania

Albania has made significant strides in digital governance, particularly through e-Albania, the national electronic services platform. According to Muça (2024), the European Union Digital Identity Wallet is a strategic initiative aimed at creating a universal identity verification system that will enable EU citizens to use a single application to access public and private services across the entire bloc. This wallet, expected to be launched in EU countries by the end of 2026, will function as a digital space for storing and selectively sharing official documents and credentials, ensuring privacy and control by the user. The use of this system will be supported by common technical and legal standards, promoting a reliable, secure, and interoperable infrastructure throughout the EU (Muça, 2024).

Albania has made progressive steps toward digital transformation, but digital identity integration with e-wallets is still developing. Some of current developments in Albania are:

- **e-Albania Platform:** Albania has launched e-Albania, a government platform offering over 1,200 digital services. Citizens log in using their national digital ID (ID card or passport), indicating early infrastructure for digital identity.
- **eID and Biometric Passports:** Albania introduced biometric ID cards and passports starting in 2009, which form the foundation for digital identity systems.
- **National Agency for Information Society (AKSHI) and National Agency for Cybersecurity (NAECCS)** are working on digitization and cyber protection, indirectly supporting digital wallet security and identity verification.

However, challenges remain regarding cybersecurity, infrastructure, and public adoption.

- Legal and Regulatory Considerations: Implementing a digital wallet requires clear legal frameworks to address data privacy, identity theft, and interoperability with international standards (European Data Protection Board, 2023).
- Infrastructure and Digital Literacy: While internet penetration has increased, ensuring accessibility across urban and rural areas is crucial (ShqipTech, 2022).
- Public Trust and Security Concerns: Addressing skepticism about data security and government surveillance is essential for widespread adoption (Mehmeti, 2023).
- Limited Integration with Private Wallets: As of 2024, most digital wallets in Albania (e.g., PayLink, EasyPay, or bank apps) rely on basic KYC and are not yet fully integrated with state-issued digital identities.
- No eIDAS-Level Interoperability: Albania is not yet part of the EU's eIDAS digital identity framework, limiting the cross-border use of digital identity and digital wallets.
- Cybersecurity Concerns: With increased digital usage, Albania faces ongoing cyber threats, making digital ID protection critical.

### 3. The Role of AI in Digital Identity and Digital Wallet Implementation

Artificial Intelligence (AI) is rapidly transforming the landscape of digital identity management and digital wallet systems, playing a central role in enabling secure, user-centric, and efficient digital ecosystems. By harnessing the capabilities of machine learning, biometric recognition, context-aware decision-making, and intelligent automation, AI enhances both the security and functionality of digital wallets and the digital identities they depend on.

#### 3.1 AI in Digital Identity Verification

Digital identity is the foundation of secure access to online services, and AI significantly strengthens this foundation. Key contributions include:

- Biometric Authentication: AI enhances identity verification through facial recognition, fingerprint matching, and iris scans. These methods are increasingly accurate and adaptive, reducing the risk of identity fraud (Johnson & Lee, 2021).
- Behavioral Biometrics: AI systems monitor subtle behavioral patterns—such as typing speed, touchscreen interaction, and smartphone tilt—to verify identity continuously in the background.
- Dynamic Risk Assessment: AI algorithms analyze contextual data (e.g., login location, time, and device) to assess risk levels and trigger adaptive authentication steps accordingly. This adaptive behavior increases resilience against sophisticated fraud tactics like impersonation and social engineering.

#### 3.2 AI in Digital Wallet Functionality

- Digital wallets are evolving beyond payment tools into integrated platforms for storing identity credentials, licenses, and verified digital documents. AI supports digital wallets by:
- Fraud Detection and Prevention: AI-powered machine learning models detect anomalies in real-time transactions, flag suspicious behavior, and help prevent unauthorized access (Singh & Patel, 2022). These systems can also be used to

combat authorized push payment fraud, where users are tricked into sending money to fraudsters—a growing threat in the EU.

