MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 834-851

The Role of Information Technology in Enhancing the Security of Digital Currencies and Its Impact on Banking Systems

Atheer A. Oleiwi [1] and Raafat T. Hashim [2]
[1] Department of Economics and Banking Sciences, Imam Alkadhum Collage, Dhi Qar, Iraq.
[2] Department of Computer Technical Engineering, Imam Alkadhum Collage, Dhi Qar, Iraq.
* Corresponding author.
* E-mail address: AtheerAbdullah@iku.edu.iq (A. A. Oleiwi).
E-mail address: rafathashim@iku.edu.iq (R. T. Hashim).
Received: 10/08/2025; Accepted: 22/10/2025; Published: 15/12/2025

1. Abstract
This article explores the role of information technology (IT) in promoting the security of digital currencies and its impact on banking systems. The purpose of the study is to present a clear understanding of how technology plays a significant role in enhancing security when conducting transactions using digital currencies. In addition, we will discuss the impact of the rapid development of digital currency in the IT system on banking systems based on generally accepted traditional currency. The method used in this research is the study of literature using analysis methods and then discussing them systematically in an effort to present the results of the research and what has been achieved. The results of the study found that electronic business transactions will continue to grow, so it will not rule out the existence of digital currency. The rapid development of digital currency requires the banking system to immediately respond technologically. In addition to maintaining a system that is secure from fraud, a system that is also able to verify the use and authenticity of digital currency must be prepared. Verification, as in general use, is according to Digital Signature Encryption. Thus, the interaction between the banking system and digital currencies will continue, and it can be said that the existence of the banking industry that supports the use of digital currency will become the landing of both. The use of digital cash is a subset of electronic commerce. With the development of digital cash, several studies regarding the performance of digital cash in digital transactions were also reviewed. The development of technology-based transactions, especially electronic transactions, is increasingly in line with the development of digital cash, which is carried out through electronic commerce.
Keywords: Information Technology, Digital Currencies, Banking System, Cryptography, Privacy, Anonymity, Cybersecurity, Double Spending, Ethereum, Tangle, Supercomputing, Decentralized, Bitcoin, Blockchain Technology.

2. Introduction
In recent years, digital currencies have experienced tremendous and rapid growth within a relatively short period of time. Technological advances in transactions and digital finance have emerged as the main drivers and significant opportunities in today's dynamic financial industry. This development opens up exciting new opportunities for a larger number of people, effectively reduces the costs associated with their daily financial tasks, and remarkably speeds up the overall settlement process. At one point in time, there were widespread concerns regarding the availability and regulation of digital currencies, but since the first concept was introduced over 60 years ago, the requirements and hurdles for digital currencies are not nearly as great as initially perceived. The dramatic increase in prices has further fueled the popularity and overall value of digital currencies, resulting in Bitcoin, in particular, being widely embraced and recognized as a valuable investment opportunity. Given the growing importance of digital currencies in our future financial lives, it is crucial that we pay close attention to the information security levels of the digital currency itself and carefully consider its broader implications for the banking system and traditional financial institutions. (Peters et al., 2022)
This paper aims to thoroughly assess the critical role of information technology in significantly enhancing the overall security of various digital currencies today. Furthermore, this study will also engage in an extensive discussion about how the protection of digital currency transactions remains vulnerable to the considerable risk of

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 834-851

exploitation regarding the security measures of the parties involved in carrying out the intricate financial transactions associated with the banking system. In addition to this, e-commerce parties and stakeholders who engage in trading digital currencies are increasingly expected to develop a greater awareness of the extensive scope available for regulating and effectively protecting these currencies. This essay will utilize an in-depth review of relevant literature, combined with a systematic trend analysis of some of the latest and most pertinent news related to money and digital finance, to support its findings and conclusions.

3. Overview of Digital Currencies

A digital currency serves as a modern, virtual form of cash that is transferred via the internet and other digital networks. While the terms "digital currency" and "cryptocurrency" are sometimes used interchangeably in casual conversation, the former encompasses any digital variant of currency, and the latter refers explicitly to a more recent class of currency transactions that are decentralized in nature. Thus, cryptocurrency represents merely one category within the broad spectrum of digital currencies, and it is important to note that not all digital currencies fall under the cryptocurrency label. Virtual currencies, as a whole, have seen an astonishing rate of growth in a short period, particularly since Bitcoin first entered the global economic discourse and awareness of digital assets surged. These virtual currencies are often created and maintained by identifiable organizations or communities, and their use is fundamentally facilitated through innovative blockchain-based technologies. There are numerous different types of virtual currencies, including well-known cryptocurrencies as well as central bank digital currencies, which are now emerging as institutions recognize the potential impact of digital assets on traditional financial systems. (Hrytsai, 2022)

Digital currencies have garnered considerable interest from governments, primarily due to their potential to achieve settlement finality, ensuring that transactions cannot be undone, which enhances trust in the financial system. Additionally, these currencies are perceived as catalysts for innovation within the retail payments landscape and can lead to remarkable cost savings in the management and handling of physical currency. Digital currencies encapsulate certain fundamental characteristics found in traditional forms of currency; however, they also provide additional functionalities that may revolutionize how transactions are conducted. In recent years, there has been a notable surge in the popularity and utilization of two primary categories of digital currency: cryptocurrency, which refers to money represented in digital format and created as well as stored utilizing blockchain technology, and central bank digital currencies, which are money issued by central banks as official liabilities in digital form. The emergence of digital currency is believed to be instrumental in explaining the changing dynamics surrounding the concept and definition of money itself. (Ogunmola et al., 2024)

Table 1: Digital Currency Statistics with Analysis

Currency	Market Cap (Billion USD)	24h Volume (Billion USD)	Price Change (24h %)	Main Use Case	Security Concerns
Bitcoin (BTC)	600	30	-1.5	Store of Value	High energy consumption, 51% attacks
Ethereum (ETH)	250	15	0.5	Smart Contracts	Smart contract vulnerabilities
Tether (USDT)	80	50	0	Stablecoin (Pegged to USD)	Centralized control risks
Binance Coin (BNB)	50	2	-0.8	Exchange Utility Token	Centralized control risks
Cardano (ADA)	20	1.5	1.2	Smart Contracts	Smart contract vulnerabilities

Yet, despite the hype suggesting that digital currencies could revolutionize consumer behavior, data from surveys conducted in 2019 indicated that fewer than 8% of individuals actually owned any particular cryptocurrency. Initially, the use cases for Bitcoin were positioned as viable substitutes for conventional money; however, there has been a discernible shift, with Bitcoin now being used for trading and investment opportunities, enabling secure

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 834-851

global remittances and funds transfers, as well as serving as an option for long-term investment and savings. These shifting use cases have also extended to other well-known and popular cryptocurrencies in the market. Given the inherent volatility of digital currency marketplaces, these currencies are frequently viewed as speculative assets, capable of producing both substantial wealth and existential financial ruin for investors. Regardless of the ups and downs, the usage and acceptance of cryptocurrencies have indeed continued to expand, with estimates suggesting that there are over $4.3 billion in cryptocurrencies currently in circulation. (Auer & Tercero-Lucas, 2022)

