DIGITAL IDENTIFICATION AND FINANCIAL MONITORING: NEW TECHNOLOGIES IN THE FIGHT AGAINST CRIME[1]

Maryna Utkina
Ph.D., Associate Professor, Sumy State University, Ukraine;
Research Fellow, School of Law University of Warwick,
The United Kingdom of Great Britain and Northern Ireland
e-mail: m.utkina@yur.sumdu.edu.uaorcid.org/0000-0002-3801-3742

Summary

The purpose of the research is to explore the role of emerging technologies in combating criminal activities, particularly in digital identification and financial monitoring. The article aims to highlight how these new technologies can enhance the effectiveness of law enforcement agencies and financial institutions in detecting and preventing crime.

Methods. The methodological basis of the research was a set of methods of scientific knowledge. In particular, the phenomenological method allowed the author to analyse national, international, and foreign law legal sources. The analytical method was used during the analysis of the conceptual and categorical apparatus, the definitions of "artificial intelligence", "digital identification", "blockchain", etc. The author also used the method of analysis and generalisation, which made it possible to clarify and generalise views on the essence and types of digital identification for further use in financial monitoring.

Results. The article discusses various technological advancements, such as biometric identification systems, blockchain technology, artificial intelligence, and data analytics, and their application in the fight against crime. It explores how digital identification systems can help verify individuals' identities more securely and efficiently, reducing the risk of identity theft and fraud. Additionally, it examines how financial monitoring tools can enable authorities to track suspicious transactions, detect money laundering activities, and disrupt the financing of criminal organisations. The article also addresses potential concerns and challenges associated with using these technologies, such as privacy issues, data security, and ethical considerations.

Conclusions. New technologies such as biometrics (e.g., fingerprints, facial recognition, iris scans) and blockchain-based systems can improve digital identification processes. These technologies offer increased security, reduced fraud, and streamlined identity verification procedures, preventing theft and other related crimes. Advanced data analytics, machine learning, and artificial intelligence algorithms can be utilised to enhance financial monitoring systems. These technologies enable faster and more accurate identification of suspicious transactions, money laundering activities, and financial crimes. Automated systems can analyse vast amounts of data and detect patterns that would be difficult for humans to identify, thereby assisting law enforcement agencies in combatting financial crimes.

Key words: artificial intelligence, blockchain technology, digital identification, financial intelligence unit, financial monitoring.

DOI https://doi.org/10.23856/5842

[1] This research project is funded by the British Academy (RaR\100538).

1. Introduction

In today's increasingly digital world, digital identification and financial monitoring have revolutionised how individuals and organisations interact with financial systems. The rapid advancement of technology and the widespread adoption of digital platforms have resulted in an unprecedented rise in financial transactions carried out online. With this shift, the need for secure and reliable identification systems has become paramount. Traditional identification methods, such as paper-based documents and physical identification cards, are no longer sufficient to meet the demands of a digital economy. The volume of digital transactions is experiencing a significant growth rate of nearly 13% annually. By 2022, approximately 60% of the global Gross Domestic Product (GDP) is projected to be digitised. This indicates a substantial shift towards digital platforms and technologies in various sectors of the economy, reflecting the increasing reliance on digital transactions for financial activities. The statistics highlight the expanding role of digitalization in shaping the global economy and the need for robust digital infrastructure to support this digital transformation.

The purpose of the research. The research aims to explore emerging technologies' role in combating criminal activities, particularly in digital identification and financial monitoring. The article aims to highlight how these new technologies can enhance the effectiveness of law enforcement agencies and financial institutions in detecting and preventing crime. Financial monitoring complements digital identification by enabling real-time tracking and analysis of financial activities. By integrating digital identification with financial monitoring platforms, regulatory authorities, financial institutions, and businesses can monitor transactions, detect suspicious activities, and mitigate risks more effectively. This combination strengthens financial systems' overall security and stability, reducing illicit financial activities, such as money laundering and terrorist financing.

The methodology. The methodological basis of the research was a set of methods of scientific knowledge. In particular, the phenomenological method allowed the author to analyse national, international, and foreign law legal sources. The analytical method was used during the analysis of the conceptual and categorical apparatus, the definitions of "artificial intelligence", "digital identification", "blockchain", etc. The author also used the method of analysis and generalisation, which made it possible to clarify and generalise views on the essence and types of digital identification for further use in financial monitoring.

