BLOCKCHAIN
TÜRKİYE

DIGITAL IDENTITY SYSTEMS AND THEIR SECTORAL IMPACTS
REPORT

On-Chain
Çalışma Grubu

JUNE 2025

TBV
TÜRKİYE BİLİŞİM VAKFI

BLOCKCHAIN
TÜRKİYE

Digital Identity Systems and Their Sectoral Impacts Report

On-Chain
Çalışma Grubu

JUNE 2025

TBV
TÜRKİYE BİLİŞİM VAKFI

DIGITAL IDENTITY SYSTEMS AND THEIR SECTORAL IMPACTS REPORT

JUNE 2025

DISCLAIMER

This report, prepared by the "On-Chain Working Group" of the Blockchain Turkey Platform operating under the Turkish Informatics Foundation, examines blockchain technology in terms of current personal data protection legislation and practices. Its technical scope is intended to facilitate the legal understanding of the technology. It does not constitute binding advice or opinion for individuals or institutions. This report contains information obtained from publicly available sources, and the accuracy or completeness of such information is not guaranteed. All information and opinions provided in this report are subject to change over time. In this context, the author assumes no responsibility or liability to readers of this report or any third party.

On-Chain
Çalışma Grubu

FOREWORD

Digital identity is not merely a technical transformation area of the 21st century, but also a global paradigm shift where individual sovereignty, data security, and digital rights are being redefined. This study examines digital identity systems not only from a technical perspective, but also through a multidimensional and interdisciplinary approach. It covers a wide range of topics, from identity management models to W3C and ISO standards, from blockchain-based infrastructures to security issues, from user experience design to hardware components, and from legal regulations to international examples. Digital identity scenarios in various sectors such as finance, public services, healthcare, and education have been examined in detail; a comprehensive assessment of the system's operation has been provided from the perspective of both corporate actors and individuals.

The evolution from centralized structures to user-sovereign systems is opening the doors to a new era with the promise of placing control of identity in the hands of individuals in the digital world. Blockchain-based architectures, zero-knowledge proof technologies, and decentralized identifiers now make it possible to establish trust beyond borders. This means not only the digitization of services, but also digital citizenship and digital economies rebuilt around identity.

The report published as part of the Central Bank of the Republic of Turkey's Digital Turkish Lira (Digital TL) project clearly highlights the importance of the Digital Identity infrastructure. For the Digital TL to work in an integrated manner with digital wallets, payment systems, and identity verification mechanisms, reliable and interoperable digital identity systems are required. In this context, digital identity solutions are considered a critical fundamental component in establishing trust, providing verification, and protecting user privacy within the architecture of the Digital TL.

In the coming years, digital identity solutions will become the cornerstone not only of financial systems but also of healthcare platforms, educational access, and even AI-based autonomous systems. New-generation business models will be built on these infrastructures, where identity verification can be performed instantly, securely, and in a user-centric manner. This transformation will fundamentally change not only how individuals but also how governments and companies trust each other.
From Turkey's perspective, the adoption of digital identity systems is not merely a technological advancement; it is an opportunity for transformation in terms of the transparency of public services, the efficiency of the private sector, and the privacy rights of individuals. Turkey's strong public infrastructure, young population, and rapidly digitizing sectors hold great potential for producing globally exemplary solutions in this field.

This report addresses many critical topics, from regulatory compliance to international standards, security threats to user experience, while also setting out a strategic vision for Turkey to take its place in global competition in the field of digital identity.
We believe that inclusive, secure, and sustainable digital identity systems will not only solve today's problems but also form the fundamental infrastructure of tomorrow's digital economy.

Finally, a governance model that further strengthens cooperation between the public and private sectors is required for the healthy functioning of the digital identity ecosystem. It is essential for the sustainability of the ecosystem that current regulations meet the needs of the digital age, that preventive legislation is developed against new security threats, and that digital identity is accepted as an interoperable standard across all sectors. This report has been written not only to understand today, but also as a roadmap to shape the future.

Dr. Gökhan Özdinç, Chief Technology Officer, Yapı Kredi

CONTENTS

EXECUTIVE SUMMARY

The global digitalization process has brought with it the need for a fundamental transformation in identity verification mechanisms. This report presents a multi-layered framework that addresses the concept of digital identity not only as a technological tool but also in terms of data security, user privacy, regulatory compliance, and digital sovereignty. On-chain, or blockchain-based, digital identity systems empower users to strengthen their control over their identity information while also providing organizations with the opportunity to create more sustainable, secure, and flexible identity verification infrastructures.

Among the models featured in the report, the most notable structure is user-sovereign digital identity systems. Users decide for themselves what information about their identity to share with whom, thereby enabling more privacy-friendly solutions based on the principle of data minimization. The foundation of this new architecture is built on the transparency, immutability, and reliability provided by blockchain technology.

Now that digital identity has become applicable not only for individuals but also for institutions, devices, service providers, and even artificial intelligence components, interoperability and international validity have become critical needs.

The report also examines examples of the applicability of digital identity across various sectors, from public institutions to the private sector, banking to education, and healthcare to real estate. The system's functionality was evaluated through scenarios involving mobile applications, hardware wallets, and IoT devices that directly impact the user experience.
The security aspect stands out as a vital element in terms of the system's sustainability. Despite the strong protection mechanisms offered by the blockchain architecture, corporate awareness, technical competence, and continuously updated control mechanisms are essential against new types of threats.
At this point, the report clearly outlines the measures that need to be taken, covering a wide range of issues from cyberattacks to user errors.

The importance of legal compliance is emphasized; by establishing a bridge between Turkey's KVKK and the European Union's GDPR and eIDAS regulations, it explains how digital identity should be positioned within the legal context.
Regulation-compliant system design and governance models based on user rights are considered indispensable for the success of the digital identity ecosystem.

Digital identities have many potential uses beyond the financial sector. The report illustrates various sectoral applications with examples, ranging from public services to the tokenization of real-world assets, the management and verification of educational and academic information, the use of tourism and travel technologies, and rapid and comprehensive access to data in the healthcare sector.

Digital identity is not merely a key that unlocks digital services; it is a strategic asset that safeguards the security, reputation, and sovereignty of individuals and institutions in the digital age. Therefore, a holistic approach is needed that addresses technological developments alongside ethical, legal, and governance dimensions. Blockchain-based digital identity systems offer significant opportunities for both the public and private sectors with their secure, interoperable, and user-centric structures. Turkey's effective adoption of these technologies will both enhance citizen data security and accelerate the transition to a digital economy.

Ali Akarçay
Yapı Kredi Technology
Manager of Individual Customer
Process Management and Business
Development

1. INTRODUCTION

This comprehensive report details the conceptual framework, technological building blocks, legal regulations, and application examples across different sectors of digital identity systems. Digital identities form the basis of identity verification processes for individuals and organizations in digital environments.

This report provides a comparative analysis of centralized, federated, and user-sovereign systems, outlines legal compliance requirements in light of global standards and regulations, and details application scenarios in areas such as public administration, finance, education, and real estate.

Digital identity and the digitization of documents play a key role in the digital transformation processes of modern societies. This transformation makes identity verification and document management processes faster, more secure, and more efficient for individuals, institutions, and organizations. In particular, this report aims to assess the legal compliance of digital identity applications in light of the current legal framework and international regulations in Turkey and to offer recommendations for the effective adoption of this technology.

2. THE CONCEPT OF DIGITAL IDENTITY

Digital Identity is defined as identity information that identifies an entity in a virtual environment and can be interpreted by software.

Identity Management Systems (IdM) are systems that regulate user access to digital resources and provide identity verification, authorization, and security. IdM manages user identity information and provides access controls based on these identities.

2.1. Digital Identity Management Models

2.1.1. Centralized Identity Management

Central identity management is a model in which users are registered in a single central database and their access rights are controlled by a central system. The foundations of this model date back to the mid-1990s and it has become widespread, particularly with the development of technologies such as Active Directory and LDAP (Lightweight Directory Access Protocol).

- Single Identity Source: User identity information is stored in a central database.
- Simplified Management: User accounts and access permissions are managed from a central point.
- Comprehensive Access Control: System administrators centrally control user access levels and permissions.
- Customized Identity Verification: Users are verified through a central identity verification service (e.g., Active Directory or LDAP).

2.1.2. Federated Identity Management

Federated identity management enables the sharing of identities between different organizations or service providers. This model has gained popularity, especially with the proliferation of cloud services and system integrations. Single Sign-On (SSO) technologies and SAML (Security Assertion Markup Language) protocols have laid the foundations for federated identity management.

- Identity Sharing: allows users to access both systems with the same identity.

• Single Sign-On (SSO): After logging in once, users can move between different systems and services without having to re-authenticate.

• Compatibility with External Sources: Secure identity verification processes are provided between different organizations or service providers.

• Protocols: Managed using protocols commonly used in federated identity management, such as SAML, OpenID Connect, and OAuth.

2.1.3. User-Centric Identity Management

User-centric identity management is an approach where users have control over their own identity information. This model has been gaining popularity since the late 2010s.

• User Control: Users manage their own identity information and have full control over authentication processes.

• Data Ownership: Users utilize computing infrastructures that store access permissions.

• Customizable Identities: Users can customize their identity information and verification processes.

• Privacy: Users can share only the necessary information with the people they choose. (Selective Disclosure).

2.1.4. Self-Sovereign Identity Management

Among digital identity management models, the Self-Sovereign Identity model, which has been gaining prominence since 2015, is a model that eliminates dependence on third-party infrastructures in terms of compliance with KVKK regulations and interoperability.

In the SSI model, identity information is controlled by the individual or organization to which it belongs. This model was proposed in 2005 and has rapidly evolved since 2015.

A blockchain-based identity management system does not require central authorities to verify individuals' identities. By eliminating intermediaries, it enables individuals to have full control over their identities. Identity owners can share their identity information in any amount and detail they choose. In the SSI model, an individual's identity information is not specific to any software or system and can be transferred and used across different platforms and services.

The system can provide digital identity certificates that can be used in digital environments, are cryptographically verifiable, and cannot be counterfeited.

Instead of processes that require human intervention and depend on reliable third parties, it becomes possible to implement more autonomous processes in which humans, companies, and smart devices can participate. Currently, services running on password-protected electronic platforms can be made more secure through digital wallets and can be run autonomously by software without requiring human intervention on the part of corporate entities.

In this model, the blockchain system plays a key role in establishing mutual trust among all parties through the information it holds. Since trust does not originate from any central authority, cross-sector and cross-border digital identity applications become possible.

3. TECHNOLOGY AND INFRASTRUCTURE STANDARDS

3.1. Current Standards

3.1.1. World Wide Web Consortium (W3C)

In this model standardized by the W3C (World Wide Web Consortium), identities consist of two main types of data: a number that uniquely identifies the entity called a Decentralized Identifier (DID) and verifiable credentials (VCs). DIDs are associated with an asymmetric key pair, similar to cryptocurrency wallet addresses. VCs are certificates cryptographically signed by an identity provider, containing various identity details about the person or organization that issued them.

Decentralized Identifiers (DIDs): DIDs (Decentralized Identifiers) are identifiers that represent a person or digital asset. These identifiers are defined in URI format and are associated with a DID document (diddoc) that represents the identity of the relevant person. DID documents may contain cryptographic keys, verification methods, and some service definitions. These elements enable the person managing the identity (DID controller) to authorize and verify that identity.

Verifiable Credentials Data Model - Verifiable Credentials (VCs): A standard proposed by the W3C to reliably represent digital identity information. It provides a mechanism for expressing the credentials we use in our daily lives (e.g., driver's licenses, university diplomas, passports) in a cryptographically secure, privacy-preserving, and machine-verifiable manner in a digital environment. This model includes the following roles:

1. Holder: The party that can generate its own DID values, possess verifiable identity information obtained from the issuer, and prove this information to other actors.
2. Issuer: The party that creates verifiable identity information.
3. Subject: An asset subject to claims (such as ownership).
4. Verifier: The party that verifies one or more verifiable identity details provided by the identity holder.
5. Verifiable Data Registry: A system that manages the identifiers and keys necessary to use verifiable identity information.

3.1.2. OpenWallet

OpenID4VCI (Verifiable Credential Issuance): OpenID4VCI is an API standard that enables digital identity providers to issue verifiable credentials (VC) to users. In this system, identity data is structured according to a predefined format and cryptographically assigned to its owner. This data is securely transmitted under OAuth protection.

Identity information can be securely and verifiably presented by the end user, even without the direct involvement of the owner. Access to the API is securely authorized using the OAuth 2.0 protocol. This ensures that the creation and transmission of identity information are protected by the security infrastructure provided by OAuth 2.0.

OpenID4VP (Verifiable Presentation): OpenID4VP is a standard that enables users to present their identity information in a verifiable manner. This structure is also built on OAuth 2.0, and the user has complete control over who sees the identity data, how much is shown, and when it is displayed. Thanks to its developer-friendly nature, flexible structure, and secure presentation layer, it is used as the fundamental protocol for digital identity presentation.

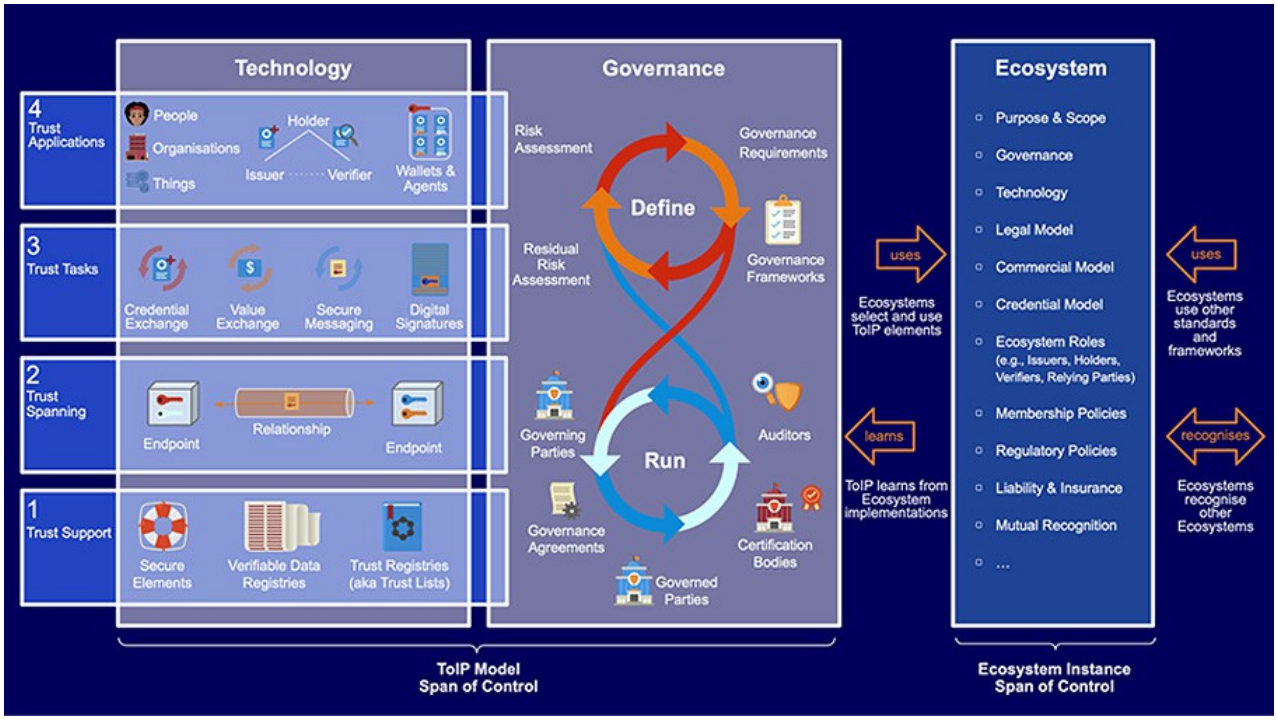
3.1.3. ISO Standards

• ISO/TR 23244:2020: This standard provides an overview of privacy and the protection of personally identifiable information (PII) applied to blockchain and ledger technology systems.