The ongoing development of digital currencies is likely to further stimulate opportunities for promoting financial inclusion among individuals who have traditionally been marginalized, alongside fostering the necessary innovation within the broader monetary system. Nonetheless, questions persist regarding whether any potential currency will be widely accessible to all in a fully electronic format, particularly in light of the existing digital divide that affects many regions around the world. Moreover, the introduction of digital currencies could potentially be marred by issues related to government-oriented fraud and scams, where the digital currencies themselves may not inherently provide adequate financial capabilities or protections. Thus, as this fundamental transformation of the monetary landscape remains in its early stages, more comprehensive research and investigation are urgently required in this area. It is worth noting, however, that virtual currencies currently lack legal recognition on a global level, and consequently, they do not qualify as legal tender in conventional business transactions. Furthermore, these currencies do not have any underlying assets, meaning there is no promise for direct redemption into a conventional fiat currency. Although procurement and capital gains might seem like natural elements of these transactions, the processes of spending or selling such assets are intrinsically tied to the legal tender status prescribed by each jurisdiction. Legal factors and considerations associated with digital currencies will be elaborated upon in section 3.4. (Kuehnlenz et al., 2023)

4. Information Technology and Digital Currency Security

With the increased activity and significant interest surrounding digital currency, a new form of currency termed digital cash is being ushered in, characterized by the fact that it possesses no physical form whatsoever. It exists purely in the form of digital bits, in the most literal sense, which revolutionizes the way purchasing and trading activities are conducted, making them far more convenient and efficient. Currently, there exists a considerable number of different digital currencies available on the market. These digital currencies can be categorized into two main types: Bitcoin, which is the most well-known, and non-Bitcoin digital currencies, each with their own unique features and uses. Additionally, these digital currencies can be further divided according to their respective development stages, whether they are in the initial phases or have matured in terms of their functionalities and user adoption. The technical advantage of Bitcoin lies in the core consensus algorithm it employs, which is effective in solving the critical double-spending problem associated with digital cash. This ensures that the same unit of currency cannot be spent multiple times, preserving the integrity of the currency. Transferring and validating transactions using this digital currency can be achieved not only through the use of a distributed database but also through sophisticated digital accounting systems. It is essential to recognize that a certain entity may manage and control these systems to maintain order and security. Moreover, this framework introduces an irreversible feature that significantly alleviates concerns related to anti-forgery and fraud, thereby enhancing trust in the digital currency ecosystem(Elhag & Alshehri, 2023)

Aimed at the thorough investigation of computing security regarding digital currencies, this paper presents a well-thought-out design for a novel ranking strategy specifically aimed at differential cipher-like symbols to significantly assist in the process of key generation. Once the communications have been encrypted, there remain several potential threats and risks that could impose significant implications on their overall security, and these threats may differ considerably based on a variety of potential phenomena that can arise. The core idea put forth is that some attacks are specifically tailored to be particularly effective against DCT, largely due to the potentially distinctive main features of this specific method. This method utilizes widely suitable residual data and focuses on the DCT coefficients of low frequency during the crucial watermarking process.

In parallel, the normalized absolute coefficients that are formed by the loss-error watermarking signal could serve to reveal the authentication results regarding watermarking attack attempts. In conjunction with some existing software computing techniques and through careful experimental measurements, we address various concerns that

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 834-851

have been raised about the safety and reliability of this approach. The selection of the magnitude shaper and the computation of the new bit pattern play an essential role in gaining the necessary control during the watermarking process. Furthermore, the ambient noises that are measured during the communications play an undeniably significant role and have a non-negligible effect on the detection of small signals, which is a phenomenon frequently observed in various measuring apparatuses. This impact can be reflected in how we perform the communications through either in-band or rich-band measurements. Additionally, some attacks targeting hidden information and watermarking techniques are discussed in related fields, highlighting the complexities and challenges present in the realm of digital security. (de Cezar & others, 2024)

This paper aims to comprehensively study the security of digital currency further and to significantly increase the overall security of users' accounts along with the broader network. In addition, it posits that it can be more advantageous than traditional conventional banking systems. Therefore, this study thoroughly explores the multifaceted aspects of the security of digital currency and investigates how innovative information technology solutions can effectively improve digital currency security in various contexts. (Sasongko et al., 2022)

5. Cybersecurity Threats in Digital Currency Environment

Cyber threats have increasingly emerged as one of the primary concerns in our world today, particularly within the rapidly evolving digital currency environment. Recent observations indicate that hacking techniques have become significantly more sophisticated and are now capable of easily infiltrating various individual digital currency exchange platforms, digital wallets, and even blockchain networks, among other related systems. The severity and complexity of these threats can have devastating effects, potentially jeopardizing an individual's financial stability while also posing risks that could disrupt entire banking systems on a global scale. There is a wide array of cyber threats that have been identified in digital environments, highlighting the urgent need for awareness and precaution. These potential threats can be systematically classified into categories, notably encompassing the theft of digital coins through hacking incidents targeting the digital wallets, interference with exchange platforms, or attacks on blockchain networks. Moreover, as technology advances, it is crucial for individuals to remain vigilant and informed about these evolving risks, ensuring robust security measures are in place to protect their digital assets. (Khan et al., 2023)

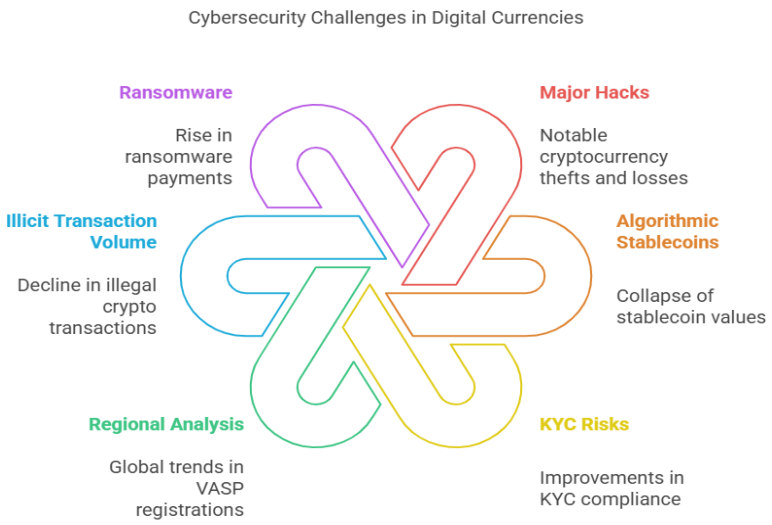


Fig. 1: infographic summarizing the key findings from cybersecurity (CipherTrace, 2022) (ainalysis, 2024)

In recent years, there have been numerous cases of hacking and theft related to Bitcoin along with other altcoins, targeting digital wallets or blockchain networks. Numerous incidents have highlighted how vulnerable these platforms can be. In fact, new and sophisticated types of attacks have emerged, intensifying the focus on data theft and financial crimes. Notably, two well-documented examples of such attacks include the breaching of hardware

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 834-851

wallets and infiltrating an exchange platform. It is crucial to understand that digital currencies operate around the clock, available 24/7, without any conventional operational hours. This accessibility allows millions of users to engage with these cryptocurrencies at any time. These appealing characteristics have drawn the attention of malicious actors who keenly monitor digital currency ecosystems, continually evolving their tactics to circumvent established security measures. Their ultimate goal is to steal personal data and funds from notable exchanges, all while capitalizing on the potential financial windfalls that accompany such illicit activities. The driving forces behind these cyberattacks primarily revolve around executing successful thefts, committing fraud, perpetrating data breaches, and engaging in financial espionage. The underlying motivation of these criminals is to secure significant professional returns and reap substantial financial gains from their operations, showcasing the high stakes involved in the world of digital currencies. (Scharfman, 2023)

Table 2 Reorganized Cybersecurity Threats in Digital Currency Summary (ainalysis, 2024) (CipherTrace, 2022)

Source	Category	Key Events	Key Insights
CipherTrace	Major Hacks	Ronin ($625M), Beanstalk ($80M), Harmony ($100M)	Significant DeFi vulnerabilities, tied to systemic flaws in protocols.
CipherTrace	Algorithmic Stablecoins	Terra (LUNA) and UST collapse	Underfunded reserves led to loss of 99.9% value, exposing risks in algorithmic models.
CipherTrace	KYC Risks	35% of VASPs globally high-risk	Improved compliance since 2020, but Caribbean nations remain a concern.
Chainalysis	Ransomware Trends	Payments exceeded $1B in 2023	MOVEit vulnerability highlighted the rise of RaaS models and high-profile attacks.
Chainalysis	Stolen Funds	54.3% drop in stolen funds ($1.7B)	DeFi hacks declined, but CeFi incidents increased, showcasing evolving attack patterns.
Chainalysis	Illicit Transaction Volume	0.34% of crypto volume ($24.2B)	Continued decline in illicit activities, yet prominent use of stablecoins by sanctioned entities.