2. General Concept of "digital identification"

Identification refers to the act of determining the identity of an individual within a given population. With the world rapidly moving toward a digital landscape, digital identities are imminent *(Kanwar, Reddy, Kedia & Manish, 2022)*. It involves answering "Who is this person?" and can be accomplished through various methods. For instance, one approach involves comparing a person's facial image with a database of multiple images. If the identified person is found within the database, it constitutes an identification. Conversely, it is considered a negative identification if the person is not found. Negative identification can be utilised to verify the absence of duplicates in a database, which is particularly useful for eliminating redundant registrations. This identification process is often referred to as 1-to-many or 1:N matching, or recognition *(Biometrics in Digital Financial Services: An Overview, 2017)*.

In general, McKinsey Global Institute researched digital identification as a key to inclusive growth. According to it, digital identification, or "digital ID", can be authenticated

unambiguously through a digital channel, unlocking access to banking, government benefits, education, and many other critical services (McKinsey Global Institute). Gratzer (2023) noted that "a digital identity allows identifying a person and thus facilities transactions in the digital world". A digital identity is one where most aspects of the system that enables it are accomplished digitally *(Kanwar, Reddy, Kedia & Manish, 2022).*

Also, we found the definition of a "digital identity" in Commonwealth FinTech Toolkit (2020). It was highlighted as a set of digital records that verify that an individual is who they say they are and allow them to engage in transactions in the modern, digital world.

We propose the next definition of the notion "digital identification" – as the process of using digital technologies to verify and confirm a person's personal identity in the online environment. Key aspects of digital identity include:

– biometrics. Digital identification can use biometrics such as fingerprints, facial recognition, iris scans, or voice data. This data can be stored in digital form and used to identify a person when accessing various services or performing financial transactions. According to the definition provided by Khushk and Iqbal (2015), biometrics refers to an automated approach for verifying or recognizing an individual's identity by leveraging physiological or behavioural characteristics. These characteristics can include unique attributes related to our physical traits, such as fingerprints, iris patterns, or facial features, as well as behavioural patterns, such as voice or signature. Biometric systems utilise these distinct attributes to establish a reliable and secure means of authentication, relying on the principle of "something we are" (referring to our physical traits) or "something we do" (referring to our behavioural patterns). Individuals can be accurately identified or verified by analysing and comparing these biometric traits, enhancing security, and enabling efficient access control in various applications and domains;

– unique identifiers. Each individual can be assigned a unique digital identifier that can be used for identification and authentication in the online environment. This identifier may be linked to biometric or other personal data that helps verify an identity;

– two-factor authentication. Digital identity can include two-factor authentication, which requires two independent ways to verify identity, such as a password and a one-time code sent to a mobile device. The combination of knowledge factors, such as a PIN, and the possession of a device has become increasingly popular in two-factor authentication (2FA) schemes *(Murdoch & Abadi, 2022).*

– security and data protection. With digital identity, it is important to ensure the security and protection of personal data. Using encryption, secure data transfer protocols, and access control measures helps prevent unauthorised access to personally identifiable information.

Digital identification typically involves collecting and verifying various types of information, such as personal details, biometric data (e.g., fingerprints or facial recognition), or unique identifiers (e.g., usernames or email addresses). This information is securely stored and used to establish a digital identity for each user.

3. Digital identification and financial monitoring

In finance, the matter of identity holds great significance for institutions. As we undergo a period of transformation, it becomes imperative for banks to establish robust and reliable digital identity systems that can mirror their existing expertise in verifying identities within the physical realm. The journey of transitioning from an analog identity model to a digital one is riddled with numerous challenges, including security issues, lack of interoperability, susceptibility to cyber-attacks, and a dearth of user control over personal data. From our perspective,

digital identity remains a distinctly human concept, distinguished by the self-awareness inherent to each individual *(Segovia Domingo & Enríquez, p. 4).* The decentralised nature of blockchain ensures that identity data is not controlled by a single entity, reducing the risk of data breaches or unauthorised access. Additionally, the immutability of the blockchain ledger makes it difficult for malicious actors to tamper with or manipulate identity information once it has been recorded. Blockchain technologies offer potential solutions to address various concerns related to digital identity. Blockchain allows for the unique authentication of identities through an immutable and secure ledger. The authentication process in blockchain relies on verifying identities using digital signatures based on public key cryptography *(ICAR, 2017).*