• ISO/TR 23249:2022: This standard provides an overview of existing DLT systems for identity management; for example, it explains the mechanisms by which one or more entities can create, receive, modify, use, and revoke a set of identity attributes.

• ISO/TR 23644:2023: This standard covers concepts and issues related to the use of trust anchors in systems that leverage blockchain and ledger technologies for identity management; for example, it explains the mechanisms by which one or more entities can create, receive, modify, use, and revoke a set of identity attributes.

• ISO/IEC 23220-1:2023: This standard specifies general system architectures and lifecycle stages for mobile eID system infrastructures in terms of building blocks; it standardizes interfaces and services for mobile authentication applications. It applies to organizations involved in partially or fully defining, creating the architecture, designing, testing, maintaining, managing, and operating a mobile eID system.



1 The Support Layer enables the secure storage of data that facilitates the verification of identity data, allows data to be found, and enables verification processes to function.

2 The Communication Layer provides secure communication between digital identity wallets, offering secure protocols and interoperability.

3 The Task Protocols Layer includes the processes of creating, proving, verifying, revoking, and sharing the user's identity certificates.

4 The Applications Layer contains industry-specific business processes and includes applications that operate based on digital identities. This layer also defines governance frameworks, such as who will issue which type of identity certificate in each industry, how these certificates will be verified, and how they will be revoked.

This layered structure enables the development of digital identity systems worldwide based on a common model and in an interoperable manner. Thanks to the isolation of the layers, products in each layer can be developed independently of the technologies in other layers.

Governance protocols that concern all layers cover policies, stakeholders, contracts, certifying authorities, auditors, and governance frameworks.

3.2. Communities

Certification Authority Browser Forum: This forum is a global collaboration platform that defines the rules for how X.509 v3 digital certificates are created and managed. X.509 v3 certificates are a global collaboration platform that defines the rules for how X.509 v3 digital certificates are created and managed. X.509 v3 certificates are a global collaboration platform that defines the rules for how X.509 v3 digital certificates are created and managed. X.509 v3 digital certificates, which enable secure communication in the digital world. X.509 v3 certificates are an international security standard used to verify the identity of individuals, organizations, and systems on the internet. They are frequently used in establishing HTTPS connections on websites, software signing, and email security.

The CA/Browser Forum is a voluntary community consisting of certificate authorities (CAs), web browser manufacturers, operating system developers, and other security software manufacturers. The guidelines established by this forum ensure the creation of a secure and standard-compliant "chain of trust" in applications such as TLS (Transport Layer Security), code signing, and S/MIME.

Cloud Signature Consortium (CSC): A global group consisting of industry, government, and academic organizations that aims to standardize highly secure and compliant digital signatures in the cloud. They enable the creation of remote signatures using REST/JSON API.

Financial Action Task Force (FATF): Established in 1989 as a G7 initiative, it is an intergovernmental organization that develops policies to combat money laundering. The Digital Identity Guide aims to assist governments, regulated entities, and other relevant stakeholders in how digital identity systems can be used in customer verification processes.

FIDO: An open industry consortium founded in February 2013 with a mission to "develop and promote authentication standards that help reduce the world's over-reliance on passwords."

Internet Engineering Task Force (IETF): An open and voluntary organization that sets the technical standards guiding the development of the Internet. It publishes technical documents that are widely accepted in areas such as electronic signatures, PKI (public key infrastructure), and secure communication. These documents are standard documents called RFCs (Request for Comments).
RFCs define how Internet protocols work, evolve over time, and are updated according to new technologies. For example, the technical definitions of common security protocols such as TLS (Transport Layer Security) or OAuth are also provided in these documents.

Organization for the Advancement of Structured Information Standards (OASIS): OASIS is a non-profit international consortium that develops open and interoperable technical standards in areas such as information security, digital identity, blockchain, IoT, and emergency management. Although initially founded by software manufacturers, academic institutions, civil society organizations, and various public agencies have since become members. It has particularly supported the development of solutions that are compatible with publicly supported projects and regulations in areas such as digital signatures, electronic documents, and identity verification.

Among OASIS's work is the standard package titled "Digital Signature Service Basic Protocols, Elements, and Links," which defines the technical foundations of digital signatures. These documents contribute to the creation of secure and standard-compliant digital signature infrastructures by defining how digital signature operations are performed, which data structures are used, and how interoperability between systems is achieved.

3.3. Infrastructure Examples Around the World

Digital identity infrastructures enable users to securely manage their own identity information and share their data only with authorized individuals and organizations. These systems protect user data, offering more secure and efficient solutions across numerous sectors such as banking, healthcare, education, and government services. Projects such as Sovrin, SSI Turkey, and Cheqd are examples of infrastructure that play an important role in digital identity management and verification processes.

3.3.1. Sovrin

The Sovrin Foundation is an infrastructure provider for decentralized digital identity systems. Built on blockchain technology, Sovrin allows users to manage their identity information without relying on any central authority. This model enables individuals to fully control their identity information.

Key features:

- Self-Sovereign Identity (SSI): Users manage their own identity information and do not need a central intermediary.
- Infrastructure: The Sovrin network uses blockchain to ensure data is stored securely and transparently.
- Data Security: Identity data remains solely under the control of users, reducing the risk of data breaches.

Sovrin provides a secure digital identity verification system by protecting users' digital identities. The process of sharing identity information with third parties is entirely under user control and does not require a central authority.

3.3.2. SSI Turkey

SSI Turkey is one of the pioneering projects in Turkey in the field of digital identity verification. Supported by public institutions and the private sector in Turkey, this initiative enables citizens and users to verify their identity information securely and in a decentralized manner.

Key features:

- Data Protection: Identity data is stored in individuals' digital wallets and is only shared when necessary.
- Public and Private Sector Collaboration: Ensures secure identity verification in both the public and private sectors by working in compliance with Turkey's legal frameworks.
- Legal Compliance: Infrastructures have been developed in compliance with Turkey's personal data protection laws.

SSI Turkey offers significant advantages in digital identity verification processes, particularly in government services, banking, and healthcare.
It is crucial for data security and privacy that users can securely verify their identity information and share their data only with authorized individuals.

3.3.3. Cheqd

Cheqd is another important blockchain-based project that enables the secure management of digital identities. Cheqd, which allows users to verify their data in a decentralized manner, stands out especially in terms of Self-Sovereign Identity (SSI) solutions.

Key features:

- Data Ownership: Users store their identity information in their own digital wallets and share it only with those they authorize.
- Decentralized Infrastructure: Thanks to its technology, identity verification processes are carried out quickly and reliably.
- Privacy and Security: Cheqd is fully compliant with data privacy laws such as GDPR and protects user data.

Cheqd offers digital identity infrastructures that are compliant with privacy regulations, particularly in Europe, and gives users complete control over their data. This allows individuals to manage their identity verification processes quickly and securely.

3.3.4. uPort

uPort is a project built on Ethereum for creating, verifying, and managing decentralized digital identities.
It allows users to fully control their digital identities and enables identity verification without the need for any central authority.

Key features:

- User Control: uPort enables users to store their identity information themselves and perform identity verification in a decentralized manner.
- Integration: Using Ethereum, it ensures that data is stored in an encrypted and secure manner.
- Wide Range of Applications: uPort can be used for secure identity verification and data sharing in sectors such as finance, healthcare, and education.

uPort is a widely used Ethereum-based infrastructure for digital identity management. In addition to identity verification, it secures users' access to digital services.

3.3.5. Microsoft Entra ID

Microsoft Entra is an infrastructure that provides verifiable credentials and decentralized identity creation tools compatible with the World Wide Web Consortium's self-sovereign identity standards, enabling organizations to establish their own identity and access management governance rules and processes.
It was developed as a result of Microsoft's Decentralized Identity strategy to enable organizations to design their own self-sovereign identity management systems.

Key features:

- Enterprise Identity Management: Provides a decentralized identity verification system for companies and organizations.
- Data Privacy: Users retain control over their identity information and only share the information that is necessary.
- Agnostic: It is not designed to work with any specific protocol.

This system is developed specifically for large companies and organizations, and is a solution that prioritizes data privacy and security.

3.3.6. Evernym

Evernym produces tools that enable the development of digital identity management applications compliant with self-sovereign identity (SSI) standards. Evernym offers a decentralized protocol called Verity for the issuance and verification of verifiable credentials.

It has developed the Connect.Me digital identity wallet product to enable users to store and use their digital identities.

Evernym is a private company founded by the creators of the Sovrin Foundation and the Hyperledger Indy protocol.

Key features:

- Ready-to-use SSI tools for organizations: Offers the Verity protocol and Connect.Me wallet for developing identity management applications compliant with SSI standards.
- ZKP application: Uses privacy-focused zero-knowledge proof methods for sharing and verifying identity information.
- Hyperledger Indy: Evernym digital identity applications and development tools are compatible with the Hyperledger Indy protocol.
- Evernym offers a solution that enables secure and fast identity verification processes in the healthcare, education, and finance sectors.

3.3.7. ID2020

One of the sustainable development goals within the United Nations Sustainable Development Agenda, published in late 2015, is to provide legal identity for everyone by 2030. John Edge, a social entrepreneur specializing in financial technology and digital identity, was inspired by this goal and spearheaded the founding of the ID2020 alliance.

ID2020 is a non-profit public-private partnership seeking solutions for the 1.1 billion people worldwide who lack any officially recognized form of identification. It aims to provide digital identity to individuals without identification globally.
It develops digital identity solutions specifically for refugees, displaced persons, and individuals without identity documents.

Using blockchain technology, it ensures the secure storage and verification of personal information.

Key features:

- Governance model: The ID2020 initiative is structured to ensure that digital identity systems are developed in accordance with the principles of privacy, user control, and interoperability. Within this framework, the system's operation is guided by an advisory board and monitored through an independent certification program that evaluates the compliance of identity solutions with the defined principles. This ensures that digital identity providers offer reliable, transparent, and standards-compliant services.
- Technology agnostic: ID2020 does not specifically offer a digital identity technology infrastructure. However, it supports the use of blockchain networks in accordance with SSI standards.
- Socially focused: It provides solutions to identity verification problems, especially for disadvantaged groups.

ID2020 is supported by the United Nations and major technology companies and aims to promote the widespread adoption of digital identity systems worldwide.

3.3.8. IBM Digital Credentials and Blockchain Platform

IBM Digital Credentials and Blockchain Platform provides an infrastructure developed for corporate organizations to manage identity management in a decentralized manner using digital identity tools (Digital Credentials). It is a flexible platform built on Hyperledger Fabric to meet the compliance and expansion requirements of organizations.

Key features:

- Compliant decentralization: The IBM Blockchain Platform leverages the advantages of decentralized technologies for user-controlled identity management while supporting organizations in implementing applications that comply with their process controls.

- Support for flexible consensus mechanisms: Supports the implementation of different consensus mechanisms tailored to the needs of organizations.

- Cross-chain interoperability: Digital Credentials are designed to support communication between different institutions and digital identity management systems. This simplifies identity information sharing and creates a chain of trust between wallets and corporate systems.

3.3.9. Veres One

Veres One is a blockchain specifically built by Digital Bazaar for decentralized identifiers (DIDs). Veres One's operational model ensures transparency, prevents attacks on the network, and financially rewards individuals and organizations that choose to run the software to secure the network. The Veres One network is global and open to the public; anyone can participate.

Key features:

- Individuals and organizations creating and managing their own identities: The mission of the Veres One project is to provide ecosystem governance to enable everyone in the world to create and manage their own decentralized identifiers.

- Interoperable across networks: Veres One is 100% compatible regardless of which wallet application is used.

- Participant incentive model: The Veres One Network is designed as a self-sustaining global public service with an appropriate economic incentive balance for joining and protecting the network.

Digital identity management is rapidly evolving with the decentralized solutions offered by technology. These projects enable individuals and organizations to manage their identity information securely and in a decentralized manner, while providing solutions for important issues such as data security and privacy. Projects such as Sovrin, SSI Turkey, Cheqd, uPort, Microsoft Decentralized Identity, Evernym, ID2020, and IBM Blockchain Identity are prominent examples of infrastructure in the field of digital identity technologies. This infrastructure enables secure digital identity verification processes and allows individuals to have more say in the digital world.

3.3.10. PrivadoID (PolygonID)

It aims to prevent the disclosure of personal data by using zero-knowledge proof technology in digital identity verification. This technology allows users to prove that a piece of information is correct without sharing the information itself. Users retain control of their data while providing only minimal information to the verification mechanism during authentication. This approach offers a significant advantage, especially for projects requiring privacy and data security.

3.3.11. WorldID (Worldcoin)

It focuses on human verification using biometric authentication methods. The project emphasizes that distinguishing humans from AI will become increasingly difficult in the future and uses iris scanning technology to uniquely verify individuals' identities.

Iris scans enable verification in decentralized structures by encrypting each user's unique biometric data through hash values. This solution creates an effective security mechanism against fake accounts and bot attacks.

3.4. Experience Designs Across Different Channels

Blockchain-based digital identity management systems can operate with different logics in different scenarios. Determining the most suitable scenario based on need is only possible with the appropriate hardware. The components on this hardware directly affect the capacity and flow of the application. For this reason, experience designs will be examined in 4 different groups.

3.4.1. Mobile Hardware

Smartphones, watches, and tablets are examples of portable devices that fall into this category. The advantages of these devices include portability, ease of use, and ease of integration with other applications, while their disadvantages include limited processing power, connectivity issues, and security concerns.

Different experiences can be designed depending on the environment interacted with using the wallet application loaded onto mobile hardware.

- Mobile: In general, this category can be divided into scenarios on the same device and scenarios on different mobile devices. Scenarios in different mobile device environments are operated similarly to the web scenarios described in the next section, while app-to-app deep linking stands out in scenarios occurring on the same device.

- Web: It is one of the most popular channels used with mobile devices. It mostly utilizes technologies such as QR codes or barcodes. It requires a second device such as a laptop or desktop computer. In identity creation and verification processes, the codes generated on the second device are completed through interaction with the mobile device camera. However, if both devices have the appropriate components, it is also possible to use technologies such as Bluetooth and NFC.

- Other Integrations: Interactions other than computers, laptops, tablets, and mobile devices fall into this category. Examples include various security points, IoT devices, etc. Depending on the components in both interacting devices, the flow can be executed using QR codes, barcodes, Bluetooth, NFC, and other technologies.

During all these processes, additional security layers can be added thanks to the components on mobile devices. Examples include 2FA, MFA, biometrics (fingerprint, facial recognition, etc.), and pin codes. However, the limited processing power of these devices may be insufficient during complex encryption processes, resulting in lengthy operations. Furthermore, the system may become inoperable in cases such as device malfunction, theft, or battery depletion.