- Smart Assistance: AI-powered chatbots and virtual agents enhance user experience by guiding users through registration, transactions, and issue resolution (Nguyen et al., 2020).
- Process Automation: AI automates KYC/AML checks, document validation, and data extraction, streamlining onboarding and ensuring regulatory compliance (Brown et al., 2021).
- Personalized Services: AI tailors content and financial advice based on spending patterns and transaction history, helping users manage their digital assets more effectively.

### 3.3 Improving Authentication: The Advantage of AI

In the context of authentication, AI is essential for implementing Multi-Factor Authentication (MFA) and Strong Customer Authentication (SCA) effectively and dynamically. SCA, as mandated by PSD2 and expanded under PSD3/PSR, requires at least two of the following factors to authorize transactions:

- Something the user knows (e.g., password)
- Something the user has (e.g., device or token)
- Something the user is (e.g., biometric data)

While Albania's eAlbania platform currently utilizes basic two-factor methods (NID, password, OTP), it lacks integration of biometric data and adaptive authentication based on AI-powered risk profiling. AI can close this gap by supporting continuous authentication and real-time fraud detection, and by enabling dynamic authentication flows based on user behavior and transaction sensitivity. Table 2 compares the EU Strong Customer Authentication (SCA) under PSD2 with eAlbania's authentication system. EU SCA uses strong multi-factor authentication with high security, biometric support, advanced AI fraud detection, and full cross-border interoperability via eIDAS. In contrast, eAlbania relies mainly on single or two-factor authentication without biometrics, has moderate security, basic fraud tools, limited digital certificate use, and lacks interoperability with EU systems. This highlights the gap between eAlbania and EU standards in authentication security and cross-border integration.

**Table 7.** Comparison – EU SCA vs. eAlbania Authentication

Criteria	EU SCA (PSD2)	eAlbania Authentication
<b>Authentication Model</b>	Multi-Factor Authentication (MFA): At least two of the following: <ul style="list-style-type: none"> <li>● Knowledge (e.g., password)</li> <li>● Possession (e.g., device)</li> <li>● Inherence (e.g., biometrics)</li> </ul>	Primarily single-factor or two-factor authentication using: <ul style="list-style-type: none"> <li>● National ID number (NID)</li> <li>● Password</li> <li>● One-Time Password (OTP) via SMS or email)</li> </ul>
<b>Security Level</b>	High – reduces fraud significantly across the EU	Moderate – secure but not fully PSD2/eIDAS compliant
<b>Biometric Authentication</b>	Supported (e.g., fingerprint, face recognition)	Not implemented

<b>Cross-Border Interoperability</b>	Full, via eIDAS/eIDAS 2.0 and EUDI Wallet	Not yet interoperable with EU digital identity systems
<b>Fraud Detection Tools</b>	Advanced AI-based tools with fraud data sharing (PSD3/PSR)	Basic – lacks AI or cross-border fraud data exchange
<b>Use of Digital Certificates</b>	Yes – supports e-signatures and secure ID	Limited usage

### 3.4 AI and the European Digital Identity Wallet

The upcoming European Digital Identity (EUDI) Wallet incorporates AI to enable:

- Selective Data Disclosure: AI enables users to share only necessary data, enhancing privacy and regulatory compliance.
- Intelligent Document Handling: Through AI, documents such as degrees, licenses, and medical records can be automatically validated and securely transmitted.
- Legally Binding eSignatures: AI helps validate user intent and identity in real time, strengthening the legitimacy and legal value of digital transactions.

Additionally, AI could support the EU-wide fraud detection platform proposed under PSD3, facilitating real-time fraud data exchange among payment service providers. Albania's alignment with this infrastructure could help reduce cross-border fraud, which is currently nine times more prevalent than domestic fraud (European Court of Auditors, 2025).

### 3.5 Strategic Importance for Albania

For Albania, integrating AI into its digital identity and wallet ecosystem is critical to achieving compliance with EU standards, including GDPR, eIDAS 2.0, and the forthcoming EU Digital Identity Wallet. AI can support:

- Biometric login and authentication for eAlbania and future wallets.
- AI-powered fraud detection systems for domestic and cross-border transactions.
- Adaptive authentication models based on behavior, device, and location data.
- Interoperability with EU-wide systems like the EUDI Wallet and fraud-sharing platforms.