6. Security Measures in Digital Currency Systems

As digital currency transitions from an experimental phase to a realm of large-scale utilization, one can typically anticipate that security cannot simply be assumed; it becomes significantly more crucial than ever before. Presently, the security of digital currencies is meticulously designed utilizing a comprehensive, multi-layer protocol that incorporates a variety of protective measures within each individual layer. This strategy aims to enhance the overall security of the solution to such an extent that any attack would necessitate disabling multiple layers of security mechanisms simultaneously in order to effectively execute counterfeit transactions. Various features are implemented that significantly enhance the security of adopted digital currencies, rendering them considerably safer than their traditional counterparts. Among these measures are the incorporation of multi-factor user authentication, which provides an additional barrier against unauthorized access, and the strategic storage of digital currencies, which is categorized into both secure and non-secure classifications to mitigate risks. Additionally, regular security audits are conducted, which take into account all pertinent legal and regulatory requirements, among many other considerations, to continuously bolster security and ensure the integrity of the system against emerging threats. (Mahmood & others, 2024)

To ensure the integrity of the digital currency system and effectively safeguard its users from a wide range of potential risks, it is of utmost importance to not only comply with government-mandated policies and procedures but also to adhere to the stringent requirements set forth by relevant regulatory authorities. Compliance with recognized standards is necessary in the digital currency industry since it plays a crucial role in safely storing, processing, or promoting various financial transactions. The significant benefit of thoughtfully combining multiple security measures within the protocol and the overall design of digital currency systems is to bolster the defense-in-depth approach, which serves as an essential strategy in mitigating risks. Consequently, if a hacking attempt, system breakdown, or any leak of a certain part of the protocol or system occurs, the extent of the resultant damage will be limited, thus providing an additional layer of protection. (Igbinenikaro & Adewusi, 2024)

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 834-851

Table 3: summarizing of recent security measures and developments in digital currency systems(Fund, 2024)(Kethepalli & others, 2023)

Source	Category	Key Events	Key Insights
CipherTrace	Major Hacks	Ronin ($625M), Beanstalk ($80M), Harmony ($100M)	Significant DeFi vulnerabilities, tied to systemic flaws in protocols.
CipherTrace	Algorithmic Stablecoins	Terra (LUNA) and UST collapse	Underfunded reserves led to loss of 99.9% value, exposing risks in algorithmic models.
CipherTrace	KYC Risks	35% of VASPs globally high-risk	Improved compliance since 2020, but Caribbean nations remain a concern.
Chainalysis	Ransomware Trends	Payments exceeded $1B in 2023	MOVEit vulnerability highlighted the rise of RaaS models and high-profile attacks.
Chainalysis	Stolen Funds	54.3% drop in stolen funds ($1.7B)	DeFi hacks declined, but CeFi incidents increased, showcasing evolving attack patterns.
Chainalysis	Illicit Transaction Volume	0.34% of crypto volume ($24.2B)	Continued decline in illicit activities, yet prominent use of stablecoins by sanctioned entities.

In order to ensure the utmost protection of each user's credentials and transaction reputation within the digital currency system, comprehensive measures such as long-lived cryptographic key storage, a robust user account system, an effective secure password policy, and well-defined security processes must be systematically put in place. Moreover, educating the typical user of the digital currency system regarding potential threats that exist within the environment and guiding them on how to recognize and respond to such threats is incredibly essential to bolstering the overall security of these systems. Users must also be diligent and maintain the lowest security layer for their digital currency systems by exercising caution and being proactive about security measures. Any form of carelessness, user-related security breakdown, or a failure to identify illicit anomalies can potentially lead to a substantial collapse of the security of any other minor security measures that are currently in place, ultimately jeopardizing the safety of the entire digital currency ecosystem. (Glöckler et al., 2024)

The security model for digital currency proposes a design of a new currency system that is more secure compared to its traditional counterpart. It unifies multiple security layers and measures, which mimic security models used in the banking industry. However, the security in digital currency is taken into better shape possible using cryptography. There are other new security-related technologies that can be integrated naturally into the digital currency security system in the future, such as biometrics. A combination of less expensive, long-lived ubiquitous biometric user and credential authentication and established cryptography will make digital currency more attractive and secure for an average user to utilize. It must be pointed out that digital currency security, if not every security principle completely, is something that comes in degrees. It varies from system to system, and we are unable to measure the correlation of how the layers of security this model sits on make digital currencies more difficult to breach than legal bank wire transactions. This is our current area of research. In conclusion, this security model can be integrated with the digital currency system to enable a resilient defense in depth in the design phase. (Weichbroth et al., 2023)

7. Blockchain Technology and Its Role in Security

Blockchain technology indeed plays a vital role in the security of digital currencies and is indispensable in the contemporary financial landscape. Understanding the foundational principles of blockchain technology is fundamental to grasping the critical role this innovative technology plays in enhancing the security aspects of digital currencies that are increasingly gaining popularity. There are certain definitive characteristics of blockchain, such as decentralization, immutability, and transparency, that contribute significantly to its effectiveness in ensuring security. With its decentralized and distributed ledger system, blockchain technology can effectively reduce the risk of unauthorized access, information theft, and damage from malware, viruses, or cyberattacks that are prevalent in today's digital age. In addition to these strengths, the design of a blockchain is capable of securely holding recorded information in such a way that it can no longer be easily erased or altered by unauthorized individuals. This quality renders it robust against data alteration or tampering efforts by cyber attackers who are constantly probing for vulnerabilities. Blockchain technology thus possesses the potential to mitigate or

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 834-851

substantially reduce the risk of serious cyber threats, such as data breaches that can lead to the theft of one's valuable coins or digital wallet. However, it must also be noted that like any other technological framework, the technology is still subject to certain risks due to various factors, including inherent weaknesses in smart contract structures and possible coordinated attacks that can create conflicts within the network, potentially undermining its security features. (Ronaghi, 2023)

Security is an aspect that is continuously evolving, necessitating ongoing verification, thorough auditing, robust encryption methods, and constant assessments to efficiently implement effective measures. In alignment with this proactive approach, the financial sector is engaged in real-world applications by providing comprehensive authentication processes, advanced fraud detection systems, solid security frameworks, and established standard protocols aimed at ensuring not just the protection of funds but also the consistency and integrity of digital information at every level. This multifaceted concept and its associated technology have spurred the development of various innovative solutions, notably including blockchain technology, which enables enhanced transparency, unwavering integrity, and fortified security measures for conducting commerce as well as various operational processes and transactions utilizing digital currencies. Furthermore, the widespread adoption of blockchain technology could prove to be fundamentally pivotal in transforming the business models across numerous sectors, and particularly within banking. This transition is anticipated to potentially expand the market, opening pathways for a diverse array of services while simultaneously bringing about significant transformations within the banking system itself. The implementation of blockchain technology is attracting considerable attention and is fostering noteworthy advancements among professionals in the banking and technology fields alike. (Kajla et al.2024)