3.4.2. Desktops and Laptops

The main disadvantage of desktop computers and laptops compared to mobile devices is that they are not easily portable and usable. However, they can offer certain advantages in terms of processing power that mobile devices do not provide. On the other hand, technologies such as Bluetooth and NFC can also be used when the devices are suitable for use.

These types of devices are typically used as secondary devices in digital identity creation processes.

Digital identities created on laptops via service providers are transferred to mobile devices via QR codes, enabling the use of digital identities in daily transactions via mobile. Although not yet widespread, digital identity holders can also use the identity data they possess on their laptops to interact with external devices and mobile devices via desktop applications or browser wallets with internet access that can be developed. Again, at this stage, a secondary device open to a solution such as Bluetooth will be needed to transfer identity information to the laptop. Considering the disadvantage of portability, this may not be very appealing, but it can offer a more secure and faster transaction process compared to mobile devices. This category, which evaluates desktop computers and laptops, can cover both web-based applications and desktop applications.

- Desktop Applications: Designed for desktop computers and laptops, these types of applications generally offer high processing power and advanced security features, as well as a high-quality user interface. They reduce the risk of data theft in offline environments. However, they can be considered limited in terms of portability and can only be used on certain types of computers.

- Browser Applications: These applications, accessed through web browsers, offer broader device compatibility. While they provide the advantages of fast use and accessibility, they typically have a limited user interface. Storing keys in the browser's local storage area creates potential security risks.

3.4.3. Hardware Wallets

They perform critical functions such as generating DID values for each user's private keys, encryption, and signing. Hardware wallets can be used to securely store these keys, which enable users to have a unique identifier in the digital identity infrastructure. Hardware wallets are divided into two types based on usability and access differences: passive and active.

Passive hardware wallets are typically devices that are offline or have limited connectivity. These hardware wallets are designed to store the private key for the user's digital identity security. Encryption and signing operations using the private key within an isolated hardware and software environment will take place within the digital identity's experience channels. Although they can securely store multiple identities owned by the user, problems may arise in terms of ease of use and integration. Interaction with other devices such as mobile phones and computers can be achieved via USB, camera, NFC, etc., but since access to other devices and the internet will be limited, usage scenarios may be more limited compared to other methods. Furthermore, even though it offers a more secure solution, it may not be preferred because it creates a carrying difficulty for the user and can also be costly. On the other hand, due to their passive nature, these devices do not require an energy source (e.g., battery) on themselves and do not need to be charged like active devices.

Active hardware wallets are devices that can directly access the network via an internet connection and also interact with mobile devices or computers (via Bluetooth, Wi-Fi). Since digital identity wallets are PKI-based, signing and encryption processes will be performed using the private key securely stored within the active hardware wallet.

While users experience the possibilities offered by digital identity using applications on their mobile devices or computers, they will be in a more secure flow with hardware wallets. As with other experience channels, attention should be paid to security vulnerabilities in the flow compared to passive hardware wallets.

3.4.4. Other Integrations

In addition to those mentioned earlier, devices that could fall under the scope of IoT, such as automobiles, home systems, and machines used in manufacturing, are included in this group. The vision here is to achieve a decentralized and reliable process involving different actors in a standardized, paperless, and error-free manner. In scenarios where sector-specific solutions will be produced, such as energy and supply chain, integration ease, secure data transfer, and verifiability can be achieved through digital identity management established on IoT devices. While the advantages of these devices are ease of use and acceleration of the process, limited use cases, connectivity, and security issues can be considered disadvantages. With the digital identity wallet that will be included in the mentioned IoT devices, many experience flows can be designed in different areas of use.

While the digital identity holder is the final decision-maker for all actions, IoT devices in other integrations can act autonomously as issuers or verifiers. The connection between interacting devices can be established via QR code, NFC, Bluetooth, or wireless network, depending on the device's capabilities. Along with ensuring a reliable and verifiable data flow, ease of use will also be provided.

4. SECURITY AND PRIVACY

Blockchain technologies, which have evolved as an implementation method of distributed ledger technologies, can store records/transactions in a distributed manner at multiple points using a consensus mechanism. Thus, all records are stored on a distributed network with the participation of members, without intermediaries, instead of being stored in centralized databases that require high security.
Data blocks containing transaction records are linked together in a chain using cryptographic mechanisms. Since each block contains the unique cryptographic hash of the previous block, the transactions recorded within are irreversibly and immutably recorded in decentralized ledgers. The blocks form a virtually unalterable chain that any user can examine. All transactions in the blocks are verified and approved by a consensus mechanism to ensure they are correct and valid. There is no single point of failure in this system, and no single user can alter the transaction records.
However, there are specific security threats associated with blockchain technologies, and companies adopting public/private solutions should carefully evaluate these security threats and vulnerabilities.

4.1. Cyber Attacks

A 2023 study by CACI identified the three most common types of cyber attacks encountered in their technologies. These are:
Exchange Attacks: Cryptocurrency exchanges are frequently attacked due to vulnerabilities in smart contracts and cross-chain bridges (IBC). Since 2012, at least 46 cryptocurrency exchanges have been affected by attacks, resulting in the theft of approximately $10 billion worth of crypto assets. Bybit suffered the most costly crypto attack in history in February 2025, resulting in a loss of approximately
1.5 billion USD in losses.

DeFi Attacks: Decentralized finance platforms are targeted by attackers who exploit security vulnerabilities, particularly in validator nodes and key management systems.

Ransomware: These attacks, which lock critical systems and demand ransom, affect many sectors.

In addition to these types of attacks, a research group examined security vulnerabilities in blockchain systems between 2009 and 2017 and listed blockchain security risks in approximately nine categories. According to this source, the most significant threats and attack types are listed below.

Phishing attacks: Traditionally, all phishing attacks can be divided into two types: social engineering methods and technical methods.
Social engineering methods rely on deceiving the victim and then causing them to perform erroneous actions on their own. Attackers using social engineering techniques can obtain users' credentials, install malicious software on user devices, and obtain recovery phrases created during the setup of crypto wallets with private keys. These recovery phrases allow users to access their wallets when they forget their passwords or lose their devices.
Technical methods mostly exploit software vulnerabilities in infrastructures or smart contracts. Examples include DNS-based phishing attacks, cookie hijacking, keylogger usage, etc.

Sybil attacks: This attack involves creating multiple fake identities on a network in an attempt to damage it. In such attacks, the attacker creates numerous fake nodes and attempts to control the network and manipulate block verification processes. In blockchain systems, such attacks threaten the reliability of the distributed ledger, creating security vulnerabilities in the system and potentially weakening consensus mechanisms.

Delays in block waiting times can lead to double spending.

51% attacks: This attack means that the majority of a blockchain network conspires against the minority. Such attacks have been seen in incidents on platforms such as Ethereum Classic, Verge Currency, and ZenCash (now Horizen). In a 51% attack, a malicious miner or group of miners can control more than 51% of the network's processing power and make changes to the blockchain. The controlling party can block transactions, halt payments, reverse transactions, or double-spend. Double spending is a type of fraud that occurs when the same cryptocurrency is used in multiple transactions.

Routing attacks: A routing attack is a type of cyber attack carried out at the internet service provider (ISP) level that affects the uptime or participation of web-based systems. In this attack, attackers split the network into two or more separate components and create parallel blockchains by blocking communication between specific nodes. When the attack ends, all blocks and related transactions produced on the smaller chain are invalidated, resulting in a loss of miners' earnings. The Bitcoin network is highly centralized in terms of both routing and mining. Most Bitcoin nodes worldwide are located on a small number of ISPs; a total of thirteen ISPs host 30% of the entire Bitcoin network. Furthermore, 60% of the traffic between Bitcoin nodes passes through only three ISPs, meaning that ISPs can see more than half of the world's Bitcoin connections. This concentration creates a central target for attackers.

The attacker can carry out the attack in two different ways:

• Split Attacks: Splits the network into two or more parts, creating parallel blockchains. Once the attack is over, the blocks on the smaller chain become invalid.

• Delay Attacks: Causes double spending and mining losses by delaying block transmission.

These attacks can be mitigated with routing-aware peer selection, connection diversity, and traffic encryption. As a precaution, connection behaviors must be made more conscious, peer selection must be based on routing awareness, and traffic encryption must be improved. Early detection can increase blockchain security by triggering more diverse connection selections.

Man-in-the-middle (MitM) attacks: MitM attacks are a type of attack where attackers insert themselves between third parties and nodes in a network, altering the data or messages being sent and manipulating the parties by impersonating them. These attacks can be carried out using various methods, such as altering smart contract parameters, redirecting transactions with fake nodes, spending the same funds multiple times (double spending), and delaying blocks. To mitigate the impact of these attacks, encrypted communication protocols (SSL/TLS), node authentication, consensus mechanisms (Proof of Work, Proof of Stake), and decentralized structures should be used. Although MitM attacks pose a serious threat to blockchain security, these risks can be significantly reduced with appropriate security measures.

Endpoint vulnerabilities: Endpoint vulnerabilities are weaknesses and potential points of exposure that arise in the user interface or at the system's points of interaction. Wallet security vulnerabilities can manifest in various ways, such as broken authentication, cryptographic errors, insecure storage of private keys, susceptibility to phishing attacks, cryptojacking, and inadequate encryption measures, and can put users' digital assets at risk.

Various methods can be used to address these security vulnerabilities. Specifically, a Trusted Execution Environment (TEE) can be added for the security of cryptographic operations, and the use of steganography may be recommended. These methods can help prevent issues such as the storage of sensitive data, faulty authentication, security configuration errors, or web security vulnerabilities.

Double Spending Threat: The double spending threat arises when the same cryptocurrency is attempted to be spent more than once, threatening the reliability and transparency of decentralized systems. This problem can stem from network delays, malicious actors, and weaknesses in the consensus mechanisms used. Among the existing approaches to solving this problem, mechanisms such as proof-of-work (PoW) and proof-of-stake (PoS) stand out. In addition, innovative technologies such as multi-party computation and zero-knowledge proofs are also being researched.

Risks associated with the use of Trusted Execution Environments (TEE): The SSI model design relies on the trusted execution environment (TEE) on devices (phones, tablets, computers) to store verifiable credentials. The TEE is an isolated, secure environment that provides processing, memory, and storage capabilities. Its security and integrity depend on the provider's ability to protect its hardware and software components. Although designed as a trusted environment, TEEs are not completely immune to security vulnerabilities and attacks. Threat actors are developing new techniques to target TEE, such as side-channel attacks, hardware vulnerabilities, and software security flaws. Continuous research, development, and careful monitoring are required to stay ahead of these threats. This ensures that TEE remains resilient against evolving security challenges.

4.2. Preventing Fraud and Protecting Citizens

Institutions and their customers' sensitive data is accessed through centralized databases. This situation may expose the institution's data to the risk of mass leakage in the event of potential attacks on these databases from outside. Fraudsters can target individuals' assets using traditional fraud methods such as social engineering and phishing through this data. Decentralizing data storage is therefore a necessity in this regard.

Digital Identity solutions can create a more robust and reliable financial ecosystem by significantly reducing fraud activities, as they are a secure and verifiable means of identity verification. With the rise of digitalization and social media usage, digital identity verification methods provide organizations with a significant protective shield, particularly as a countermeasure to the increase in identity theft cases.

4.2.1. How Data is Compromised in Known Fraud Methods

Social engineering, malware, and phishing are among the most commonly known fraud methods, where users either share their passwords, click on a malicious/fake website link, or are directly manipulated into performing an action. Additionally, in identity theft, one of the most common methods, the user is not involved at all; their identity is copied and used to impersonate them. A common feature of all these methods is that fraudsters possess certain data about their target audience before launching an attack.

Users can access many internet-based environments, primarily mobile applications, social media applications, and banking applications, with their passwords. Any data leak in any of these environments can lead to the exposure of the user's data both in that environment and in other environments where they use the same password. This collectively accessed information can be used through various fraud methods, primarily social engineering, to gain access to customers' financial assets or as a means of threat.

Organizations invest in various costly security measures to protect their customers' data. However, despite these measures, data breaches can still occur, and information can be leaked through internal misconduct. Storing data in traditional centralized systems has led to known identity verification methods being insufficient to protect users.

4.2.2. What is the advantage of digital identity verification over traditional identity verification methods?

Although the transactions performed by customers vary across different sectors, particularly in remote service delivery processes, certain traditional identity verification methods are still used. It is critical that these identity verification methods cannot be manipulated and that identities cannot be copied. Digital Identity solutions minimize the risk of data leakage by recovering data without centralizing it, while at the same time enabling users to access services more securely through identity verification based on encrypted data. Although third parties are involved in the verification process in digital identity verification, the risk of stored data being used by unauthorized persons is minimized because they cannot have access to all sensitive data.

Traditional identity verification methods may require more tools, manual processes, and human resources, whereas blockchain-based digital identity verification methods reduce such requirements, enabling the verification process to be completed in less time and at lower cost.

4.2.3. What should be considered when using digital identity verification?

As with other identity verification methods, balanced use in terms of privacy and experience is just as important as minimal information and user security in the implementation of digital identity verification. A robust ecosystem should be designed with a comprehensive view of all application risks, and the power of digital identity verification systems should be leveraged to the maximum extent. Digital identity verification solutions empower organizations to reduce data leaks and identity fraud with the advanced security offered by blockchain technology. However, both organizations and users have responsibilities in its implementation.

Once a piece of information is added to a blockchain, it can never be deleted or altered. Personal data added may be forgotten over time, and there will always be a risk of data being compromised for a blockchain component that has fallen out of use over time. Therefore, digital identity IDs that do not contain personal data can be used, and verifiable identity information with these IDs can be stored in the user's wallet instead of the blockchain.

In social engineering cases, one of the most common fraud methods, users are manipulated into acting entirely under the guidance of fraudsters, sharing their information, passwords, and verification components. This necessitates that the human factor always be considered a significant risk factor.

In this regard, while it is difficult to manipulate digital identity in terms of data security, the user's lack of sufficient awareness regarding the key information used to access data poses a risk. Organizations should make it standard and continuous practice to educate both their employees and customers in this regard and to conduct regular awareness/information activities on current fraud trends.

As a result, by taking the human factor into account, digital identity verification solutions offered to both employees and customers can be designed to be much more secure and streamlined than existing traditional identity verification methods. For the development of such innovative methods, it will be important to carry out awareness activities that will enable industries to better understand the blockchain world and for institutions to quickly adapt to the parallel regulatory changes.

5. LEGAL COMPLIANCE AND REGULATIONS

5.1. Required Legal Regulations and Ensuring Compliance with Legislation

In this section of the report, our goal is to examine the regulations necessary to support the adoption of digital identity systems and how compliance with personal data protection regulations can be achieved.

Before moving on to the situation in Turkey, we believe it would be useful to mention the steps taken in comparative law regarding the provision of digital identity and privacy and the development of compliance.

It is known that international institutions and organizations have also carried out various studies on establishing a legal framework in the field of digital identity and data protection and have drawn attention to the importance of this issue.