Biometrics, such as fingerprints or palm prints, have played a crucial role in enhancing security at Japanese ATMs. Prior to the availability of fingerprint sensors on high-end mobile phones, this technology was primarily utilized for user verification at ATMs. To access their accounts, users are required to present both their bank card and provide their biometric data *(Biometrics in Digital Financial Services: An Overview, 2017).* Biometrics, such as fingerprints or palm prints, have enhanced security at Japanese ATMs. Before the availability of fingerprint sensors on high-end mobile phones, this technology was primarily utilised for user verification at ATMs. To access their accounts, users must present both their bank card and their biometric data.

The FATF has developed guidance that help governments, financial institutions, virtual asset service providers and other regulated entities determine whether a digital identity (ID)is appropriate for use for customer due diligence (CDD) *(FATF Guidance on Digital Identity in Brief, 2020).*

Digital identification is used for financial monitoring in various aspects:

– client authentication. Biometric data such as fingerprints, facial recognition or eye scans can be used to authenticate customers before financial transactions. This allows you to confirm that the person trying to access financial resources is a legitimate user;

– opening bank accounts: Banks can use biometric identification to open bank accounts. Customers can provide their biometric data to verify their identity and prevent the creation of fake accounts;

– fraud detection: Biometric data can be used to detect fraudulent activities in financial transactions. For example, if a customer tries to carry out a transaction under the guise of another person, a biometric identification system can recognise the discrepancy and prevent abuse;

– regulatory compliance: Biometric identification can help financial institutions comply with regulatory requirements, such as anti-money laundering (AML) and counterterrorism (CFT) requirements. Collecting biometric data may be required for identity verification and financial crime prevention.

In FATF Guidance on Digital Identity in Brief (2020), it is noted that the potential of digital identity systems that adhere to rigorous technological, organisational, and governance standards is immense. These systems offer promising solutions for enhancing trust, security, privacy, and convenience when it comes to verifying the identity of individuals in various domains, including financial services, healthcare, and e-government, within the context of the digital era's global economy. To the FATF Standards, appropriately reliable, independent digital ID systems could: facilitate customer identification and verification at on-boarding support ongoing due diligence and scrutiny of transactions throughout the business relationship, facilitate other customer due diligence measures, and aid transaction monitoring to detect and report suspicious transactions, as well as general risk management and anti-fraud efforts *(FATF Guidance on Digital Identity in Brief, 2020).*

The use of digital identification in financial monitoring can have the following advantages:

– efficiency. Digital identification allows for automating identity verification and financial monitoring processes. This reduces the need to manually verify documents and identification data, increasing processing speed and efficiency;

– convenience for customers: Digital identification provides convenience to customers as they can go through the identification and verification process online without the need to visit physical offices or send documents by post. This provides quick access to financial services and reduces time and effort;

– fraud prevention: Digital identity is based on using biometrics and verifying other unique identifiers, making it difficult to forge or use false identities. This helps prevent fraud, fake accounts, and other financial crimes;

– improved accuracy and reliability of data: With the use of digital identity, it is possible to ensure more accurate and reliable information about customers and their financial data. This helps to reduce errors, improve data quality and ensure the reliability of financial monitoring;

– compliance with regulatory requirements: Digital identity can help financial institutions meet regulatory requirements related to customer identification and prevent financial crimes. It enables the collecting, storing, and transferring necessary data to comply with Anti-Money Laundering (AML) and Counter-Finance of Terrorism (CFT) requirements.

Financial monitoring uses various unique identifiers to identify individuals and monitor financial transactions. Some of them include:

– customer identification number, CIN. This is a unique number assigned to each bank or financial institution customer. It is used to identify the client and related financial transactions;

– account Number. Each bank account has its unique number that identifies the account and allows tracking of financial transactions related to that account;

– payment identification code, PIC. This is a code used to identify the person or organization making payment transactions. It can be used to track payments and monitor financial transactions;

– tax identification number, TIN. This number is assigned to an individual or legal entity in the country's tax system. It is used for personal identification and connection with financial data;

– identity document series and number. This includes the series and number of a passport, identity card, driver's license or other document used to identify an individual when carrying out financial transactions.