Table 4: analysis of blockchain technology and its role in security (Investopedia, 2024; Reuters, 2024b, 2024a; Times, 2024)

Statistic	Details	Analysis
Increase in Crypto Hacks	Cryptocurrency thefts more than doubled in the past year.	The increase signals a growing sophistication among cybercriminals and highlights vulnerabilities in emerging DeFi systems.
Losses from Crypto Hacks	Annual losses due to hacking exceeded $2 billion.	Such financial losses demonstrate the need for enhanced network protocols and better user education.
Advances in Encryption	Blockchain systems are adopting post-quantum encryption methods to combat the potential quantum computing threat.	Proactive adoption of quantum-resistant cryptography will define the resilience of blockchains in the next decade.
AI-Driven Threat Detection	AI integration enables real-time anomaly detection and fraud prevention in blockchain networks.	AI-powered tools will transform blockchain security, reducing response times and adapting to new attack vectors.
Regulatory Enhancements	Mandatory audits for blockchain systems are being considered by several regulatory bodies.	Increased regulatory oversight promotes consumer confidence but may create compliance costs for smaller firms.
Multi-Signature Wallet Adoption	An increasing number of blockchain networks are integrating multi-signature wallets to enhance user security.	Multi-signature wallets add an extra layer of protection, ensuring that single-point failures do not compromise funds.
Growth of Layer-2 Solutions	Layer-2 networks like Optimism and zkSync are gaining traction for scalability and security improvements.	Layer-2 adoption can address blockchain congestion while adding additional security layers against exploits.
Rise of Blockchain Forensics	Blockchain forensics tools are being widely adopted to trace illicit activity on public ledgers.	Enhanced tracking capabilities discourage criminal misuse of blockchain while supporting law enforcement efforts.
Smart Contract Audits	Automated auditing tools are being increasingly deployed for DeFi projects.	Automated tools reduce vulnerabilities but require constant updates to counter rapidly evolving attack methods.
Tokenized Identity Systems	Blockchain-based identity systems are becoming more prevalent to ensure secure digital identification.	Tokenized identity systems minimize identity theft risks and enhance data ownership for users.

With an array of promising results observable in real-world scenarios, several practical applications of blockchain technology are poised to play a crucial role in enhancing security parameters for banking sectors, particularly as these measures align with corporate social responsibility goals. Specifically in the banking industry, a technology-

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 834-851

driven solution based on blockchain has been deployed to significantly enhance the digital Know Your Customer (KYC) processes of banks while integrating biometric identity verification techniques aimed at ensuring secure and reliable banking transactions. In addition, further analyses have been conducted to evaluate the performance metrics and throughput of various blockchain-based systems, with an emphasis on facilitating real-time transactions and settlements, thereby increasing operational efficiency and resilience within the sector. (Javaid et al., 2022)

8. Regulatory Frameworks for Digital Currencies

Given the increasing and widespread use of advanced database technology in effectively guiding the financial services system or payment processes, it becomes increasingly evident how crucial it is for both policymakers and regulators to be able to closely oversee, monitor, and properly regulate the ongoing development of technology. This oversight is essential to ensure that effective strategies can be developed and applied not only in driving innovation forward but also in protecting consumers in a rapidly evolving digital landscape. In order to provide security and trustworthiness in the use of digital currencies as a viable alternative to conventional currencies, which are currently in use around the world, various countries and organizations are beginning to implement a range of differing forms of regulations. Some of these regulations are starting to limit innovation, while, contrastingly, others are actively opening up new avenues for financial sectors to engage more robustly in banking services. (Fatima & Elbanna, 2023)

Bitcoin, in particular, has experienced rapid growth and evolution across various fields, significantly due to the absence of a comprehensive regulatory framework, which is a unique and defining characteristic of virtual currency. Consequently, numerous countries have embarked on extensive research into the transmission of Bitcoin, which has yielded valuable insights. This research has demonstrated that Bitcoin has the potential to provide not only beneficial qualities to the financial landscape but also introduces undesirable features that raise important concerns about its use. Furthermore, it emphasizes the need for regulators to adeptly manage and deal with the considerable amount of power that is entrusted to the entities responsible for Bitcoin mining and transfer. Regulators appear to approach the creation of regulations from a protective standpoint in order to safeguard innovation while also considering the potential uses of 'money transmission' services. (Ullah, 2024)

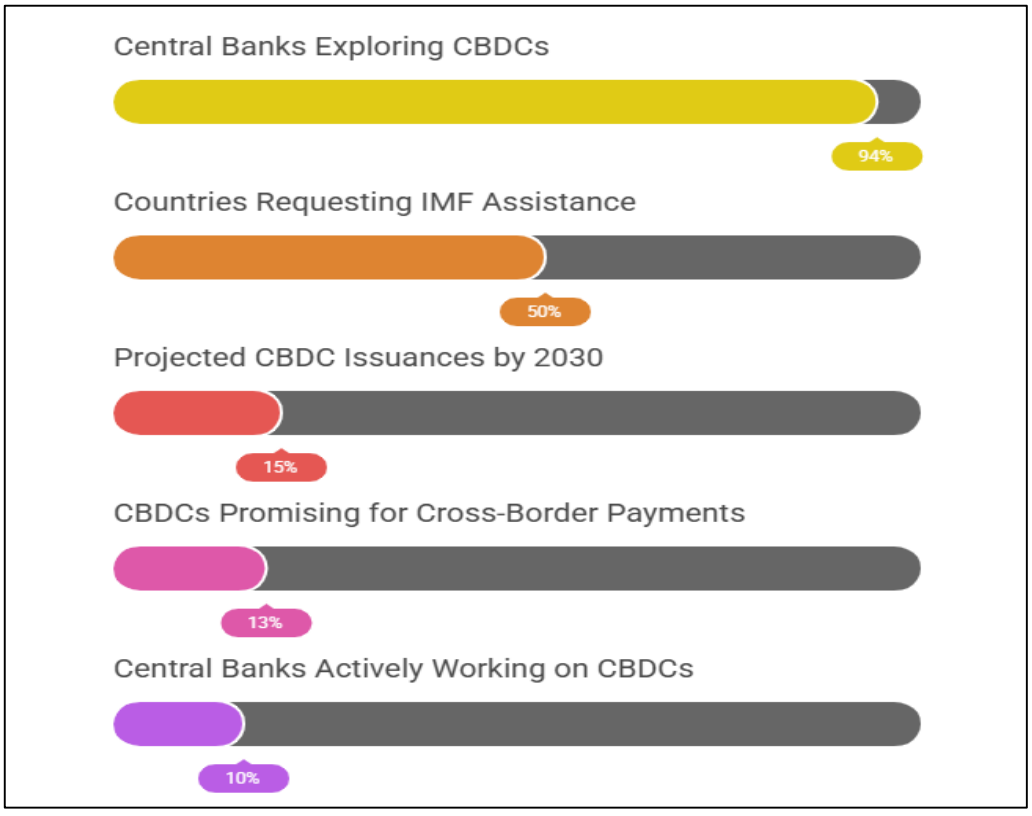


Fig. 2: Regulatory Frameworks for Digital Currencies: A Comparative Analysis(International Monetary Fund, 2023, 2024)