The World Economic Forum (WEF) publishes reports addressing the economic and social impacts of digital identities and encourages global cooperation in this area.
In particular, its report titled "Reimagining Digital ID Insight Report (June 2023)" states that decentralized ID systems can increase privacy, control, efficiency, and effectiveness when implemented correctly. Various technologies, standards, and recommendations exist for implementing decentralized identity systems, such as verifiable identity information, decentralized identifiers, principles, and governance frameworks. However, it is noted that this approach also carries certain risks. While efforts to scale decentralized identities continue, attention is drawn to the many obstacles encountered in practice. The report advises industry representatives to invest in technological innovation, standard harmonization, and skills development. Priorities have also been set for the public sector, including developing supportive regulations, encouraging collaboration, and defining interoperability and portability requirements. However, the lack of commonly accepted technologies, standards, and recommendations constitutes a significant limitation to the widespread adoption of these systems. It is noted that the absence of supportive policies and regulations could reduce the effectiveness of decentralized identities and also pose challenges in areas such as governance, communication, and functionality.

Reliable, independent digital identity systems for organizations subject to regulations under the Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) framework established by the OECD and FATF.

It is recommended that clear guidelines or regulations be developed that permit its use with an appropriate and risk-based approach (Guidance on Digital Identity). In this context, understanding the digital identity systems available in the relevant jurisdiction and assessing how these systems comply with existing requirements or guidance on customer identification and verification, ongoing monitoring, record keeping, and third-party reliance processes is seen as a starting point. The OECD and FATF also recommend adopting principles, performance, and/or outcome-based criteria in determining the necessary attributes, evidence, and processes for proving official identity for customer due diligence (CDD) purposes. Given the rapid evolution of digital identity technologies, this approach will both encourage responsible innovation and ensure that regulatory requirements remain compatible with future technological developments. Furthermore, the potential of digital identity systems to support financial inclusion is also highlighted. An integrated and multi-stakeholder approach is recommended to understand the opportunities and risks associated with digital identity and to develop regulations and guidelines to mitigate these risks. In this context, it is necessary to evaluate existing digital identity verification frameworks and technical standards adopted by authorities responsible for identity, cybersecurity/data protection, and privacy, and to leverage them where appropriate. In this process, aspects such as technology, security, governance, and resource management should be considered when assessing the confidence levels of digital identity systems for customer due diligence (CDD) purposes.

Additionally, it is stated that cooperation and coordination among relevant authorities is necessary to understand and address the risks in the digital identity ecosystem.

This approach is critical to ensuring that AML/CFT (anti-money laundering and counter-terrorist financing) requirements on digital identity systems are in line with data protection and privacy rules. This supports the secure and compliant use of digital identities.

The OECD's "Recommendation of the Council on the Governance of Digital Identity" provides member countries with a comprehensive framework for developing and implementing digital identity systems in a reliable, inclusive, and user-focused manner. This recommendation aims to ensure the secure and effective use of digital identities while protecting individuals' rights and freedoms.

Reliability and data security are key elements in the creation of digital identity systems. These systems must be able to accurately verify users' identities and ensure the security of personal data. At the same time, the accessibility of digital identities to everyone is critical to the inclusiveness of these systems. The OECD recommends that digital identity systems be designed to meet user needs and allow individuals to have control over their personal data.
Furthermore, it emphasizes the need to strictly adhere to privacy and data protection principles.

Attention is drawn to the need for a robust legal and regulatory framework to enable the effective and reliable implementation of digital identities. In this context, the OECD recommends that member countries review their existing rules on the recognition and use of digital identities and make the necessary updates. It is also stated that national and international standards need to be established to increase the interoperability and reliability of digital identity systems.

Developing effective oversight and enforcement mechanisms is crucial to ensuring these systems comply with legal frameworks. It is recommended that countries assess their existing legal requirements and trust frameworks and ensure the compliance of digital identity systems. Furthermore, harmonizing technical standards is an important step that will increase the interoperability of systems. Increasing information sharing and cooperation between countries will contribute to strengthening the digital identity ecosystem.

The document states that the success of the digital identity ecosystem also depends on effective cooperation between the public and private sectors. The OECD recommends that the public and private sectors work together on issues such as policy development, standard setting, and the promotion of technological innovation. Combining the innovation capacity of the private sector with the regulatory support of the public sector can accelerate the development of digital identity solutions. In addition, education and awareness campaigns are needed to enable users to use digital identity systems effectively and securely. Another point emphasized in the report is that the success of digital identity systems depends on user trust and participation. To increase user confidence in the system, transparency and accountability must be ensured, and systems must be continuously improved by taking user feedback into account. Providing guarantees regarding the security and privacy of individuals' personal data will increase trust in the systems.

The ID4D (Identity for Development) initiative, established within the World Bank Group, aims to help countries achieve their Sustainable Development Goals by leveraging global knowledge and expertise to support the Transformation Potential of digital identity systems. This initiative responds to government requests based on diagnostic studies in countries.

It provides technical support based on global best practices for the design of digital identity systems. In this context, it promotes the development of legal and operational foundations based on principles such as universal access, multi-purpose use, interoperability, robust and unique structures, as well as trust and accountability. In this context, it supports governments in establishing a robust legal and regulatory framework that covers data protection and privacy requirements.

Regulation (EU) 2024/1183 of the European Union was adopted by the European Parliament and the Council on April 11, 2024, and entered into force on May 21, 2024. This regulation amends Regulation No. 910/2014 (eIDAS) with regard to provisions on digital identities and electronic transactions and establishes the European Digital Identity Framework. In 2021, the European Commission proposed a European digital identity framework accessible through interoperable European digital identity wallets for all EU citizens, residents, and businesses. On March 26, 2024, the European Parliament and Council adopted this proposal with revisions. Under the new regulation, member states must offer digital wallets by the end of 2026 or early 2027 that allow citizens and businesses to link their national digital identities to other personal attributes (e.g., driver's license, academic qualifications, bank account information).

The United Kingdom has developed various legal regulations and standards to promote the secure and effective use of digital identities. Within this framework, the Office for Digital Identity and Attributes (OfDIA) sets standards to ensure the reliability of digital identity services. These standards enable individuals to securely verify their identities in the digital environment while also protecting privacy and personal data.

The government has also submitted the Data (Use and Access) Bill to Parliament to create a legal basis for digital identity verification services. This bill aims to establish a legal framework for digital verification services without requiring a mandatory digital identity system or identity cards.

In the field of privacy and personal data protection, the UK government introduced the Data Protection and Digital Information (No. 2) Bill to the House of Commons in March 2023. This bill aims to reduce the burden on organizations and update the data protection framework while maintaining high data protection standards. It also proposes reforms to the structure of the Information Commissioner's Office (ICO) and provides a framework to ensure the reliable use of digital identities.

In Turkey, blockchain-based digital identity applications are planned to be implemented through the e-Government platform.
In a statement from the Presidency, it was announced that citizens will be able to log into e-Government with digital identities integrated into the blockchain network using the e-wallet application. This step is seen as an important milestone in Turkey's digitalization process.

5.1.1. Current Legal Framework and Regulations

Digital identity and document digitization is an area that

must be handled with care in terms of personal data , ensuring security, and legal compliance. In this context, regulations applicable in Turkey and internationally aim to protect individuals' privacy and ensure transparency in data processing. This section evaluates the current legal framework for digital identity in light of the KVKK, GDPR, and other relevant regulations.

Basic Principles for the Protection of Personal Data under the KVKK and GDPR

Both the KVKK implemented in Turkey and the GDPR in the European Union have established fundamental principles for the processing of personal data. These principles serve as guidelines for ensuring the legal protection of digital identities and digital documents. The fundamental principles can be summarized as follows:

- Processing in accordance with the law and principles of fairness: Data must be processed in a manner that is compliant with relevant regulations and transparent.
- Processing for specific, explicit, and legitimate purposes: Personal data may only be collected for specific and legitimate purposes.
- Data minimization: Processed data must be limited to what is necessary for the purpose.
- Accuracy and timeliness: Processed data must be accurate and updated when necessary.
- Processing limited by storage period: Data should be stored for a period appropriate to the purposes of processing and deleted when that period expires.
- Privacy and security: Data must be protected against unauthorized access and damage by appropriate security measures.

KVKK (Personal Data Protection Law)

In Turkey, the Personal Data Protection Law No. 6698 (KVKK) establishes the basic legal framework for the processing and protection of personal data. The salient aspects of the law are as follows:

- Data Processing Conditions: The KVKK requires explicit consent or other processing conditions specified in the law for the processing of data.
- Data Subject Rights: Data subjects have the right to know whether their data is being processed, to question the purpose of processing, and to request the correction or deletion of their data.
- Data Controller Responsibilities: Data controllers are responsible for ensuring data security, reporting data breaches, and registering with VERBİS.

The KVKK requires strict supervision, particularly in sectors where digital identity is used extensively, such as banking. Regulations regarding data security are quite detailed in the processes of identity verification, customer information collection, and storage of this information.

GDPR (General Data Protection Regulation)

The European Union General Data Protection Regulation (GDPR) is legislation that has set the standard for digital identity regulations on a global scale. Organizations operating in Turkey that process the data of EU citizens must comply with the GDPR. The effects of the regulation on Turkey are highlighted under the following headings:

GDPR has an impact that extends beyond the borders of the EU. Digital service providers in Turkey must comply with these regulations when processing the data of EU citizens. GDPR clearly defines explicit consent and requires transparency in data processing procedures. The GDPR provides for severe penalties in cases of non-compliance. This requires Turkish companies to be careful about complying with the GDPR.

Other Relevant Legislation

Digital identity and document digitization are evaluated not only under the KVKK and GDPR, but also in light of sector-specific regulations. The banking sector, in particular, is subject to strict regulations in digital identity verification and data processing processes:

International Standards: Standards set by international organizations such as the FATF (Financial Action Task Force) directly impact digital identity verification processes to prevent money laundering and terrorist financing.

Compliance with regulations in the field of digital identity is a critical element that not only protects individuals' rights but also enhances the reliability of businesses and protects them from criminal penalties. Therefore, it is important to develop infrastructures that comply with both national and international regulations.

Banking Regulations: The Banking Regulation and Supervision Agency (BDDK) has established detailed rules on digital identity verification processes and customer information storage. Processes such as electronic identity verification and remote customer acquisition are evaluated within the scope of these regulations.

Digital Identity under the Regulation on Banks' Information Systems and Electronic Banking Services

The Regulation on Banks' Information Systems and Electronic Banking Services is one of the fundamental pieces of legislation governing digital identity verification and information security processes in the banking sector. The Regulation establishes the standards that must be followed in the protection of customer information, the security of digital transactions, and remote identity verification processes.

This regulation includes the following important elements regarding digital identity verification and electronic banking services:

Remote Identity Verification: The regulation requires the use of technologies such as reliable electronic signatures and biometric identity verification in remote customer acquisition and identity verification processes.

Compliance with the KVKK is mandatory in these processes.

Information Security: Banks must implement information security management systems to protect customers' digital identities and other personal data. The regulation requires these systems to be regularly audited and security vulnerabilities to be addressed in a timely manner.

- Access Authorization: In digital identity verification processes, only authorized personnel should be able to access customer information. Authorization policies are designed to protect the confidentiality and integrity of data.

- Risk Management: Banks are responsible for identifying and managing risks associated with digital identity verification in electronic banking services. The regulation requires regular penetration tests and information security training to minimize risks.

- Data Processing and Storage: The Regulation stipulates that digital data containing customer information must be stored only for the specified period and must be deleted or anonymized at the end of this period. This requirement is in line with the KVKK.

- Transparency and Duty to Inform: Banks are required to provide clear and understandable information to their customers during digital identity verification processes. In particular, information must be provided regarding the technologies used during remote identity verification and the purposes for which the data will be processed.

- Audit and Compliance: Under the regulation, banks are required to operate their information systems and digital identity verification processes in accordance with the standards set by the Banking Regulation and Supervision Agency (BDDK). Non-compliance may result in administrative sanctions and criminal liability.

These regulations play a critical role in enhancing the security of digital identity verification processes in the banking sector, while ensuring the confidentiality of customer information and legal compliance.

5.1.2. Developments Related to the Legal Framework of Digital Identity

Legal Definitions and Standards of Digital Identity

The European Union's new regulation, the European Digital Identity Regulation, which aims to provide electronic services in a secure environment, amends Regulation (EU) No. 2014/910 on Electronic Identification and Trust Services (eiDas), defines digital identity as "the process of using electronic personal identity data that uniquely represents a natural or legal person, or a natural person representing another natural or legal person."

The technical and legal rules established to ensure that digital identities can be used securely, efficiently, and compatibly are called standardization. In order for digital identities, i.e., digital tools used to verify individuals' identities, to function consistently and systematically across different platforms, services, and countries, certain standards must be established.
Standards are aimed at ensuring the security, privacy, interoperability, and ease of use of digital identities.

The Importance of Digital Identity Standardization

- Security: Protecting digital identities is critical to preventing identity theft and fraud. Standards define security measures such as strong encryption and the protection of biometric data.
- Compatibility: Digital identities should be consistently usable across different service providers and government systems. Standards ensure that identities work seamlessly across multiple platforms.
- Accessibility: Users should be able to manage their digital identities easily and securely. Standards ensure that digital identities are accessible to everyone.
- Data Protection and Privacy: The security of personal data contained in digital identities is important. Standards include rules for data minimization and ensuring users' rights to control their data.

Digital Identity Standardization in Europe The

European Union, standardization of digital identities has taken significant steps in this regard. Regulations such as the EU Digital Identity Regulation and eIDAS (electronic IDentification, Authentication and trust Services) ensure that digital identities are used within a common framework.

eIDAS Regulation (2014/910/EU)

eIDAS is a regulation that standardizes digital identities and digital signature services in Europe and ensures that member states' digital identities are compatible with each other. This means that digital identities created in one country can also be valid in another EU country. It standardizes security measures such as identity verification and digital signatures. It ensures the legal validity of electronic documents and guarantees the international validity of digital signatures.

European Digital Identity Regulation (2024):

The European Digital Identity Regulation aims to establish a single digital identity standard across the EU. This regulation aims to enable citizens of member states to manage their digital identities securely themselves. It also enables digital identities to be used in government and private sector services. Digital identity not only provides users with the ability to verify their identity, but also gives them control over their personal data. Users can protect their privacy by sharing their digital identity only when necessary.

The new regulations foresee the preparation of implementing legislation that will amend or replace the existing rules of application under Regulation 910/2014. The development of this implementing legislation is planned within 12 months of the adoption of the revised regulation.

The new regulation aims to ensure that digital identity systems operate in a secure, user-friendly, and interoperable manner.
European digital identity wallets will enable users to securely manage and share not only their identity information but also other personal attributes necessary for accessing specific services. This aims to accelerate digital transformation by simplifying processes for both individual users and businesses.

E-Signature and E-Seal Regulations

Reviewing regulations related to the legal validity and usability of electronic signatures and seals is also important.

E-signature (electronic signature) and e-seal (electronic seal) are two different technologies used to verify identity and ensure document security in digital environments. Although both concepts involve different technologies, they are used in digital transactions to guarantee the authenticity, integrity, and security of documents.

E-signature

An e-signature is, simply put, a security tool that makes a person's actions in a digital environment legally binding. Similar to a handwritten signature, an electronic signature functions as a signature on a digital file. This signature is used specifically to ensure the legal validity of digital documents. The Electronic Signature Law defines an electronic signature as "electronic data that is attached to or logically linked to other electronic data and used for the purpose of identity verification."

An electronic signature is used to verify the identity of the signer. This ensures that the person signing the document is indeed who they claim to be. An electronic signature guarantees that signed documents have not been altered afterward. If the document is tampered with, the signature becomes invalid.