These unique identifiers make it possible to accurately identify individuals and track their financial transactions as part of financial monitoring. They contribute to the effective detection of fraud, money laundering and other financial crimes.

Two-factor authentication (2FA) is an effective tool for ensuring security in financial monitoring. It includes using two different identity verification methods to provide a higher level of protection.

In the context of financial monitoring, two-factor authentication can be used at different stages of the process:

– logging in. When trying to log into the system of a financial institution (for example, a bank), the user, in addition to entering his login and password, also provides a second authentication factor. This can be a one-time password received via SMS or mobile application, fingerprint, face scan or other biometric data;

– transaction confirmation. Two-factor authentication may be required when making financial transactions, especially for large amounts or unusual transactions. In addition to entering the necessary data, the user can receive a one-time verification code or use biometric data to verify his identity further.

Financial monitoring tools protect against money laundering, terrorist financing, and other financial crimes. By leveraging technology and data analysis, these tools empower authorities to track suspicious transactions, detect patterns of illicit activity, and disrupt the financial networks supporting criminal organisations.

4. Conclusions

Integrating digital identification and advanced financial monitoring technologies presents significant advancements in the ongoing battle against criminal activities. These technologies offer robust solutions for verifying identities, conducting due diligence, and monitoring real-time transactions. By leveraging digital ID systems, financial institutions can enhance security, detect and report suspicious activities, and manage risks more effectively. Combining these new technologies provides a powerful toolset to combat crime and foster a safer and more trustworthy financial ecosystem. As these technologies evolve, regulatory bodies, financial institutions, and technology providers must collaborate to ensure effective implementation and adherence to global standards, ultimately contributing to a more secure and resilient financial landscape.

References

1. Biometrics in Digital Financial Services: An Overview (2017). Reducing Poverty through Financial Sector Development. Report. URL: https://www.fsdafrica.org/wp-content/uploads/2019/08/Biometrics-in-finance-03.08.2017.pdf. Accessed 09 Jun 2023.
2. Commonwealth FinTech Toolkit. Helping Governments to Leverage Financial Innovation (2020). The Commonwealth Secretariat. URL: https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/migrated/inline/Commonwealth%20Fintech%20Toolkit.pdf. Accessed 13 Jun 2023.
3. ICAR (2017). Blockchain technology and its effect on the financial industry. URL: https://www.icarvision.com/en/blockchain-technology-and-its-effect-on-the-financial-industry. Accessed 03 Jun 2023.
4. FATF Guidance on Digital Identity in Brief (2020). URL: https://www.fatf-gafi.org/media/fatf/documents/reports/Digital-ID-in-brief.pdf. Accessed 15 Jun 2023.
5. Gratzer, N. (2023). Digital identity: The Complete Guide to Digital Identification. Adnovum. URL: https://www.adnovum.com/blog/digital-identity Accessed 14 Jun 2023.
6. McKinsey Global Institute. Digital identification: A key to inclusive growth. URL: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-In-brief.pdf. Accessed 04 Jun 2023.
7. Kanwar, Sh., Reddy, A., Kedia, M. & Manish, M. (2022). The Emerging Era of Digital Identities: Challenges and Opportunities for the G20. Asian Development Bank Institute Policy Brief. No.2022-3 (August). URL: https://www.adb.org/sites/default/files/publication/822681/adbi-brief-emerging-era-digital-identities-challenges-and-opportunities-g20.pdf. Accessed 18 Jun 2023.
8. Khushk, K. & Iqbal, A. (2005). An Overview of Leading Biometrics Technologies Used for Human Identity. In Engineering Sciences and Technology, 2005. SCONEST 2005. Student Conference on. pp. 1-4.
9. Murdoch, St. J., & Abadi, A. (2022). A Forward-secure Efficient Two-factor Authentication Protocol. URL: https://discovery.ucl.ac.uk/id/eprint/10153744/7/Abadi_2022-1006.pdf. Accessed 05 Jun 2023.
10. Segovia Domingo, A. I. & Enríquez, Á. M. Digital Identity: the current state of affairs. No. 18/1. URL: https://www.bbvaresearch.com/wp-content/uploads/2018/02/Digital-Identity_the-current-state-of-affairs.pdf. Accessed 02 Jun 2023.