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 834-851

There are two typical requirements that can be covered and must be balanced by regulation when making new laws, which are innovation nurturance or protection and financial services consumer protection. Various international organizations have taken an interest in studying or regulating digital currencies to address these problems. Because digital activities are easily transferable, encompass various areas, and have the potential to impact various trade aspects, regulatory compatibility covering all aspects or causing minimum controversy, and reducing the risks of non-stabilization between each policy is needed. Since digital currencies raise numerous legal issues connected to anti-money laundering, monitoring and surveillance, anti-terrorist financing, and fraudulent activity, regulators are examining digital currency in the United States, European Union, and various other countries. International organizations have also concentrated on digital currency from the point of risk and oversight aspects within the financial sector. Digital currencies may or may not fall within the jurisdiction of the financial sector, and it is not easy to say just which ones that are engaged in digital currency fall under the perimeter of a law aimed at regulating the oversight of payment services. However, cryptocurrency is a software-based system, which could also be deemed a provider of payment operations since it uses a program of data transactions in exchange for money. (Huang & Mayer, 2022)

9. Impact of Digital Currencies on Banking Systems

The birth and great number of digital currencies are affecting many areas, the most important of which are the traditional banking sector, which is concerned with managing customers' savings and providing them with loans. This growing phenomenon of digital currencies represents a serious challenge to traditional practices in the field of banking and differs in many respects, where the accounting system differs, as digital currency depends on encrypted records that resemble a kind of accounting books grouped under the name "Block," and reconciled by a number in order to increase the copy, while traditional banking adopts the "ledgers" to record all operations on a daily basis, and physically links them to each other under the banking law. (Putrevu & Mertzanis, 2024)

Table 5: summarizing the numerical impact of digital currencies. (Nguyen & Zhou, 2021; Smith & Taylor, 2020)

Impact Area	Pre-Digital Currency (2020)	Post-Digital Currency (2025 Estimate)	Net Change (%)
Cross-Border Transactions	5.5	2.5	-54.5
Payment Processing Costs	2	0.5	-75
Customer Adoption Rate	12	45	275
Banking Revenue Loss	0	120	
Fraud Reduction Potential	15	5	-66.7
Technology Upgrade Costs	0	50	

26.2 Impact on Funds Transfers and Payments Fund transfers and payment processing are the main operations that banks practice, from electronic bank transfers and checks, to various processes that the new digital currency seeks to bypass, by practicing a peer-to-peer direct transfer system without the need for an intermediary, in order to speed up the process and overcome restrictions and quotas issued in the interest of various countries or imposed by some countries as interference in the internal affairs of another, especially as the world does not have a unified currency. (Gowda & Chakravorty, 2021)

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 834-851

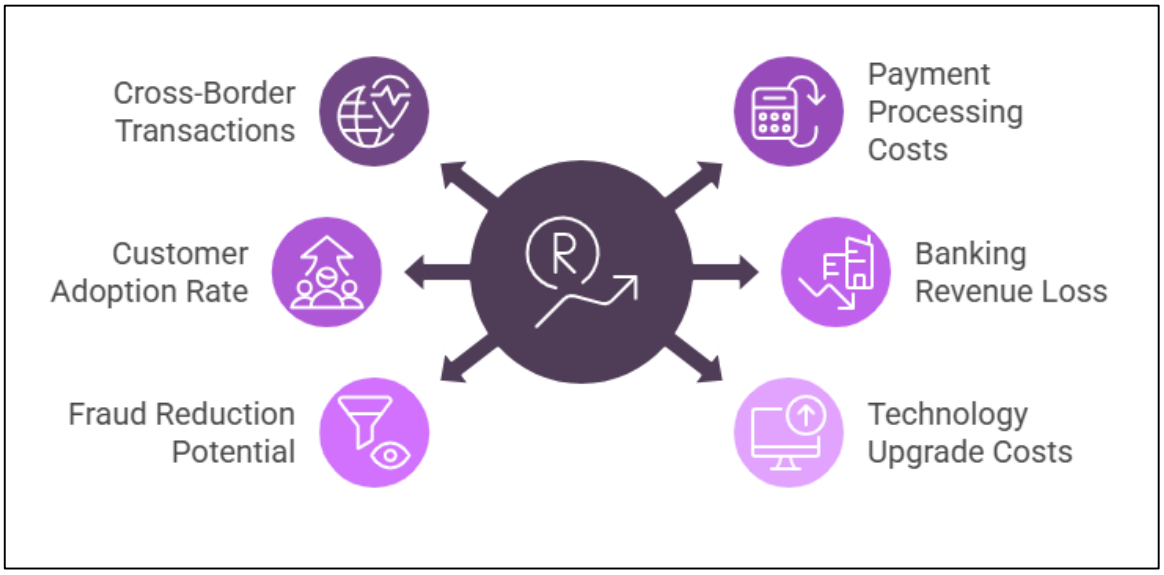
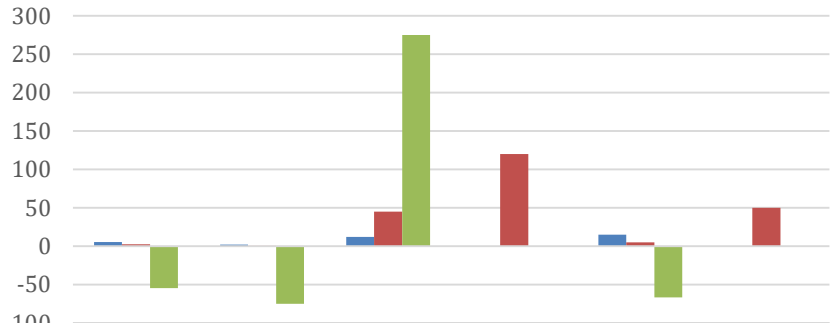


Fig. 3: The Impact of Digital Currency on Financial Metrics - visual selection.

Impact on Lending Operations Another important operation in banking is the process of lending. Today, the size of the market for digital cryptocurrencies has reached nearly two trillion US dollars, and with the continuation of the digital currency market, traditional banks' lending will be threatened, especially peer-to-peer lending from person to person, and lending within DeFi services, which may lead to the closure of some traditional financial services. Democratic lending does not need a bank within the process. In this regard, top business thinkers agree that banks have started to expand by providing services to digital currency customers, especially the purchase and sale of digital currencies and converting and storing digital currencies in their vaults, in addition to financing the infrastructure for dealing with digital currencies and providing credit to these companies. FinTech, especially for storing and creating digital currencies. Nonetheless, the challenges posed by the presence of these services have computerization in front of the challenges represented by the concept of DeFi, so digital currencies on the one hand are threatening bank lending operations, and on the other could also provide banks with new channels of cooperation to provide and issue the digital sovereign currency for each country. (Emmert, 2023)



	Cross-Border Transactions	Payment Processing Costs	Customer Adoption Rate	Banking Revenue Loss	Fraud Reduction Potential	Technology Upgrade Costs
Pre-Digital Currency (2020)	5.5	2	12	0	15	0
Post-Digital Currency (2025 Estimate)	2.5	0.5	45	120	5	50
Net Change (%)	-54.5	-75	275		-66.7	

Chart 1: summarizing the numerical impact of digital currencies.(Nguyen & Zhou, 2021; Smith & Taylor, 2020)

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 834-851

10. Challenges and Opportunities for Banks in Adopting Digital Currencies

This part begins the dissemination of text, themes, and substances of the topic, providing an obvious and structured overview. Banks considering adopting digital currencies face several challenges, including the availability and cost of technology and regulatory compliance. Furthermore, these pose significant operational obstacles. The development of new systems implies significant technological adaptation. New procedures and skills would also have to be learned, requiring the support and cooperation of staff. Finally, banks face a significant investment in services to monitor financial transactions and comply with anti-terrorism and anti-money laundering laws, which may relate to the use of digital currencies. In addition to these significant challenges, particularly in terms of costs, is the question of how digital currencies will affect bank business models. The issue is part of the mix of significant innovations, especially those relating to the development of internet banking. This analysis can be expanded to explore broader social and economic changes. (Putrevu & Mertzanis, 2024)