Both in our country and in the European Union, electronic signatures have the same legal validity as handwritten signatures. In our country, the Electronic Signature Law No. 5070 defines and regulates e-signatures and legally recognizes their validity.

In Turkey, electronic signatures, which have the same legal validity as wet signatures, are widely used in various areas such as e-invoicing, e-prescriptions, and electronic correspondence packages. It should also be noted that the importance of electronic signatures is increasing in parallel with the digital transformation efforts being carried out in Turkey.

In this context, it is important to note that the standards used in creating electronic signatures have also gained considerable importance.

One of the important points in this regard is that it is crucial to follow the relevant electronic signature standards in the European Union and to analyze the updates made and incorporate them into Turkey's electronic signature legislation. The electronic signature standards adopted in Turkey in accordance with the Electronic Signature Directive 1999/93/EC have been updated over time within the European Union with eIDAS regulations and have begun to be implemented. However, Turkey has not yet complied with the current standards introduced by eIDAS. It is stated that there is an important need to provide a common infrastructure between the European Union and Turkey in the scope of electronic signature and trust services in order to ensure the security and effectiveness of digital trade and communication between the European Union and Turkey.

E-seal (Electronic Seal)

An e-seal is a digital security tool typically used by legal entities. E-seals are used to ensure the security and validity of transactions made by an institution or organization in a digital environment. E-seals are commonly used to sign digital documents belonging to a company or government agency. The Electronic Signature Law, the Regulation on Procedures and Principles Regarding Electronic Seals, and the Procedures and Principles Regarding Corporate Encryption and Electronic Seal Certificates Used in the Sharing of Documents in Electronic Environments Between Public Institutions and Organizations define an e-seal as as "electronic data added to another electronic data or logically linked to electronic data and used to verify the information of the electronic seal owner."

The e-seal is a security tool designed for legal entities rather than individuals. Companies or public institutions ensure the validity and security of their transactions by signing digital documents with the e-seal.

to ensure the validity and security of their transactions.

An electronic seal is a record of evidence that guarantees that the electronic document or data was created by the seal owner and that the document or data is authentic and intact. An electronic seal has the same legal status as any physical seal, including an official seal.

While e-signatures verify the identity of individuals, e-seals verify the digital identity of an organization or institution. In other words, e-signatures are used for individual transactions, while e-seals are used for corporate transactions.

Regulations Required for the Adoption of Digital Identity Technology

Although there is no specific regulation on digital identity in our country yet, the foundations for digital identity were laid with the Electronic Signature Law No. 5070 ("E-Signature Law"), which entered into force on July 23, 2004. The E-Signature Law also addresses the distinction between secure electronic signatures and electronic signatures, as well as the definitions and regulations of concepts such as time stamps, electronic data, and electronic certificates. Following the E-Signature Law, the legal framework for mobile electronic signatures was established by the Communiqué on Processes and Technical Criteria Related to Electronic Signatures.

We can list some of the proposals developed to ensure that electronic signature systems in Turkey comply with current technologies and standards and the situation in the EU as follows:

- Regulating the electronic signature legislation and secondary regulations currently in force in Turkey in accordance with current standards,

- Developers providing electronic signature software libraries (API) must provide software updates to comply with current standards.

It is important to ensure the interoperability of signed files created with old (current) standards with files created in accordance with current standards. This will make data and files created in the past compatible with current technologies. This will enable electronic signature technologies to be more widely used and accepted.

In our country, the general and identity-specific legal regulations that can be applied to the digital identity system include the Turkish Civil Code No. 4721, the Population Services Law No. 5490, the Passport Law No. 5682, and the Turkish Citizenship Law No. 5901.

In addition to these regulations, an important cornerstone forming the framework of an identity system is the protection and confidentiality of personal data.
In our country, the protection of personal data is regulated under the Personal Data Protection Law No. 6698 and its secondary regulations.

Of course, in addition to this, with the development of technology and changes in people's habits, it is important to establish a legal framework for the provision of banking and all kinds of financial transactions through digital identity, smart contracts, or more generally, digitalization, and regulatory institutions are continuing their legislative work.

However, to ensure that the legislative changes made to date can be fully implemented and the expected benefits can be achieved, it is also important that the legislative changes listed below are made.

- Electronic Signature Law No. 5070
- Law No. 6100 on Civil Procedure
- Turkish Code of Obligations No. 6098
- Turkish Commercial Code No. 6102
- Turkish Civil Code No. 4721
- Enforcement and Bankruptcy Law No. 2004
- Law No. 6750 on Movable Pledge in Commercial Transactions
- Regulation on Housing Accounts and State Contributions
- Regulation on Dowry Accounts and State Contributions
- Law No. 5941 on Checks
- Regulation on Distance Contracts for Financial Services
- Regulation on Housing Finance Contracts

6. IMPACT ON THE FINANCIAL SECTOR AND AREAS OF USE

6.1. National Blockchain Infrastructures in the Financial Sector and the Impact of Digital Identity

Customer Acceptance, KYC Processes, and Use in CBDC Systems

KYC (Know Your Customer) is a process that enables financial institutions such as banks, insurance companies, fintech companies, etc. to prevent illegal activities such as money laundering and terrorist financing, and to obtain information about their customers' financial situations, income sources, and risk profiles. In traditional finance, KYC processes involve both people and systems. At the same time, KYC plays a vital role for financial institutions in verifying the identities of their customers.

Each bank has its own unique KYC process and requires customers to submit the same information and documents separately to each bank. This makes KYC processes costly, time-consuming, and inefficient for both institutions and customers today. Furthermore, the fact that customer data is stored in central databases makes it a target for cyberattacks.

Blockchain technology is an innovation that will revolutionize KYC processes and the use of digital IDs.

This technology promises not only to redefine identity verification and KYC processes, but also to shape the future of banking in the digital age. There are many benefits to using blockchain infrastructure for digital identity verification.

Transparency: Using blockchain, KYC data can be stored immutably and provides a transparent system that can be accessed and verified by authorized individuals and organizations.

Security: The decentralized nature of blockchain makes changes, fraud, and cybersecurity risks nearly impossible by ensuring that multiple copies of transactions are stored across the network.

Digitalization: It speeds up processes by enabling users to access their identity data electronically and ensures seamless progress in banking services without interruption. With current technologies, it is possible to establish contractual relationships remotely and sign risk-bearing documents digitally. Digital identity eliminates the need for physical visits to financial institutions' branches and agencies, reduces waiting times, and provides an instant verification, offering a user-friendly experience.

Identity Data Control and Customer Consent: The centralized nature of current identity systems raises issues regarding data ownership and control sharing. As customers become more aware of the importance and value of their personal information, privacy concerns are increasing. Digital identity, with its decentralized and user-controlled structure, provides customers with control over their personal information, the ability to choose what data to share, and the option to give consent.

Access, Usability, and Interoperability: With digital identity verification, customers have more control over their data, enabling financial institutions to better address customers' individual needs and offers customized products and services tailored to their preferences. With the establishment of interoperability standards, financial institutions can expand their services globally and increase their inclusivity by attracting customers worldwide without the need for physical presence.

6.2. Documents to Be Digitized and Their Impact on the Blockchain World

Remote Contract Formation in the Financial World and the Advantages Created by Blockchain Technology

Blockchain technology has ushered in a new era in the digital world by increasing the reliability and transparency of traditional contracts. These digital agreements, known as smart contracts, consist of code fragments that can be automatically executed when certain conditions are met.

The ability to establish contractual relationships remotely in the remote services provided by institutions and organizations to their customers is critical for the uninterrupted provision and sustainability of services. In terms of establishing contracts remotely, the most important criteria emphasized by regulatory bodies to prevent potential disputes between institutions and customers are identity verification and transaction security.

The establishment of distance contracts in banking takes place via communication tools without time or location constraints during product applications and usage between banks and customers. Due to the increasing transaction speed, digitalization trend, and the financial risks involved in recent years, banking is one of the most heavily regulated sectors. The establishment of distance contracts for products and services offered to customers was first regulated by the Regulation on Distance Contracts for Financial Services, published by the Ministry of Customs and Trade on January 31, 2015.

Following this regulation, banking transactions began to shift towards digitalization. The trend towards digitalization gained significant momentum, particularly during the pandemic period as remote service models began to take center stage.

Banking Regulation and Supervision Agency; Regulation on Banking Information Systems and Electronic Banking Services, published in the Official Gazette dated 15/03/2020 and numbered 31069and the Circular dated 27/03/2023 on the Criteria to be Provided for Identity Verification and Transaction Security in Electronic Banking Services and in Establishing Contractual Relationships in Electronic Environments , which was published in the Official Gazette dated 27/03/2023 and numbered 31069, regulates how identity verification and transaction security should be implemented in electronic banking service channels and that techniques enabling non-repudiation and assignment of responsibility for both the bank and customers in transactions carried out through these channels should be used.

On the other hand, the Regulation on Remote Identification Methods to be Used by Banks and the Establishment of Contractual Relationships in Electronic Environments, published in the Official Gazette dated 01/04/2021 and numbered 31441published in the Official Gazette dated 01/04/2021 and numbered 31441, the Regulation on Remote Identity Verification Methods to be Used by Banks and the Establishment of Contractual Relationships in Electronic Environments has determined the criteria required for the establishment of a remote contractual relationship between real person customers and banks, which will replace the written form. The scope of the same regulation was expanded with the update published in the Official Gazette dated 25/05/2023 and numbered 32201; criteria were determined for establishing remote contracts with legal customers in addition to real persons.

Thanks to the regulations enacted by the BDDK, it is now possible to open accounts remotely and establish contractual relationships for many banking products at a distance. However, there are some pending legal regulations that need to be resolved in order for banks to expand the scope of products and services they offer remotely. Contracts that must be established in "written form" under various articles of law still cannot be established remotely. While the criteria regulated by the BDDK's regulation provide a legal basis for establishing contracts that are not subject to written form, they do not provide banks with legal certainty in the contract types listed below due to the articles of law.

Blockchain can offer opportunities to fundamentally solve this problem faced by the financial world by guaranteeing the immutability, reliability, and transparency of the data it stores on a distributed network. The use of blockchain technology, particularly in the field of digital identity management, can provide significant advantages to the entire sector in terms of transaction security and identity verification processes. Therefore, digitizing documents using blockchain technology will enable the creation of more secure and effective document management systems in the future, increase remote transactions, and contribute to sustainability by saving paper and time.

Sözleşme Adı	İlgili Kanun/Yönetmelik	Yasal Alınma Şekli	Kullanıldığı Ürünler
Cari Hesap Hükümleri	• 6102 Sayılı Türk Ticaret Kanunu	Yazılı Şekle Tabi	• Esnek Ticari Hesap • Borçlu Cari Hesap
Temlik Sözleşmesi	• 6098 Sayılı Türk Borçlar Kanunu	Yazılı Şekle Tabi	• Temlik Teminatlı Kredi
Çek Karnesi Beyannamesi	• 5941 Sayılı Çek Kanunu	Yazılı Şekle Tabi	• Çek Karnesi
Alacak ve Haklar Üzerine Rehin Sözleşmesi	• 4721 Sayılı Türk Medeni Kanunu	Yazılı Şekle Tabi	• Vadeli ve Vadesiz Mevduat Rehni • Hisse Senedi ve Menkul Kıymet Rehni • Motorlu Araç Rehni
Kefalet Sözleşmesi	• 6098 Sayılı Türk Borçlar Kanunu	Resmi Şekle Tabi	• Ticari Kredi (GKTS)
Ticari İşletmelerde Taşınır Rehni Sözleşmesi	• 6750 Ticari İşletmelerde Taşınır Rehni Kanunu	Resmi Şekle Tabi	• Ticari Taşıt Rehni
İpotek Sözleşmesi	• 4721 Sayılı Türk Medeni Kanunu	Resmi Şekle Tabi	• İpotekli Ticari Söz
Konut Finansmanı Sözleşmesi	• 6502 Sayılı Tüketicinin Korunması Hakkında Kanun - 31 Ekim 2024'te güncellendi. • Konut Finansmanı Sözleşmeleri Yönetmeliği – 31 Aralık 2024'te güncellendi. • 2644 Sayılı Tapu Kanunu	Resmi Şekle Tabi	• Konut Kredisi

6.3. New Services and Operational Efficiency

Digital identities are becoming increasingly indispensable worldwide for all types of organizations—private companies, government agencies, civil society organizations, and the people and organizations they serve. The growing use of digital technology and the advancement of artificial intelligence make the creation of digital identities even more important.

In the coming period, the widespread adoption of digital identity initiatives is expected to bring about fundamental changes in many sectors and industries. While these new technologies drive change, they also bring new services and enhance operational efficiency in existing systems.

We can classify the new service areas and operational efficiency processes expected to emerge in the future in relation to this identity into 6 categories. These are:

- Digital Identity Verification Platforms
- Biometric Identity Verification Systems
- Identity and Access Management (IAM) Developments
- Automated Credit Assessment and Risk Management
- Foreign Trade Sector and Digital Asset Management
- Secure Access Solutions

6.3.1. Digital Identity Creation and Verification Platforms

The development of digital identity technology and the verification of digital identities, along with the scalability of this service at the micro-transaction level, constitute one of the important steps in the widespread adoption of this technology. In this regard, digital identity systems form a trust triangle that connects three main roles: issuers, owners, and verifiers.

Digital Identity Creators are institutions or organizations that create digitally certified documents and provide them to their owners. They are responsible for creating and verifying identity information.

Digital Identity Holders, like individuals, manage their own identity information and use it to prove the accuracy of their data or identity. They have control over how and with whom their information is shared.

Validators evaluate these documents to determine whether they meet certain requirements. They verify the validity of the identity information provided by the holders.

This system enables individuals to manage their identities while enhancing privacy and security by increasing trust in the process through cryptographic verification.

In this context, digital identity creation platforms are emerging as a new type of service. Legal authorities must be involved in the digital identity creation process and serve as the source of the data that will be included in the digital identity. Parallel to the digital identity creation process, digital identity verification platforms are also expected to emerge as a new type of service.