Strategic implementation of AI not only strengthens digital infrastructure but also builds citizen trust, improves regulatory alignment, and accelerates Albania's path toward digital EU integration.

Advancements in AI and blockchain for digital identity must be supported by strong cybersecurity measures. Institutions like National Computer Incident Response Team (ALCIRT) and the National Authority for Electronic Certification and Cybersecurity (NAECCS) play a crucial role in strengthening legal frameworks, technical infrastructure, and human capacity in Albania. Without a robust cybersecurity foundation, digital identity solutions cannot fully ensure trust, privacy, and resilience against cyber threats. Albania's alignment with EU regulations such as GDPR and EDPB is essential for its digital transformation and EU integration. A coordinated approach combining advanced digital identity technologies with comprehensive cybersecurity and regional cooperation will enable Albania to build a secure, transparent, and interoperable digital environment for itself and the Western Balkans (Leka & Leka, 2025).

## 4. Conclusions

In this study, we have examined the evolving role of artificial intelligence (AI) and blockchain technology in improving digital identity solutions, focusing on Albania and the challenges it faces in adopting digital wallets in compliance with European Union (EU) standards. Blockchain-based digital identity offers secure, decentralized, and tamper-resistant processes for identity verification, while AI strengthens these systems through biometric authentication, real-time fraud detection, advanced decision-making, and the delivery of personalized user experiences.

The convergence of AI and blockchain technologies has the potential to address critical issues such as identity theft, secure user authentication, and data privacy, while supporting self-sovereign identity management. For Albania, this represents a significant opportunity to modernize digital infrastructure and align more closely with EU regulations, including the General Data Protection Regulation (GDPR), the updated eIDAS 2.0 regulation, and the new Payment Services Directive (PSD3).

Albania is still in the early stages of implementing the EU Digital Identity Wallet. Key challenges include building a sustainable technological infrastructure, developing an effective legal and ethical framework, and strengthening national cybersecurity capabilities. Public education and awareness on the safe and ethical use of digital technologies are also essential to gain citizens' trust and promote widespread adoption.

The EU initiative for the Digital Identity Wallet—which includes biometric authentication, real-time fraud verification, and personal data storage via blockchain—offers transformative potential for Albania. It enables secure, cross-border, and citizen-controlled access to public and private services, supports digital mobility, and promotes transparent and efficient governance. This aligns with the EU's vision of a unified digital space and a citizen-centered digital economy.

### Main benefits:

- Enhanced security through biometric authentication and blockchain technology.
- User privacy via self-sovereign identity.
- Faster access to public and private services.
- Cross-border digital interactions compliant with EU standards.
- Improved fraud detection and risk management through AI.

### Potential challenges:

- Need for a stable legal and regulatory framework harmonized with EU policies.
- Significant investments in technological infrastructure and cybersecurity.
- Public awareness and education on digital identity and privacy risks.
- Ensuring interoperability and cross-border acceptance.
- Managing ethical concerns related to AI and data privacy.

Recent regulatory developments underscore the urgency of addressing these challenges. For example, the U.S. Consumer Financial Protection Bureau (CFPB) has approved regulations expanding oversight of tech giants such as Apple, Google, and Amazon—companies that collectively process over 13 billion digital transactions annually (Gillison, 2024). Similarly, in Europe, the European Court of Auditors (2025) has reported a

significant shift toward the use of digital wallets in retail transactions, emphasizing the need for harmonized standards and consumer protection across member states.

Strategic adoption of AI and blockchain technologies in digital identity systems is essential for Albania's digital transformation. With a coordinated, transparent, and citizen-focused approach, Albania has the potential to become a regional example for secure, interoperable, and EU-aligned digital identity management—thus fulfilling its goals for technological development and European integration.