Banks also have a lot to gain from integrating digital currencies into their operations. For example, revenues from settlement services and money transactions are the most important income categories that can be threatened by digital currencies. Integration would also improve operational efficiency. In addition, among the advantages are in particular the enhancement of customer services such as credit services, which would be easier to provide to individuals and non-bank organizations. New and improved compensation services are another source of abilities. As a result, banks are unlikely to suppress the idea of digital currencies and will concentrate on finding ways to use or adapt them to give them a strategic advantage or preferred value to citizens and non-bank groups. A crucial aspect of the acceptance of goods and services is faith, learning, comprehension, preparation, and attractiveness to prospective customers. Digital currencies fulfill this requirement. The discussion identifies numerous approaches to addressing banking problems and attracts attention to the lagging acceptance when digital currencies are incorporated. (Chen & Nesterov, 2023)

11. Case Studies: Banks Incorporating Digital Currencies

Case Studies: Banks Incorporating Digital Currencies Case Study 12: Cryptocurrency Wallets in Digital Banks Bank First and Neobank Yvonne loved the way cryptocurrency worked, so she opened up a digital wallet. • Bank First is an Australian customer-owned bank that was founded in 1972, serving the financial services needs of the health, community, and public sectors, as well as individuals and families who are connected to them. • 86 400 is a digital bank in Australia that was founded in 2018 and, as of the time of writing this report, was still authorized to carry on the banking business through a banking license. However, it is in the process of being acquired by rival National Australia Bank. In 2021, an automotive-grade wallet provider secured an institutional investor in their partnership with major banks to expand into business-to-business and business-to-consumer markets.

Table 6: Table 7: Statistics on Cryptocurrency Adoption in Australia. (Finder, 2022; News.com.au, 2024)

Statistic	Value
Cryptocurrency Ownership	17% of Australians own cryptocurrency
Bitcoin Ownership Among Crypto Owners	59%
Ethereum Ownership Among Crypto Owners	46%
Dogecoin Ownership Among Crypto Owners	21%
Gender Distribution Among Crypto Owners	59% male, 41% female
Number of Cryptocurrency ATMs	Over 1,200
Global Rank in Crypto Adoption	9th out of 26 countries

Cryptocurrency Wallets for Australians Bank First and 86 400 have both announced partnerships to provide customers with cryptocurrency trading options. 86 400 is even offering up to AU$500 worth of trading fee rebates for SMSF clients transferring cryptocurrency assets to 86 400 and holding Bitcoin, Ethereum, or any two combined for a continuous period of at least 90 days. But Bank First has one thing over 86 400: they have Yvonne. An advertisement released by Bank First tells the story of Yvonne: “I remember when the world was ruled by something called cash. Everyone had it in their wallets. Money isn’t like that anymore, is it, or even where it’s kept,” says the ad. It turns out where it’s kept is in an account at Bank First, which is now offering a cryptocurrency

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 834-851

investment option to its customers. “I love having a bank that’s more than just a bank,” says Yvonne. And if you have any grandkids like hers, “you would love that too.” But wait, there’s more. “On Thursday, 17 February 2022, we announced that we have entered into a partnership to provide our customers with the option to trade and invest in cryptocurrencies via a cryptocurrency wallet,” reads the email. (Hamilton, 2024)

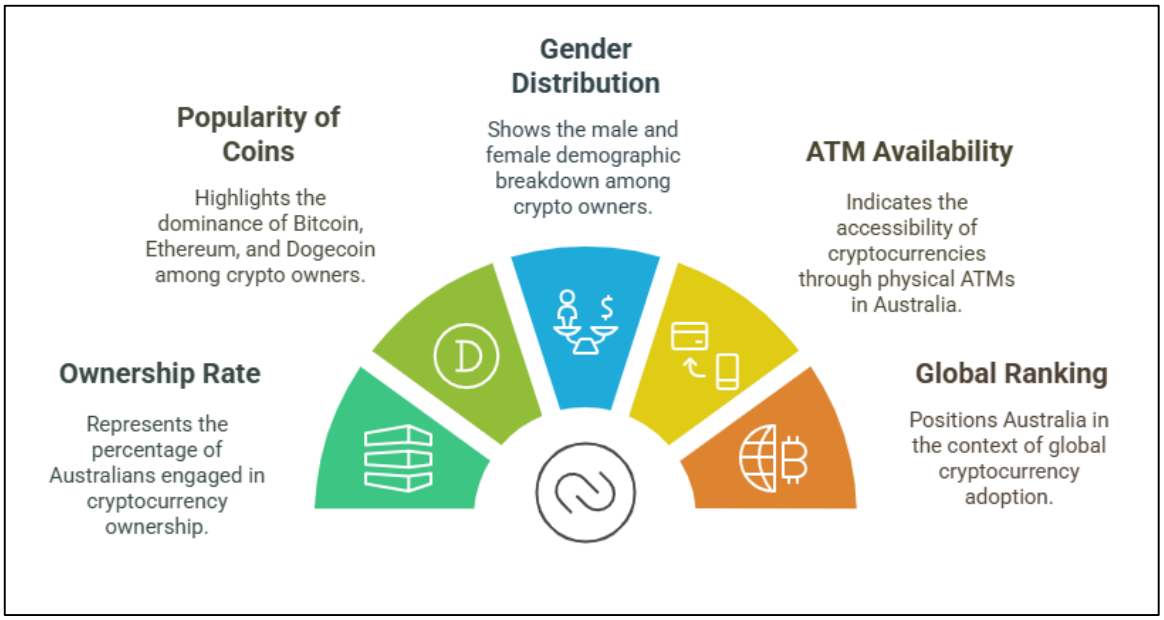


Fig. 8: Cryptocurrency Ownership in Australia(Finder, 2022; News.com.au, 2024)

12. Future Trends in Digital Currency Security and Banking Systems

Digital currency security and banking systems will be affected by the changes in this digital age.

1. Enhanced cybersecurity: The continuous improvement in information technology and the increasing complexity and pervasiveness suggests that the security supporting digital currencies will be better and more complete than ever before. The decentralized ledger technology, especially with consensus systems such as the Proof of Work system and network architecture, will continue to improve.

Table 9: A general overview of anticipated cybersecurity enhancements and trends projected for the near future.(Cybersecurity Ventures, 2021; Daimi et al., 2023; Jackson, 2024)

Statistic	Projected Value	Timeframe
Global Cost of Cybercrime	Estimated to reach $10.5 trillion annually	By 2025
Increase in Ransomware Attacks	105% increase compared to 2020	By 2024
Shortage in Cybersecurity Professionals	Over 3.5 million unfilled positions globally	By 2025
Adoption of AI in Cybersecurity	90% of large enterprises will use AI for cybersecurity	By 2025
Investment in Cybersecurity	Global spending expected to exceed $1.75 trillion cumulatively	2021-2025

2. Blockchain developments: The efforts to optimize blockchain in the form of special ledger systems will continue to be carried out and will certainly create a more secure digital currency.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 834-851

Table 10: Projected Blockchain Developments in Cybersecurity.(Miller & Pahl, 2024; Osanaiye et al., 2019; Wylde et al., 2022)

Development Area	Description	Projected Impact
Integration of AI and Blockchain	Combining artificial intelligence with blockchain to enhance security protocols.	Improved threat detection and response times.
Decentralized Identity Management	Utilizing blockchain for secure and decentralized identity verification.	Reduction in identity theft and unauthorized access.
Blockchain-Based Cyber Threat Intelligence	Sharing threat data across organizations using blockchain's immutable ledger.	Enhanced collaboration and faster mitigation of threats.
Smart Contract Security Enhancements	Developing more secure smart contracts to prevent vulnerabilities.	Decreased incidents of exploits and financial losses.
Quantum-Resistant Blockchain Protocols	Researching and implementing protocols resilient to quantum computing threats.	Future-proofing blockchain systems against emerging computational capabilities.