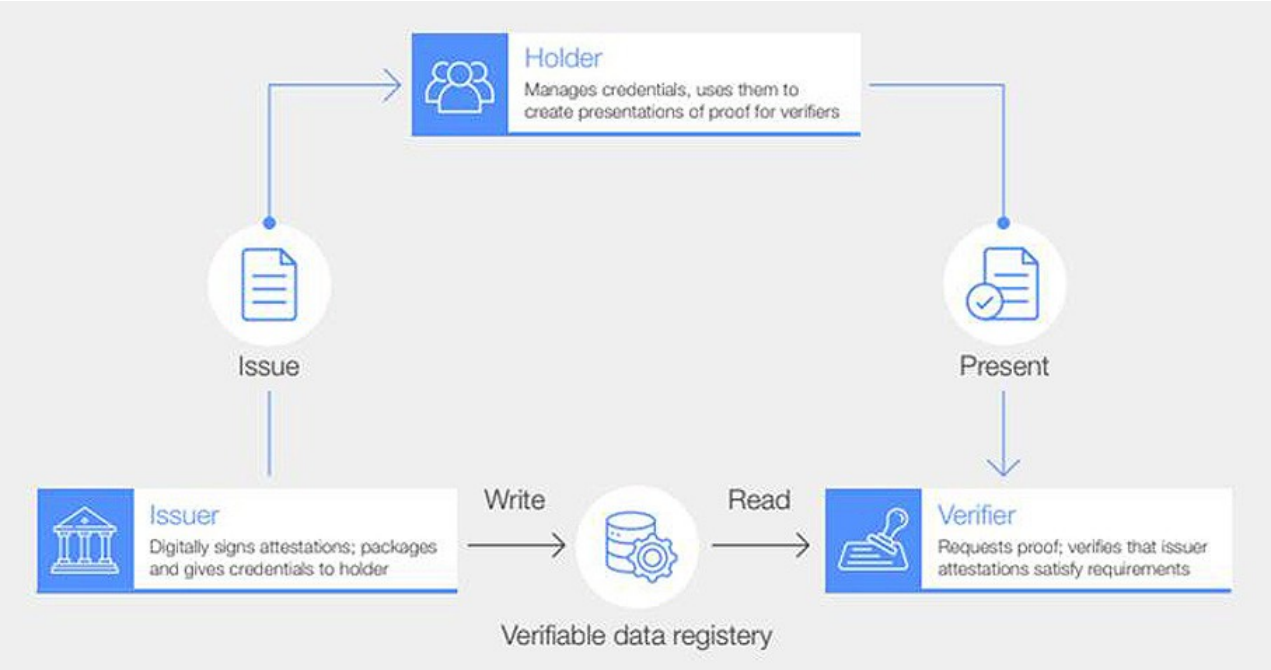


Figure 1 Verifiable Identity Information Trust Triangle (WEF, 2023)

With digital identity verification platforms, users can easily verify themselves using methods such as one-time identity verification and multi-factor identity verification in processes that require identity verification. In this process, the service of reading the relevant data can be provided to companies requesting information for institutions/organizations that will be verifiers on the chain with the creation of the identity.

For example, a citizen can quickly and easily open an account with a financial institution during the identity verification process in the account opening steps by approving the information required for account opening, which is stored in their digital identity within the wallet application.

Advances in artificial intelligence have also increased the importance of digital identity. With the development of artificial intelligence's visual processing technology, the potential to bypass identity verification mechanisms has also developed in parallel. In this regard, the importance of digital identity systems that verify that the user is a real person and can manage the necessary information/documents in KYC processes is increasing.

6.3.2. Identity and Access Management (IAM) Developments

With the proliferation of digital identities, identity access and management are expected to emerge as a new service. The implementation methods of identity access and management and the technologies being developed in this field ensure that this set of functions comes to the fore as a new form of service.

Cloud-Based IAM Solutions

With the proliferation of cloud technologies in recent years, cloud-based IAM solutions have begun to come to the fore.

Traditional IAM systems typically rely on local servers, while cloud-based systems offer flexibility and scalability, providing cost savings for businesses. These systems enable users to securely access resources from anywhere, while helping organizations consolidate identity and access management on a centralized platform.

Multi-Factor Authentication (MFA)

In the face of evolving cyber threats, multi-factor authentication (MFA) has become increasingly important. MFA requires users to provide multiple forms of proof to verify their identity. This is a much more secure method than relying solely on a password. For example, after entering their password, a user may also need to enter a code sent to their mobile phone. This makes it much more difficult for malicious individuals to access accounts.

Artificial Intelligence and Machine Learning

Artificial intelligence (AI) and machine learning (ML) technologies play a significant role in making IAM processes more effective. These technologies can detect unusual activities by analyzing user behavior. For example, if a user logs in at an unusual time or location, the system can detect an abnormal situation and take the necessary measures. Such proactive approaches offer a major advantage in providing protection against cyber attacks.

Identity and Access Management Standards

Standards and compliance requirements are also gaining importance in the field of IAM. For example, the European Union's General Data Protection Regulation (GDPR) and other similar regulations set rules for how organizations should manage user data. Therefore, configuring IAM systems to comply with these standards is critical both from a legal and security perspective.

Zero Trust Approach

The zero trust model has become an important trend in modern IAM applications. This approach is based on the principle of "never trust any user." Regardless of whether users are internal or external, identity verification and authorization are required for every access request. This helps organizations achieve a higher level of security while also improving the user experience.

As a result, developments in identity access and management continue rapidly alongside digital transformation. Cloud-based solutions, multi-factor authentication, artificial intelligence, standards, and zero trust approaches are critical for organizations to increase security and ensure efficiency. IAM will continue to be one of the most important components of cybersecurity in the future.

7. IMPACT ON OTHER SECTORS AND AREAS OF APPLICATION

Blockchain technology offers revolutionary innovations by providing security, transparency, and efficiency in digital identity verification processes. In this section of the report, we will examine how digital identity is used in different sectors, particularly with examples of applications supported by blockchain technology.

7.1. Public Administration

The use of digital identities is particularly important in the public sector. It minimizes the risk of error and fraud in identity verification processes while also enabling users to access services quickly and securely.
Blockchain technology can support us in protecting against data manipulation and increasing the transparency and reliability of these processes.

Below are examples and applications of digital identities used by governments; where applicable, the use of blockchain technology is highlighted.

Aadhaar, a 12-digit number issued to citizens by the Unique Identification Authority of India (UIDAI), was launched by the Indian government in 2009 with the aim of collecting, storing, and using the biometric information of over one billion people. Designed to serve as a unique identifier for Indian citizens, Aadhaar aims to prevent identity fraud and the resulting financial scams.
Blockchain technology is seen as having the potential to make the Aadhaar system more secure and transparent in this largest digital identity project supported by biometric data.
It is acknowledged that blockchain technology has potential for use cases such as security and voting systems.

Singpass, a trusted digital identity that enables citizens to access government and business services online, processes over 41 million transactions each month by 5 million users in Singapore. It provides secure and easy access to services at 800 public agencies and over 2,700 businesses. Thanks to the Singpass app developed by GovTech, users can perform many daily tasks, from identity verification to document signing, by logging in with biometrics (fingerprint, facial recognition) or SMS Two-Factor Authentication (2FA). The service, which enables the electronic signing of contracts, agreements, and other legal documents using the digital identity system, is based on blockchain technology. Thanks to cryptographic assignment to the signer and automatic verification at the time of signing, an electronic document can be easily signed digitally.

With the EU Digital Identity Wallet application, EU citizens, persons residing in the EU, and businesses operating in EU Member States will be able to access all online services using their new electronic identity, prove their identity online, and also share a document contained in their digital identity online through applications integrated into the system. Thanks to this application, citizens will have a secure and comprehensive account where they can add their diplomas, driver's licenses, and bank accounts by connecting to national digital identities. Users can use the wallet to open a bank account, prove their age eligibility, renew medical prescriptions, rent a car, and view airline tickets. Italy has launched IT-Wallet, the new version of the EU Digital Identity Wallet scheme, enabling citizens to digitize their identity documents through a single application.

Estonia offers a secure digital identity application through its E-Residency program, enabling individuals to access government services online.
Blockchain technology plays a critical role in verifying the identities of individuals who will use the service and ensuring the security of the identity information obtained.

Dubai plans to integrate blockchain-based digital identity systems into municipal services as part of its "Dubai Blockchain Strategy 2020" program. This will allow citizens to access municipal services with their digital identities. At the same time, the country is working on pilot projects to verify various legal documents, aiming to accelerate public processes and increase transparency by using blockchain-based digital identity verification systems.

Sierra Leone has implemented a pilot project to enhance the accuracy and transparency of election results using blockchain technology.

Within the scope of this project, digital identities have been used in voter identity verification processes. In local elections held in Russia, a blockchain-based voting system was used to ensure voter identity verification and vote security.

Brazil is running pilot projects using blockchain technology in notary services that require digital identity verification to ensure the accuracy and security of documents.

In Canada, Toronto is running projects that combine digital identity and blockchain technologies to provide its citizens with faster and more secure access to municipal services.

In Sweden, SEB bank and Nasdaq use blockchain-based digital identity systems in corporate identity verification processes. These systems ensure that inter-company transactions are conducted in a more secure and transparent manner.

7.2. Real Estate

Real estate is inherently immovable, indivisible, and illiquid. The process of converting illiquid real estate into liquid, tradable securities—known as securitization—dates back to the 1960s.

To enable the use of digital identity and blockchain technology in the real estate sector, real estate must first be digitally represented on the blockchain, i.e., tokenized. Tokenization refers to the process of creating a digital representation of an asset, which enables partial ownership, digital transfer, and management of these real assets on a blockchain. Real estate tokenization has various outcomes:

- It divides ownership into parts,
- contributes to operational efficiency,
- reduces payment times,
- ensures data transparency, and
- increases liquidity.

One promising detail in this area is the possibility of peer-to-peer (P2P) transactions involving land titles and other property rights.

Many countries have been using electronic cadastral systems for years, but they still rely heavily on paper-based processes. In fact, no country has yet enabled electronic peer-to-peer transactions for property rights. Although property rights and ownership rights are recorded electronically in such registries, these records are secondary and subordinate to transactions carried out on paper. A few countries, such as the United Kingdom, Australia, Canada, and New Zealand, have made more progress in electronic transactions and actively use electronic registration and application systems.

Real estate tokenization is a new trend that involves representing the ownership or rights of a single property or a property portfolio on a distributed ledger. Real estate tokenization first captured the world's attention in 2018 with the tokenization of the St. Regis Aspen Resort by Elevated Returns. This was followed in 2019 by a similar real estate tokenization project known as RealToken. The tokenization of the '9943 Marlowe' property was one of the first tokenized properties worldwide, and the token was subsequently made available for 24/7 trading on the public and permissionless Ethereum blockchain.

However, many countries lack the regulatory, legal, and technical frameworks necessary to enable the tokenization of property rights.
Real estate tokenization is now possible using current methods:

- Asset Selection: The real estate to be tokenized is selected. This can be a single property or a property portfolio.
- Legal Framework: A legal structure is established to ensure tokenization complies with local regulations. This typically involves creating a Special Purpose Vehicle (SPV) to hold the property.
- Token Creation: Digital tokens are developed on a blockchain platform. These tokens represent partial ownership of the property. Depending on the objective, these can be non-fungible tokens (NFTs) for unique properties or fungible tokens for partial ownership.
- Smart Contracts: Smart contracts are implemented to automate the management and transfer of tokens. These contracts define the rules and conditions for transactions, ensuring transparency and security.
- Token Offering: Tokens are offered to investors. For example, investors can buy, sell, exchange, or provide liquidity to the real estate market with these tokens as a Security Token Offering (STO).
- Management and Compliance: Rental income or profits are distributed to token holders according to smart contract terms to ensure the property is continuously managed and complies with legal requirements.

The platform issuing the tokens is responsible for fulfilling regulatory obligations (including the KYC - Know Your Customer - process) and providing the information required by the specific regulations governing STOs based on the target investors. At this stage, Digital Identities play a crucial role in tokenizing real estate on the blockchain.

- Identity Verification: Digital identities reduce fraud risk by ensuring all participants in the tokenization process are verified, and ensure compliance with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations.

• Transparency and Trust: By linking digital identities to transactions, all activities can be traced back to verified individuals or organizations. This increases transparency and builds trust among investors and stakeholders.

• Efficient Transactions: Digital identities facilitate the purchase, sale, and trading of real estate tokens. They accelerate transactions and reduce administrative burden by enabling fast and secure identity verification.

• Access Control: Digital identities can be used to manage access to sensitive information and ensure that only authorized individuals can participate in specific transactions or access certain data.

• Regulatory Compliance: Ensuring that all participants have verified digital identities helps maintain compliance with various legal requirements that are crucial for the legitimacy and acceptance of tokenized real estate.

• Enhanced Security: Digital identities provide an additional layer of security by reducing the risk of unauthorized access and fraud, ensuring that only verified individuals can initiate transactions.

Many platforms have successfully implemented the use of Digital IDs in real estate tokenization.

RedSwan specializes in commercial real estate tokenization. It uses digital identities to verify investor identities and ensures compliance with KYC and AML regulations.

Securitize partners with various real estate companies to tokenize assets. It uses digital identities to facilitate the investor verification process, ensuring regulatory compliance and enhancing transaction security.

Kasa Korea focuses on tokenizing real estate assets in South Korea. It uses digital identities to verify participants and provide a secure transaction environment. It facilitates cross-border investments by complying with international regulations.

Polymath provides a platform for tokenizing various assets, including real estate. It integrates digital identities to ensure only verified investors can participate in token offerings. Robust identity verification processes enhance security and compliance. These platforms demonstrate the effectiveness of integrating digital identities into real estate tokenization and provide secure, transparent, and efficient transaction environments.

7.3. Education

Blockchain-based digital identity systems are changing the way educational institutions create, manage, and verify academic identity information. These systems aim to provide academic documents such as diplomas, transcripts, and certificates in a secure, immutable, and easily verifiable format.

Such identity information enhances the accuracy of academic achievements and streamlines the process by reducing manual tasks between students, employers, and institutions. They also have the potential to contribute to continuous education and career development by making it easier for individuals to update their identity information. With the proliferation of blockchain-based identity systems, a more transparent, reliable, and efficient identity verification ecosystem is expected to be created in the field of education.

Storage and Verification of Academic Identity Information

Blockchain provides the ability to securely store and verify academic credentials such as diplomas, certificates, and transcripts.

By creating this identity information on the blockchain, institutions ensure that this information is immutable and can be instantly verified by employers or other educational institutions.

The Massachusetts Institute of Technology (MIT) was one of the first institutions to adopt this technology, issuing blockchain-based diplomas in 2017. In 2023, the University of Lille also launched its Dem-Attest project, beginning to issue verifiable digital diplomas worldwide.

Ownership and Portability of Education Data

Blockchain-based digital identities give students full control over their academic records. Thanks to SSI (Self-Sovereign Identity), students can own, manage, and share their educational credentials without the need for intermediaries. Users can prove their educational history even if the original documents are lost.

The European Union's "EBSI" (European Blockchain Services Infrastructure) project is researching SSI solutions to enable cross-border recognition of academic qualifications across Europe and reduce verification costs.

Decentralized Transcript Systems

Using blockchain and digital identity, institutions can create decentralized systems for storing and sharing academic transcripts. These systems enhance data integrity and simplify the process for students transferring between schools or applying for jobs. Transcripts become instantly accessible to students while also becoming verifiable by third parties.

In Japan, the University of Tokyo and Sony Global Education have partnered to develop a blockchain-based platform to facilitate transcript management and inter-institutional credit transfer.

Decentralized Learning and Socialization Platforms

Decentralized learning systems offer students more control and transparency, allowing them to determine their own learning processes and content. This approach can help overcome the limitations of traditional education systems and make learning experiences more accessible.
Traditional education systems typically involve many intermediaries, such as educational institutions, publishers, and content distributors. Blockchain aims to reduce costs and increase accessibility by enabling direct peer-to-peer interactions.

The Digital Badge project, carried out by the Ministry of Industry and Technology of the Republic of Turkey, enables the transfer of achievements to a digital platform by converting certificate-issuing institutions into users. This allows competencies that cannot be conveyed through resumes and diplomas to be shared using the advantages of digital certificates and badges. Digital Badges are verifiable digital symbols that showcase individuals' achievements or demonstrate that an individual has acquired specific knowledge, skills, and abilities. Institutions can send certificates and badges to individuals, and individuals can share their certificates and badges in a digital environment. Individuals and organizations can verify certificates and badges using an email address or Certificate/Badge ID.