## References

- 1) Abusam, A., Keesman, K. J., Spanjers, H., Straten, G., & Meinema, K. (2002). Effect of oxidation ditch horizontal velocity on the nitrogen removal process. *European Water Management Online*, EWA 2002.
- 2) Brown, T., et al. (2021). Automating identity verification with AI: Challenges and opportunities. *Journal of Digital Transformation*.
- 3) European Commission. (2021). The European digital identity framework. <https://digital-strategy.ec.europa.eu/en/policies/european-digital-identity>
- 4) European Commission. (2024). European digital identity: A digital identity for all Europeans. [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en)
- 5) European Court of Auditors. (2025). Special report 01/2025: Digital payments in the EU – Progress towards making them safer, faster, and less expensive, despite remaining gaps. Publications Office of the European Union. <https://www.eca.europa.eu/en/publications/SR-2025-01>
- 6) European Data Protection Board. (2023). Regulatory aspects of digital identity systems.
- 7) Fuentes, G. (2024, August 26). Exploring the rise of digital wallets and ensuring customer satisfaction. *Forbes Business Development Council*.
- 8) <https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2024/08/26/exploring-the-rise-of-digital-wallets-and-ensuring-customer-satisfaction/>
- 9) Gillison, D. (2024, November 21). US watchdog issues final rule to supervise Big Tech payments, digital wallets. *Reuters*. <https://www.reuters.com/article/us-watchdog-rule-idUSKBN2XU28T>
- 10) Johnson, M., & Lee, H. (2021). AI in identity management: A security perspective. *Cybersecurity Journal*.
- 11) Kumar, R., et al. (2021). Aadhaar and digital identity in India: Lessons for global adoption. *Technology & Society Journal*.
- 12) Leka, B., & Leka, D. (2025). Advancing cybersecurity through AI: Insights from EU and candidate nations. *Baltic Journal of Modern Computing*, 13(1), 166–176. <https://doi.org/10.22364/bjmc.2025.13.1.09>
- 13) Li, W., & Zhang, Y. (2020). The evolution of digital payments in China: The role of government and private sector collaboration.
- 14) Mane, N. S., & Joshi, P. (2024). Role of AI-based e-wallets in business and financial transactions. *International Research Journal of Humanities and Interdisciplinary*

- Studies (IRJHIS), Special Issue, February 2024.  
<https://www.researchgate.net/publication/377780543>
- 15) McCarthy, N. (2021, June 29). The companies with the most digital wallet complaints. Statista.  
<https://www.statista.com/chart/25192/complaints-about-digital-wallets/>
- 16) Mehmeti, A. (2023). Public perceptions of digital services in Albania. Albanian Journal of Public Administration.
- 17) Mets, K., et al. (2019). E-governance in Estonia: A model for digital identity integration. Public Policy Review.
- 18) Mohamed, A. (2024, November 5). Digital wallets and AI: Creating smarter, safer online transactions.  
<https://blogs.oregonstate.edu/nexus/2024/11/05/digital-wallets-and-ai-creating-smarter-safer-online-transactions/>
- 19) Muça, E. (2024). Planet e BE-së për një portofol universal identiteti dixhital.  
<https://businessmag.al/nje-portofol-universal-identiteti-dixhital-ne-planet-e-be-se/>
- 20) Nguyen, T., et al. (2020). AI-powered chatbots in digital government services. Digital Governance Review.
- 21) OpenAI. (2025). Key Components of Digital Wallets [AI-generated figure].  
<https://openai.com>
- 22) Reuters. (2021). EU to push digital transformation with digital identity wallet.  
<https://www.reuters.com>
- 23) Salazar, R. H. (2017). Apple Pay & digital wallets in Mexico and the United States: Illusion or financial revolution? IJ Journal, 18, 10775.  
<https://doi.org/10.22201/ij.24485306e.2017.18.10775>
- 24) Singh, P., & Patel, S. (2022). Machine learning approaches for cybersecurity in digital transactions. AI & Security Review.
- 25) ShqipTech. (2022). Digital infrastructure and e-government in Albania.  
<https://shqiptech.al>
- 26) Smith, J., et al. (2022). Digital wallets in the United States: Trends and policy considerations. Financial Innovation Journal.
- 27) TechTarget. (2022). Digital wallet. TechTarget.  
<https://www.techtarget.com/whatis/definition/digital-wallet>