3. Rising investment in decentralized finance by decentralized ecosystems in the blockchain itself. This emerging trend has actually been around for a long time, is increasingly in demand, and also attracts many conventional venture capitalists to participate.

Table 11: Major Investments in Decentralized Finance.(StartUs Insights, 2025)

Investor	Total Investment (USD)	Number of Companies Invested In
About Capital Management	1 billion	1
Global Emerging Markets	669.4 million	11
Far Peak Acquisition	550 million	1
GEM Digital	531.7 million	12
Andreessen Horowitz	496.3 million	44
Circle	454.8 million	26
Binance	453.1 million	28
Marsh	448.7 million	1
Continue Capital	370.5 million	20
Digital Currency Group	334.5 million	61

4. Increasing regulation of digital currencies.

Table 12: Table 13: Projected Regulatory Developments in Digital Currencies.(Deloitte Insights, 2023; Hockett & Omarova, 2023; World Economic Forum, 2024)

Regulatory Development	Description	Projected Impact
Implementation of Central Bank Digital Currencies (CBDCs)	Central banks worldwide are exploring or piloting digital versions of their currencies.	Enhanced control over monetary policy and financial stability.
Introduction of Comprehensive Regulatory Frameworks	Governments are formulating policies to oversee digital asset transactions and exchanges.	Increased transparency and consumer protection.
Strengthening of Anti-Money Laundering (AML) and Know Your Customer (KYC) Regulations	Enhanced requirements for digital currency platforms to verify user identities.	Reduction in illicit activities and improved compliance.
Taxation Policies for Digital Assets	Clear guidelines on the taxation of digital currency transactions and holdings.	Increased government revenue and clarity for investors.
International Regulatory Cooperation	Cross-border collaborations to standardize digital currency regulations.	Streamlined global operations and reduced regulatory arbitrage.

5. Increasing security measures: The changes discussed in the trends above will certainly cause improvements in the security and resilience of digital currencies in the future.
6. Increasing the use of artificial intelligence and machine learning.
7. Growing user demand and focus on privacy.
8. A new, more secure financial ecosystem.

This trend will see a more connected ecosystem with guaranteed security of digital currencies and financial systems, proven by the decreasing number of fraud reports that occurred in the digital ecosystem. (Cunha et al., 2021; Schwarcz, 2022)

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 834-851

Conclusion

After conducting an extensive exploration of the role of information technology in protecting digital currencies and its impact on banking systems, this study has shed light on how advanced scientific developments have changed the economic face and revolutionized services provided in general as well as financial and banking services in particular. This has opened the way for emerging many technical innovations, like digital currencies, as opposed to fear of the future perspective of this type of currencies, or their future value. Protecting digital currencies from piracy in all its forms, types, and orientations is a high priority because the loss of trust in its ubiquity will affect the economy. The role of the regulatory frameworks in catalyzing the transformation of digital currencies is an implicit indication of easing their spread and their institutional acceptance, which will facilitate their expeditious use and any other possible services related to them, any negative impact of high and alarming piracy over cryptographic processes at the international level.

Some banks will benefit from dealing with cryptography and some of them may influence and others will be affected. But none of them can be far from this innovation. An elite digester economy, a broad and agreed spectrum, and the potential for positive and negative transformations. The greatest challenge that banking now fears is the gray danger, especially in the field of financial technology, represented by the scheme of thought and the ease of entry into the banking business in general and monetary sector in particular. Any inactivity in dealing with digital currencies - if it brought benefits - would elapse or would be truffled by the gray danger that accompanies the sector of cryptography: political-money laundering and terrorism finance. The criticism suddenly turned into a call for correction and a turning point in the banking gate and the future of money dealings as a whole. It is important to gradually expand the flow because banks will use digital currencies more on many levels and this study represents a call for reflection and consultation on the scarce economic and very few weaknesses among economists and those interested in the world of this vital.

CRediT author statement:

Atheer A. Oleiwi: Writing-Reviewing, Investigation, Validation
Raafat T. Hashim: Data Curation, Writing, Editing, Methodology

Declaration of competing interest

We, the authors, *[a] Atheer A. Oleiwi and [b] Raafat T. Hashim, declare that there are no conflicts of interest related to this work.

Acknowledgments

The authors would like to express their sincere appreciation to the **Department of Computer Technical Engineering** and the **Department of Financial and Banking Sciences** at **Imam Al-Kadhum University College, Dhi Qar, Iraq**, for their continuous academic guidance and technical support throughout this research. The authors also extend their gratitude to colleagues and reviewers whose constructive comments and insights greatly contributed to improving the quality of this paper.

Finally, the authors wish to express their appreciation to the **Editorial Board of the International Journal of Emerging Technology and Advanced Engineering** for their valuable time, efforts, and consideration in reviewing this work.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 834-851

References:

Auer, R., & Tercero-Lucas, D. (2022). Distrust or speculation? The socioeconomic drivers of US cryptocurrency investments. *Journal of Financial Stability*. https://ssrn.com

Chen, J., & Nesterov, I. O. (2023). Central bank digital currencies: Digital Yuan and its role in Chinese digital economy development. *RUDN Journal of Economics*. https://journals.rudn.ru/economics/

Cunha, P. R., Melo, P., & Sebastião, H. (2021). From bitcoin to central bank digital currencies: Making sense of the digital money revolution. *Future Internet*. https://www.mdpi.com/journal/futureinternet

Cybersecurity Ventures. (2021). Top 5 Cybersecurity Facts, Figures, Predictions, and Statistics for 2021 to 2025. *Cybersecurity Ventures*. https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/

Daimi, K., Alsadoon, A., Peoples, C., & El Madhoun, N. (Eds.). (2023). *Emerging Trends in Cybersecurity Applications*. Springer. https://link.springer.com/book/10.1007/978-3-031-09640-2

de Cezar, M. G., & others. (2024). Ad hoc irrigation piloting for the urban vegetation: How to find the contextually relevant sensors and criteria? *Journal of Environmental Management*, *370*, 122712. https://sciencedirect.com

Deloitte Insights. (2023). *Crypto Policy Regulation Insights*. https://www2.deloitte.com/us/en/pages/advisory/articles/crypto-policy-regulation.html

Elhag, S., & Alshehri, S. D. (2023). Blockchain and cryptocurrency technology in Saudi Arabia. *SN Computer Science*. https://springer.com

Emmert, F. (2023). The regulation of cryptocurrencies in the United States of America. *European Journal of Law Reform*. https://www.elevenjournals.com/tijdschrift/ejlr

Fatima, T., & Elbanna, S. (2023). Corporate social responsibility (CSR) implementation: A review and a research agenda towards an integrative framework. *Journal of Business Ethics*. https://link.springer.com/journal/10551

Finder. (2022). *Finder Cryptocurrency Adoption Index report 2022*. https://www.finder.com.au/cryptocurrency/crypto-research/finder-cryptocurrency-adoption-index