With the growth of online courses and micro-credentialing programs, blockchain has become valuable for securely issuing digital badges and certificates for completed courses. These verifiable digital certificates can be stored in digital identities and shared with potential employers.

IBM has partnered with various educational institutions to offer blockchain-backed certificates for online courses. These certificates can be stored in students' digital identities.

7.4. Travel

The time passengers spend identifying themselves while traveling can be summarized as "making flight reservations, checking baggage at the airport, passing through security, boarding the plane, using in-flight services, and passing through the necessary checks upon arrival."

The airline industry has great potential to benefit from digital identity applications. There is a need for innovation in reducing pre-flight congestion at airports, managing the process from ticket purchase to flight completion quickly and reliably, reducing costs, and increasing passenger satisfaction. Therefore, the tourism sector is striving to develop solutions using biometrics and digital identity in line with technological developments.

The use of biometric and digital identity technologies is expected to play a significant role in the aviation sector. As the positive impacts of the solutions being tested on airlines, airports, and passengers become apparent, increased investment and widespread adoption in this area are anticipated.

In current applications, passengers can upload their ID cards or passport documents using their smartphones during the reservation process and then pass through security checks via facial recognition. In the US, as part of the Customs and Border Protection (CBP) 'Biometric Exit' program, some major airports such as Orlando, Los Angeles, and Miami International Airport

It has launched biometric screening programs at airports. The United Kingdom is testing the application at many airports as part of the Heathrow Biometrics project to speed up the passenger transportation process. The United Arab Emirates is also among the first countries to implement biometric screening during check-in, security screening, and boarding.

In the near future, the European Digital Identity Wallet (EUDIW) is expected to be introduced, which will enable the secure and transparent storage and management of electronic identity information, including biometric data, in a single location.

The International Air Transport Association (IATA) has successfully tested a fully integrated digital identity travel experience for selected flights from London Heathrow (LHR) to Rome Fiumicino (FCO) with British Airways, covering the entire process from ticket purchase to arrival at the destination. The project was carried out as a Proof of Concept (PoC) study developed at the IATA Innovation Lab, which brings together stakeholders in the travel chain to develop solutions. Digital identity-integrated wallets have made it possible for individuals to store the necessary information and loyalty program details and move quickly through the processes, thereby improving the travel experience.

IDNOW offers its users a digital identity application that replaces legal signatures, aiming to make transactions faster and more efficient with instant identity verification. The digital identity only needs to be loaded into the wallet once and can be used in many places. It also provides convenience to customers by being integrated into the verified European identity pool.

Developed in collaboration with iProov and Eurostar, SmartCheck is a digital identity solution that facilitates ticket and passport checks using facial biometrics for identity verification. SmartCheck is a digital identity solution that facilitates ticket and passport checks using facial biometrics for identity verification. SmartCheck is a digital identity solution that facilitates ticket and passport checks using facial biometrics for identity verification. SmartCheck is a digital identity solution that facilitates ticket and

biometrics for identity verification, simplifying ticket and passport checks. SmartCheck enables contactless travel by utilizing biometric facial recognition and remote identity verification technology.
Passengers can pass through security checks using their faces instead of tickets. It is used at London St. Pancras International Train Station. The application saves time by eliminating congestion and waiting times at train stations, shortens processing times by reducing manual control processes, increases staff efficiency, and provides a fast and secure solution to the end user.

7.5. Health

The use of digital identity in the healthcare sector offers many advantages for both patients and healthcare providers. Digital identity systems enable the quick and accurate verification of patients' identity information. This speeds up patient registration and reduces the error rate. Patients' medical history, current treatments, and medication information are integrated with their digital identities, providing healthcare providers with instant access.

Some examples of blockchain-based digital identity used in the healthcare sector are as follows:

Patient records in Estonia are digitized and secured by blockchain, providing a single, immutable data source for healthcare professionals. The country's e-Health system uses blockchain to securely store patient data and facilitate data sharing among healthcare providers. Thanks to this system, patients can access their own health data and see who has viewed it.

The MedRec project, created as part of a study supported by the MIT Media Lab Consortium, uses a decentralized record management system to process electronic health records using blockchain technology. The system design provides patients with access to comprehensive and immutable records and information at healthcare institutions. MedRec manages identity verification, data entry, updating, and sharing processes. Healthcare sector stakeholders are encouraged to join the network as blockchain "miners." In return for this participation, they are granted access to anonymized data as a mining reward.

Apart from this, even without the use of blockchain technology, many different examples can be seen in our country. In addition to E-Nabız, other applications in Turkey such as e-Government, MHRS, HES, and AHBS support the use of digital identity in the healthcare field.

- e-Government Portal: In Turkey, digital identity verification and access to healthcare services are provided through the e-Government Portal. Citizens can access their health reports, medication prescriptions, and medical history through e-Government.

- E-Nabız: This system aims to securely store and share patients' health data. Through this system, patients can access their own health data and monitor who views it.

- Centralized Physician Appointment System (MHRS): MHRS is a system that makes it easier for patients in Turkey to make appointments with doctors at hospitals. Thanks to digital identity verification, patients can securely make and manage appointments. This system speeds up access to healthcare services and allows patients to use their time efficiently.

• Family Medicine Information System (AHBS): AHBS is a system that enables family physicians to store patient health information digitally. With digital identity verification, patients' medical history, examination results, and prescriptions are securely stored and managed.

Additionally, Apple Health and Google Health, which we frequently use individually, are also good examples. The Apple Health app securely collects and stores users' health data. Users can access and share this data using identity verification methods. Similarly, Google Health also uses digital identity verification systems for managing health data. Similarly, IATA offers a digital health passport with Travel Pass, which allows travelers to securely store and share their COVID-19 test results and vaccination records. This identity has been adopted by major airlines such as Emirates and Qantas and is used on many continents.

7.6. Transportation

Digital identity and blockchain technologies are creating a significant transformation in the modern transportation sector. These technologies offer major advantages in areas such as identity verification, data security, and transaction efficiency. Below are various application areas and examples of these technologies in the transportation sector.

• Digital Twin and Graph Technology: In London, digital twin and graph technology is used to digitally model and manage transportation infrastructure. This technology simulates various scenarios to identify traffic congestion, road maintenance, and emergency response situations in advance and determine the best intervention solutions. This application is being developed by Transport for London.

• Global Digital Identity Initiatives: Digital identity technologies accelerate identity verification processes and enhance security during international travel and border crossings. For example, the paperless flight project between Canada and the Netherlands allows passengers to complete their flights using their digital identities. This project was carried out in collaboration between Canadian and Dutch airlines.

• Logistics: Blockchain technology is used in the logistics and transportation sector to track material movements and delivery processes. This ensures transparency and traceability in the supply chain while minimizing losses and errors. For example, Maersk uses blockchain-based digital identities to track products.

• Smart Contracts and IoT: Blockchain-based smart contracts enhance data sharing and process automation by integrating with IoT devices in the transportation sector. For example, the logistics company Fr8 uses smart contracts to make supply chain processes transparent and error-free.

• Automotive and Autonomous Vehicles: Blockchain technology is used in data security and identity verification processes for autonomous vehicles. For example, vehicle ownership information, maintenance records, and usage history are stored on the blockchain, increasing vehicle security and traceability. Companies using this technology include Tesla and BMW.

• Maritime Transport and Marine Insurance: Companies engaged in maritime transport worldwide are accelerating and securing marine insurance transactions using blockchain-based systems. This makes maritime transport operations more efficient and secure. Companies using this technology include Maersk and IBM.

Helium People's Network is the world's largest LoRaWAN network, enabling information transfer between IoT devices. This network has the ability to monitor and manage real-time asset data for smart cities and logistics. This system ensures that devices used in the transportation sector communicate securely and efficiently and guarantees data integrity.

The Istanbul Metropolitan Municipality is developing projects to integrate the city's transportation systems with blockchain technology. These projects aim to increase the efficiency of public transportation services by securing the identity verification processes of vehicles and users in urban transportation.

The TradeLens platform, developed by Maersk and IBM, uses blockchain technology in the maritime transport sector to ensure the traceability of products throughout the supply chain. This platform is used to increase transparency and efficiency in container shipping.
TradeLens supports real-time data sharing and collaboration among various stakeholders throughout the entire supply chain. This enables maritime transport operations to be carried out in a safer, faster, and more efficient manner.

7.7. Smart Cities

In today's rapidly digitizing world, digital identities play a vital role in managing identity verification and security processes for individuals and organizations. Especially in smart cities, digital identities stand out as a critical component in making city management and services more efficient, secure, and user-friendly. Digital identities enable users to perform their online transactions securely.

In smart cities, digital identities facilitate citizens' access to public services, improve ticketing processes and user experience in public transportation systems, enhance the effectiveness of security measures and emergency response in the city, and enable citizens to conduct their transactions with the government digitally through e-government applications.
Blockchain-based digital identities can contribute to making smart cities more efficient, transparent, and user-focused. By using this technology, smart cities can make citizens' identity verification processes, data management, and service integration more secure and efficient.

State-supported digital identities such as e-Identity in Estonia, SingPass in Singapore, Aadhar in India, DigiD in the Netherlands, and e-Government in Turkey. Platform-based applications play a significant role in the creation of smart cities and digital societies.

In Turkey, chip-based identity cards containing biometric data and identity information, chip-based driver's licenses containing driver information, and chip-based passports containing travel documents are in use. Electronic signature (e-Signature) is another important tool used for digital identity verification. E-Signature enables users to securely sign digital documents and verify their identity. In Turkey, e-Signature is widely used, particularly in areas such as public institutions and the banking sector.

The United Arab Emirates (UAE) has an integrated digital identity platform called UAE Pass, which is part of its smart city projects. UAE Pass provides a secure login mechanism for various websites and applications for government agencies and private companies in the UAE, enabling users to access over 6,000 services provided by more than 130 organizations.

UAE Pass eliminates the need for users to carry physical ID cards or documents, allowing them to conduct transactions digitally. The Dubai Blockchain Strategy aims to move all government transactions in the city onto the blockchain. Consensys has also collaborated on UAE Pass.

The energy sector is rapidly transforming through digitalization and the integration of innovative technologies. Blockchain technology, a key component of this transformation, provides transparency, security, and efficiency in energy trading and management processes. One of the greatest advantages blockchain technology offers the energy sector is its integration with the concept of digital identity.
Digital identities enable individuals and organizations to verify their identities in the digital environment and manage them securely. In the energy sector, digital identities simplify identity verification processes for energy consumers and producers and secure their transactions.

Blockchain also works in conjunction with systems such as renewable energy certificates (I-REC), carbon credits, and Guarantees of Origin (Go). These systems enable energy producers to certify their green energy production and offset their carbon emissions. Blockchain technology reduces the risk of fraud and facilitates the achievement of sustainability goals by ensuring that these certificates and credits are secure, transparent, and traceable. Digital identities play a critical role in verifying and tracking all transactions related to these certificates and credits. For example, when an energy producer certifies the green energy it produces using the I-REC system, this is linked to the producer's digital identity. This allows the energy producer's identity and the source of the energy it produces to be securely recorded and tracked on the blockchain.

Similarly, digital identities are also used in carbon credits and Guarantees of Origin (Go) systems to ensure the accuracy and transparency of transactions.

Elia Group and Energy Web have developed a solution that supports digital identity applications in the energy sector. This application digitizes the identity verification processes of energy consumers and producers, offering a more secure and efficient system. Digital identities increase transparency in energy transactions and consumption tracking. Elia Group uses this technology to make energy systems smarter and more flexible, enabling users to manage their energy consumption more effectively.
Supported by Energy Web's blockchain infrastructure, this digital identity application secures users' energy transactions and enables new business models to emerge in the energy market. This solution paves the way for digitalization in the energy sector while also providing a secure and transparent energy trading environment.

In a project carried out in collaboration with Elia, Energy Web, and BMW, the visibility of electric vehicle (EV) charging stations by grid operators has been successfully demonstrated. This project facilitates the integration of electric vehicle charging infrastructure into energy systems by improving its management and transparency. As part of the project, electric vehicle charging processes are tracked and managed using blockchain-based digital identities. This helps to better balance energy demand and supply, increase energy efficiency during charging, and improve the user experience. Furthermore, this technology allows the occupancy and availability of charging stations to be monitored in real time. This project contributes to the secure and transparent management of the electric vehicle charging infrastructure.

Shell has developed decentralized digital passports to increase the efficiency of the supply chain. These digital passports are used to verify and track the identity of each component in the supply chain. Supported by blockchain technology, this system ensures that transactions in the supply chain are secure and transparent. Digital passports track the entire process of products from the production stage to the end user and provide verification at each step. This prevents counterfeiting and irregularities in the supply chain, increasing product quality and reliability. In addition, this system enables Shell to manage its supply chain more quickly and efficiently, reducing operational costs.

Energinet, Denmark's energy grid operator, has developed a blockchain-based energy data management system in collaboration with Microsoft. This project securely records and shares energy production data on the blockchain. Digital identities are used to verify the identities of energy producers and track energy data. This system increases transparency in the energy market and ensures data security. The collaboration between Energinet and Microsoft demonstrates the potential of blockchain technology in energy data management and offers innovative solutions for the energy sector.

The SmartCommunity project launched in Austria through a collaboration between Energie Steiermark and Power Ledger utilizes blockchain technology to facilitate energy sharing and trading among local energy communities. As part of the project, users can share and trade their surplus energy with other users via a blockchain-based platform.

In this process, digital identities play a critical role in enabling users to securely perform identity verification and energy transactions. Digital identities verify the identity of each energy user, secure energy transactions, and ensure that all transactions are recorded transparently. This encourages local energy production, supports environmental sustainability, and fosters strong collaboration among energy communities.

A new application manages the digital identity traffic between decentralized energy sources and the grid. This application uses biometric data and digital identity technologies to verify the identities of energy consumers and optimize energy flow. Biometric digital identities securely record users' energy consumption profiles, providing personalized energy solutions. This makes energy management more efficient and reduces users' energy costs. Furthermore, the use of biometric data increases security in identity verification processes and enables users to carry out their energy transactions more quickly and easily. These technologies play an important role in increasing efficiency and security in the energy sector.

7.8. Training and Awareness Campaigns Necessary for the Adoption of Digital Identity

7.8.1. Social Impacts

Increased Inclusivity

- Keeping Everyone Included in the System: Digital identity offers an important solution, especially for people living in rural areas who have limited access to physical identity offices or cannot verify their identity using traditional methods. For example, digital identity solutions accessible via mobile devices enable everyone to benefit from social services.

• Reducing the Digital Divide: In many countries, digitization can create a serious barrier for individuals who lack access to technology. However, digital identity solutions can reduce this inequality through low-cost integration and simplified access methods. User-centered design makes it easy for everyone to access these services, regardless of age or technological experience.

Convenience and Accessibility

• Ability to Perform Transactions Quickly: Consider the time wasted during online transactions due to steps such as constantly uploading documents and showing identification. Digital identity speeds up processes in many areas, such as e-commerce, secure transactions, and government services.

• 24/7 Access: Traditional institutions may have limited working hours for identity verification, but digital identities can be used 24 hours a day. This allows individuals to overcome physical constraints and carry out the transactions they need at any time.