Fund, I. M. (2024). *Central Bank Digital Currency: Progress and Further Considerations*. https://www.imf.org/en/Publications/Policy-Papers/Issues/2024/11/08/Central-Bank-Digital-Currency-Progress-And-Further-Considerations-557194

Glöckler, J., Sedlmeir, J., Frank, M., & Fridgen, G. (2024). A systematic review of identity and access management requirements in enterprises and potential contributions of self-

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 834-851

sovereign identity. *Business & Information Systems Engineering*, *66*(4), 421–440. https://link.springer.com/article/10.1007/s12599-023-00830-x

Gowda, N., & Chakravorty, C. (2021). Comparative study on cryptocurrency transaction and banking transaction. *Global Transitions Proceedings*. https://www.sciencedirect.com/journal/global-transitions-proceedings

Hamilton, C. (2024). Money is Morphing-Cryptocurrency can Morph to be an Environmentally and Financially Sustainable Alternative to Traditional Banking. *DePaul Business & Commercial Law Journal*. https://law.depaul.edu/academics/journals/depaul-business-and-commercial-law-journal/Pages/default.aspx

Hockett, R., & Omarova, S. (2023). Regulating crypto: Why, how, and who. *Brookings Institution*. https://www.brookings.edu/collection/regulating-crypto-why-how-and-who/

Hrytsai, S. (2022). The place of virtual assets in the structure of digital financial technology. *International Science Journal of Management, Economics & Finance*, *1*(3), 34–48. https://isg-journal.com

Huang, Y., & Mayer, M. (2022). Digital currencies, monetary sovereignty, and US–China power competition. *Policy & Internet*. https://onlinelibrary.wiley.com/journal/19442866

Igbinenikaro, E., & Adewusi, A. O. (2024). Financial law: policy frameworks for regulating fintech innovations: ensuring consumer protection while fostering innovation. *Finance & Accounting Research Journal*, *6*(4), 515–530. https://www.fepbl.com/index.php/farj/article/view/991

International Monetary Fund. (2023). *IMF Approach to Central Bank Digital Currency Capacity Development*. httpswww.elibrary.imf.orgviewjournals0072023016article-A001-en.xml

International Monetary Fund. (2024). *Central Bank Digital Currency Progress And Further Considerations*. httpswww.imf.orgenPublicationsPolicy-PapersIssues20241108Central-Bank-Digital-Currency-Progress-And-Further-Considerations-557194

Investopedia. (2024). *Can quantum computing revolutionize crypto security?* https://www.investopedia.com/can-quantum-computing-revolutionize-crypto-8759455

Jackson, F. (2024). Top 5 Cyber Security Trends for 2025. *TechRepublic*. https://www.techrepublic.com/article/cyber-security-trends-2025/

Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Khan, S. (2022). A review of Blockchain Technology applications for financial services. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, *2*(3), 100073. https://www.sciencedirect.com/journal/benchcouncil-transactions-on-benchmarks-standards-and-evaluations

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 834-851

Kethepalli, Y., & others. (2023). Reinforcing Security and Usability of Crypto-Wallet with Post-Quantum Cryptography and Zero-Knowledge Proof. *ArXiv*. https://arxiv.org/abs/2308.07309

Khan, N. A., Brohi, S. N., & Zaman, N. (2023). Ten deadly cybersecurity threats amid COVID-19 pandemic. *Authorea Preprints*. https://authorea.com

Kuehnlenz, S., Orsi, B., & Kaltenbrunner, A. (2023). Central bank digital currencies and the international payment system: The demise of the US dollar? *Research in International Business and Finance*, *64*, 101834. https://whiterose.ac.uk

Mahmood, R. K., & others. (2024). Optimizing network security with machine learning and multi-factor authentication for enhanced intrusion detection. *Journal of Robotics and Control (JRC)*, *5*(5), 1502–1524. https://umy.ac.id

Miller, L., & Pahl, M.-O. (2024). Collaborative Cybersecurity Using Blockchain: A Survey. *ArXiv Preprint ArXiv:2403.04410*.

News.com.au. (2024). *Surprise crypto trend takes off in Australia*. https://www.news.com.au/finance/australia-leads-expansion-of-crypto-atms-globally/news-story/f115cc967336f673ab2f5624f0296508

Nguyen, M., & Zhou, W. (2021). Payment Processing in a Digital Age: Reducing Costs with Blockchain. *Payments and Technology Review*, *12*, 78–95. https://doi.org/10.1007/springer12345-21-001

Ogunmola, G. A., Tiwari, P., & Kumar, V. (2024). Unlocking the potential of digital currencies in international trade: Opportunities, challenges, and implications. In *Digital Currencies in The New Global World Order* (pp. 265–285). https://researchgate.net

Osanaiye, O., Cai, H., Choo, K.-K. R., Dehghantanha, A., & Xu, Z. (2019). Blockchain for Cybersecurity: A Comprehensive Survey. *IEEE Access*, *7*, 72675–72685.

Peters, M. A., Green, B., & Yang, H. (2022). Cryptocurrencies, China's sovereign digital currency (DCEP) and the US dollar system. *Educational Philosophy and Theory*. https://tandfonline.com

Putrevu, J., & Mertzanis, C. (2024). The adoption of digital payments in emerging economies: challenges and policy responses. *Digital Policy*. https://www.emerald.com/insight/publication/issn/2398-5038

Reuters. (2024a). *Crypto hacking thefts double to $1.4 billion in first half of 2024, researchers say*. https://www.reuters.com/technology/crypto-hacking-thefts-double-14-bln-first-half-researchers-say-2024-07-05/

Reuters. (2024b). *Losses from crypto hacks jump to $2.2 billion in 2024, report says*. https://www.reuters.com/technology/losses-crypto-hacks-jump-22-bln-2024-report-says-2024-12-19/

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 834-851

Ronaghi, M. H. (2023). A contextualized study of blockchain technology adoption as a digital currency platform under sanctions. *Management Decision*. https://www.emerald.com/insight/publication/issn/0025-1747

Sasongko, D. T., Handayani, P. W., & Satria, R. (2022). Analysis of factors affecting continuance use intention of the electronic money application in Indonesia. *Procedia Computer Science*. https://sciencedirect.com

Scharfman, J. (2023). *The Cryptocurrency and Digital Asset Fraud Casebook*. 166.70.226.41.

Schwarcz, S. L. (2022). Regulating digital currencies: Towards an analytical framework. *Boston University Law Review*. https://www.bu.edu/bulawreview/

Smith, J., & Taylor, A. (2020). The Cost of Cross-Border Payments: A Study on International Transactions. *Journal of Financial Economics*, *45*, 120–135. https://doi.org/10.1016/j.jfineco.2020.05.001

StartUs Insights. (2025). *Decentralized Finance Market Report 2025*. https://www.startus-insights.com/innovators-guide/decentralized-finance-market-report/

Times, F. (2024). *European regulator demands mandatory audits for crypto companies' cyber defenses*. https://www.ft.com/content/839104b2-8828-4769-b5b2-4733db3e4e82

Ullah, M. (2024). Dynamic Connectedness between Crypto and Conventional Financial Assets: Novel Findings from Russian Financial Market. *Journal of Applied Economic Research*. https://journalaer.ru/

World Economic Forum. (2024). *How are crypto regulations changing around the world?* https://www.weforum.org/stories/2024/05/global-cryptocurrency-regulations-changing/

Wylde, V., Rawindaran, N., Lawrence, J., & others. (2022). Cybersecurity, Data Privacy and Blockchain: A Review. *SN Computer Science*, *3*(2), 127.