Security and Data Management

• Preventing Fraud and Identity Theft: Digital identities are more secure than physical identities thanks to measures such as strong encryption and two-factor authentication. They minimize situations such as data breaches or identity theft. For example, India's Aadhaar system provides high security in identity verification processes because it uses biometric data.

• Decentralized Data Storage: A system where users control their own data and share it only when necessary increases personal privacy. Decentralized digital identity solutions are an excellent example of this.

7.8.2. Requirements for Increasing Adoption Rates

Organizing Educational Campaigns

• Creating Awareness: Understanding the benefits of digital identity facilitates adaptation. Informative campaigns can be organized using mass communication tools such as social media, television, and the internet.

• Demonstrating User Experience: Simple step-by-step guides or user stories are effective ways to clearly show how digital identity provides convenience.

• Addressing Security Concerns: Users may have questions such as "Are my data secure?" or "Is this technology safe?" Therefore, it is important to explain the security infrastructure behind digital identity in simple and understandable language.

Designing More Accessible Platforms

• Increasing Mobile Integration: Today, most people's first choice is mobile devices. Therefore, the mobile compatibility of digital identity applications is critical.

• Providing Incentives: Governments can offer incentives to encourage the use of digital identities. For example, offering transaction fee discounts to those who use digital identities can encourage more people to join the system.

• Simplifying Usage: If digital identity applications are complex, users will not be able to adapt to the system. Adaptation can be accelerated by providing a "user-friendly" interface and step-by-step guides.

8. CONCLUSION AND RECOMMENDATIONS

Digital identity and the digitization of documents play a critical role in the digital transformation processes of individuals, institutions, and governments. However, this transformation requires a robust legal and technical infrastructure to achieve the goal of protecting personal data and ensuring privacy. In particular, digital identity systems must be secure, accessible, user-friendly, and compliant with legal regulations.
In light of international practices and research, certain steps must be taken to ensure the sustainability of digitization processes.

The legal and regulatory frameworks must be reviewed and strengthened to successfully implement digital identities. While existing regulations in Turkey aim to protect privacy, they may need to be continuously updated to keep pace with the rapid technological developments in digital identities and documents. In particular, it is important to develop interoperability standards and bring national legislation into line with international standards, drawing on examples from the European Union's eIDAS and Regulation 2024/1183.

In terms of personal data protection, the KVKK and GDPR frameworks should remain the fundamental reference points. However, the effectiveness of these frameworks in practice should be enhanced, and oversight mechanisms should be made more comprehensive. For example, data minimization, transparency, and data subject control rights must be fully implemented in digital identity systems. Furthermore, specific regulations should be established regarding the processing of sensitive personal data, such as biometric data, under the KVKK, and difficulties encountered in practice should be resolved.

To enhance the reliability of digital identity systems, cybersecurity measures must be prioritized. Strong encryption methods, multi-layered security mechanisms, and regular penetration tests should be implemented to minimize security vulnerabilities or risks of misuse. Furthermore, leveraging innovative technologies such as blockchain can enhance the security and transparency of identity verification processes.

Raising user awareness is another critical factor in the adoption of digital identities.
Citizens should be informed about how digital identity systems work, how their personal data is protected, and how they can use these systems securely. Education programs and awareness campaigns jointly organized by the public and private sectors will play a major role in this process.

Finally, a multi-stakeholder collaboration mechanism should be established. Public institutions, the private sector, academia, and international organizations should work in coordination to develop the digital identity ecosystem. As emphasized by the FATF and OECD, aligning AML/CFT requirements with data protection and privacy standards will enhance the reliability of these systems and ensure their adoption by a wider user base.

The opportunities provided by digitization in digital identity and documents must be balanced with sensitivity to individuals' privacy and data security. In this regard, strengthening the legal and technical infrastructure, ensuring user confidence, and benefiting from international best practices are critical for Turkey to achieve its digital transformation goals. This approach will position Turkey as a key player not only at the national level but also within the global digital ecosystem.

9. REFERENCES

Vitalik Buterin. A Next-Generation Smart Contract and Decentralized Application Platform. 2014. URL: https://github.com/ethereum/wiki/wiki/White-Paper.

Daniel Macrinici, Cristian Cartofeanu, and Shang Gao. “Smart contract applications within blockchain technology: A systematic mapping study”. In: Telematics and Informatics 35.8 (2018), pp. 2337–2354. DOI: https://doi.org/10.1016/j.tele.2018.10.004.

J. Frankenfield, "51% attack," Investopedia, 2019.

J. L. Zhao, S. Fan, and J. Yan, "Overview of business innovations and research opportunities in blockchain and introduction to the special issue," Financial Innov., vol. 2, no. 1, pp. 1–7, Dec. 2016.

Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. Future Gener. Comput. Syst. 2020, 107, 841–853.

Alajlan, R.; Alhumam, N.; Frikha, M. Cybersecurity for Blockchain-Based IoT Systems: A Review. Appl. Sci. 2023, 13, 7432.

Andryukhin, A.A.. (2019). Phishing Attacks and Preventions in Blockchain-Based Projects. 15-19. 10.1109/EnT.2019.00008.

Shijie Zhang and Jong Hyouk Lee. "Double-Spending with a Sybil Attack in the Bitcoin Decentralized Network." In: IEEE Transactions on Industrial Informatics 15.10 (2019), pp. 5715–5722. DOI: 10.1109/TII. 2019.2921566.

I. Riadi, R. Umar, I. Busthomi and A. W. Muhammad, "Block-hash of blockchain framework against man-in-the-middle attacks", Register: Jurnal Ilmiah Teknologi Sistem Informasi, vol. 8, no. 1, pp. 1-9, 2022.

P. Ekparinya, V. Gramoli, and G. Jourjon, "Impact of man-in-the-middle attacks on ethereum," 2018 IEEE 37th Symposium on Reliable Distributed Systems (SRDS), pp. 11-20, 2018.

Faizi, Azeem & Mustafa, Khurram. (2024). Mitigating Blockchain Endpoint Vulnerabilities: Conceptual Frameworks. International Journal of Computer Networks and Applications. 11. 933-953. 10.22247/ijcna/2024/56.

A. Kumar, B. Kumar Sah, T. Mehrotra and G. K. Rajput, "A Review on Double Spending Problem in Blockchain," 2023 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES), Greater Noida, India, 2023, pp. 881-889, doi: 10.1109/CISES58720.2023.10183579.

X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen A survey on the security of blockchain systems, Future Generat. Comput. Syst., 107 (June 2020), pp. 841-853 [accessed Jul 09 2024].

BCTR Digital Identity Report, Access Date: April 2019

Decentralized Identifiers (DIDs) v1.0, Access Date: July 2024

Verifiable Credentials Data Model v1.1, Access Date: July 2024

OpenID4VCI, Access Date: July 2024 OpenID4VP,

Access Date: July 2024 DIGITAL IDENTITY

STANDARDS, Analysis of standardization requirements in support of cybersecurity policy, ENISA, July 2023

European Data Protection Supervisor, Where are we heading with digital identities,

Konstantin Schaarschmidt, Data protection and data security in the context of digital identities

Beduschi, A. (2019). Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. Big Data & Society, 6(2).

Nikhil Ghadge. (2024). Digital Identity in the Age of Cybersecurity: Challenges and Solutions. London Journal of Research In Computer Science and Technology, 24(1), 1–10. Retrieved from https://journalspress.uk/index.php/LJRCST/article/view/1023

Mary-Jane Sule, Marco Zennaro, Godwin Thomas, Cybersecurity through the lens of Digital Identity and Data Protection: Issues and Trends, Technology in Society, Volume 67, 2021, https://doi.org/10.1016/j.techsoc.2021.101734.

The security and privacy features of the EU Digital Identity Wallet,

UNDP, Drafting Data Protection Legislation, Global Frameworks, Reimagining Digital ID INSIGHT REPORT JUNE 2023,

World Bank, DIGITAL ID AND THE DATA PROTECTION CHALLENGE, October 2, 2019,

OECD, Recommendation of the Council on OECD Legal Instruments for the Governance of Digital Identity,

WEF, Digital Identity Module, https://widgets.weforum.org/blockchain-toolkit/digital-identity/index.html

Saturday, January 31, 2015 Official Gazette Number: 29253

Republic of Turkey Official Gazette, March 15, 2020, Issue No.: 31069

Circular on the Criteria Required for Identity Verification and Transaction Security in Electronic Banking Services and the Establishment of Contractual Relationships in Electronic Environments Number: 77574904-010.06.02

Official Gazette of the Republic of Turkey, April 1, 2021, Issue No.: 31441

Official Gazette of the Republic of Turkey, May 25,

2023, Number: 32201 e-Residency of Estonia. (n.d.).

Retrieved from

Marr, B. (2019, January 21). Estonia's e-Residency: Redefining Citizenship in a Digital Age. Forbes. Retrieved from Forbes

UIDAI (Unique Identification Authority of India). (n.d.). Retrieved from

How Blockchain Could Improve India's Aadhaar System. (September 22, 2018). The Economic Times. Retrieved from Economic Times

Blockchain Can Transform Notary Services in Brazil. (n.d.). Cointelegraph. Retrieved from Cointelegraph

Dubai Courts and Blockchain: A New Era of Legal Transparency. (November 17, 2019). Zawya. Retrieved from Zawya

Blockchain Used in Sierra Leone's Election for the First Time Ever. (March 15, 2018). TechCrunch. Retrieved from TechCrunch

Moscow's Blockchain Voting Platform Fails, Attracts Just 1,500 Users. (2019, September 11). CoinDesk. Retrieved from CoinDesk

Dubai Aims to Be the World's First Blockchain-Powered Government. (2017, April 25). World Economic Forum. Retrieved from WEF

Toronto Explores Blockchain Technology for Municipal Services. (March 28, 2019). The Globe and Mail. Retrieved from The Globe and Mail

Nasdaq and SEB Partner on Blockchain for Mutual Funds. (September 27, 2017). Finextra. Retrieved from Finextra

IBM and SecureKey Partner for Blockchain-Based Digital Identity System. (March 20, 2017). IBM. Retrieved from

Think Digital Partners. (2024). How Digital Twin Powered Graph Technology Keeps London Moving. Retrieved from https://www.thinkdigitalpartners.com/news/2024/05/09/how-digital-twin-powered-graph-technology-keeps-london-moving/

Think Digital Partners. (2023). Digital Identity Global Roundup. Retrieved from https://www.thinkdigitalpartners.com/news/2023/01/23/digital-identity-global-roundup-99/

Think Digital Partners. (2019). Now You Can Fly Paperless Between Canada and the Netherlands. Retrieved from https://www.thinkdigitalpartners.com/news/2019/07/03/now-you-can-fly-paperless-between-canada-and-the-netherlands/

Think Digital Partners. (2023). Digital Identity Global Roundup. Retrieved from https://www.thinkdigitalpartners.com/news/2023/05/30/digital-identity-global-roundup-117/

Google Drive. Blockchain in Logistics and Transportation. (Article 11, Pages 81-88). Retrieved from https://drive.google.com/file/d/1reY0wxfMIfrDPsOP-sPIrnbgt5DReHuP/view

Astarita, V., Giofrè, V. P., Mirabelli, G., & Solina, V. (2020). A Review of Blockchain-Based Systems in Transportation. Information, 11(1), 21. doi:10.3390/info11010021

Subramanian, N., Chaudhuri, A., & Kayıkcı, Y. (2020). Blockchain Applications and Future Opportunities in Transportation. In: Blockchain and Supply Chain Logistics. Palgrave Pivot, Cham. doi:10.1007/978-3-030-47531-4_5

Stanford Online. Blockchain use cases in the supply chain. Retrieved from https://online.stanford.edu

Built In. (2024). 37 Top Blockchain Applications to Know for 2024. Retrieved from https://builtin.com/blockchain/blockchain-applications

Dock.io. (2024). Blockchain Identity Management: Complete Guide 2024. Retrieved from https://www.dock.io/blog/blockchain-identity-management

Deloitte Insights. (2024). Blockchain trends. Retrieved from https://www2.deloitte.com/insights/us/en/focus/ tech-trends.html

IBM. (2024). Blockchain for Digital Identity and Credentials. Retrieved from https://www.ibm.com/blockchain-identity

Faizi, Azeem & Mustafa, Khurram. (2024). Mitigating Blockchain Endpoint Vulnerabilities: Conceptual Frameworks. International Journal of Computer Networks and Applications. 11. 933-953. 10.22247/ijcna/2024/56.

A. Kumar, B. Kumar Sah, T. Mehrotra and G. K. Rajput, "A Review on Double Spending Problem in Blockchain," 2023 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES), Greater Noida, India, 2023, pp. 881-889, doi: 10.1109/CISES58720.2023.10183579.

X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen A survey on the security of blockchain systems, Future Generat. Comput. Syst., 107 (June 2020), pp. 841-853 [accessed Jul 09 2024].

BCTR Digital Identity Report, Access Date: April 2019

Decentralized Identifiers (DIDs) v1.0, Access Date: July 2024

Verifiable Credentials Data Model v1.1, Access Date: July 2024

OpenID4VCI, Access Date: July 2024 OpenID4VP,

Access Date: July 2024 DIGITAL IDENTITY

STANDARDS, Analysis of standardization requirements in support of cybersecurity policy, ENISA, July 2023

European Data Protection Supervisor, Where are we heading with digital identities,

Konstantin Schaarschmidt, Data protection and data security in the context of digital identities

Beduschi, A. (2019). Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. Big Data & Society, 6(2).

Nikhil Ghadge. (2024). Digital Identity in the Age of Cybersecurity: Challenges and Solutions. London Journal of Research In Computer Science and

Technology, 24(1), 1–10. Retrieved from https://journalspress.uk/index.php/LJRCST/article/view/1023

9. CONTRIBUTORS

Alev Orbay
Ali Akarçay
Alican Şahin
Arda Ata
Aykut Şahin
Ayşe Keleş
Barbaros Buyukyilmaz
Belamir Irem Acar
Bengisu Ozgehan
Berkay Doğan
Berke Bayhoca
Berke Sohtaoğlu
Berna Elyıldırım
Burcu Sakız Burcu
Tümer
Burçin Bozkurt Günay
Cansu Yaşar
Cemal Enis Ös
Erhan Yılmaz
Erman Mutlu
Erol Alkan
Ersin Yılmaz
Esra Özdemir
Gökhan Polat
Göksel Doğan
İlayda Aydın
İskender Kalkan
Macit Mete Oğuz Mahir
Kubilay Dağlı Mehmet
Yasin Akpınar Meltem
Erdem
Merve Akgün Sarı,
Murat Güç,
Mustafa Öztürk
Mustafa Serdaroğlu Dr.
Mustafa Takaoğlu Naz
Büke Bolluk Necati
Keskin
Nesrin İlker Peker
Ogün Sarıer Oktay
Adalıer Onur Çakır
Onur Köse
Ozan Ege
Özlem Aydın Bulut
Pınar Çağlayan Aksoy
Sadettin Kerim
Selin Pekmezci,
Taner Dursun,
Tolga Ünal, Umut
Can Erten, Vedat
Güven,
Yalçıncan İkin,
Yiğit Akkoyunlu

BLOCKCHAIN
TÜRKİYE

DIGITAL IDENTITY SYSTEMS AND THEIR SECTORAL IMPACTS
REPORT

On-Chain
Çalışma Grubu

JUNE 2025

TBV
TÜRKİYE BİLİŞİM VAKFI