

Cyber security as a Mechanism for Achieving the Economic Sustainability of Digital Currencies- Analytical Study from 2015 to 2024-

Guecherou Fatiha*¹

¹Laboratory of the management of local authorities and their role in achieving development, Economics, Business and Management Faculty, University of Blida 2-Algeria, f.guecherou@univ-blida2.dz

Received: 13/11/2025

Accepted: 27/12/2025

Abstract:

This study highlights the pivotal role of cybersecurity in achieving economic sustainability for digital currencies by analysing cyber threats and their financial impacts. Findings reveal escalating threats, with projected 2025 losses exceeding \$5 billion and 45% geographic concentration in Asia. Technical protection mechanisms currently outperform regulatory frameworks. The study recommends strengthening security infrastructure, developing unified regulations, enhancing international cooperation, and building human capacities. It concludes that an integrated approach combining technology, regulation, and collaboration is essential for ensuring digital currency sustainability amid evolving cyber challenges.

Keywords: Cybersecurity; Economic Sustainability; Digital Currencies; Cryptocurrencies; Cyber Threats; Financial Losses

Jel Classification Codes :G28; O44;E42;G23;G32;G01

* Guecherou Fatiha

1.Introduction:

1.1.Problem Statement :

In the digital age we are living in, technological transformation is no longer just a secondary option, but has become an imperative necessity that imposes itself on all aspects of life, especially the economic and financial sector. The digital revolution marked a historical turning point that led to the re-engineering of traditional financial structures, as advanced financial technologies emerged that caused a break with traditional monetary systems. At the heart of this radical transformation, digital currencies have emerged. As a natural consequence of the convergence of crypto science with the global economy's needs for decentralization and financial inclusion – one of the most significant financial innovations since the advent of electronic money.

These currencies, by relying on groundbreaking technologies such as blockchain, have succeeded not only in introducing a new model for financial transactions, but in creating an economic philosophy based on decentralized trust and transparency. This success has been manifested in the widespread spread of cryptocurrencies such as Bitcoin and Ethereum, as well as the accelerated trend of many countries to issue official digital currencies (CBDCs) It is based on the sovereignty of central banks. All of these developments indicate that the world is on the cusp of a new phase of financial development, which may redefine the concept of money itself.

However, this rapid rise of cryptocurrencies has not been without challenges and obstacles. Despite the promising advantages they offer in terms of speed, cost reduction, and financial inclusion, they are also exposed to existential risks that threaten their stability and future. The data indicates a steady increase in the size of the cyber threat unit targeting the infrastructure of these currencies, from penetration of global exchange platforms, to cyber extortion attacks, to exploiting vulnerabilities in smart contracts. These threats reveal the stark contrast between the supposedly secure nature of these technologies and the reality of the security fragility they suffer from.

From this standpoint, the main problem of the article emerges in the following fundamental question: **How can cybersecurity transform from being a mere complementary defence tool to a pivotal strategic mechanism to ensure the economic sustainability of digital currencies?**

1.2.Research Objectives:

This study aims to:

- Analyse the nature of the relationship between cybersecurity and the economic sustainability of digital currencies
- Monitoring and classifying various cyber threats targeting digital currencies
- Assess the effectiveness of current coping mechanisms and identify their shortcomings
- Providing an Integrated Framework to Enhance Cybersecurity as a Mechanism for Economic Sustainability
- Develop practical recommendations to strengthen cybersecurity in the context of digital currencies.

1.3. Research Importance:

This study gains its importance from the critical challenges facing the emerging digital financial system, as cyber threats pose an existential threat to digital currencies that undermine the pillars of their economic sustainability. The importance is highlighted in:

- The Critical Nature of Cyber Threats Targeting Modern Financial Infrastructures
- The urgent need to build integrated defense systems that protect investments in cryptocurrencies
- The significant economic impact of losses caused by cyber attacks
- The Strategic Imperative to Keep Up with the Global Trend Towards Official Cryptocurrencies (CBDCs)

1.4. Research Methodology:

The study relied on the descriptive analytical approach through the analysis of secondary data in specialized international reports, quantitative analysis of statistics related to financial losses and the geographical distribution of attacks, qualitative analysis of historical cases of security breaches, and comparative analysis of the effectiveness of various protection mechanisms, with the use of forward-looking extrapolation to analyse future trends of threats and coping mechanisms.

2. Conceptual Framework for Cryptocurrencies and Cybersecurity

This section represents a fundamental building block in the theoretical structure of the study, as it establishes the conceptual foundations for understanding the nature of digital currencies and their security requirements. The first section begins by defining and classifying digital currencies, tracing their historical development path that embodies their transformative role in the contemporary financial landscape. Meanwhile, the second section focuses on the concept of cybersecurity, highlighting its pivotal role in protecting digital infrastructure, financial assets, and the pillars of trust upon which these modern financial systems are built. Together, these two components form the necessary theoretical framework for analysing the intersection of the financial and technical fields in the current digital age.

2.1. Conceptual Framework for Digital Currencies:

Digital currencies represent a fundamental shift in the concept of money, moving it from a physical to an intangible, electronic form. Enabled by advanced technologies like cryptography and blockchain, they facilitate direct, borderless transactions between parties. This framework explores the definition, evolution, and diverse types of these modern financial instruments.

2.1.1. Definition of Digital Currencies :

Digital currencies are a new development in the field of payments, and they rely heavily on technology, especially crypto and blockchain, these currencies represent an intangible form of currency in electronic form, where payments between parties can be transferred using current technologies such as computers, the internet, and smartphones, and digital currencies can be used for payments between individuals or with commercial entities, whether locally or internationally, and they may also be limited to use within games or social networks, and it may be a legal currency (fiat)e.g. e-money or fiat-non (fiat-non) such as virtual currencies(Othmania& Bin Qirat, 2022, p.86).

The digital currency acts as a medium of exchange value and uses the crypto process to secure and control transactions, relies on blockchain technology to create currency units, provides benefits such as instant transactions between dealing parties without the need for intermediaries, and facilitates the payment of payments across borders and across devices and global information networks (Saleh, 2021, pp.7-8).

The International Monetary Fund defines it as a monetary value in the form of credit units stored in electronic form or in electronic memory for the benefit of the consumer, and therefore it can be said that digital currency is a new type of currency, or in other words, it is an electronic alternative to paper and metal money of a physical nature (Srouf,2022, p.40).

2.1.2. The Origin and Development of Digital Currencies:

The means of financial exchange have evolved since the first appearance of money, and with the advancement of technology, modern financial technologies such as blockchain have emerged, blockchain is considered a new financial system that differs from the traditional system by recording and securing transactions in a distributed and secure manner. These technologies are the key point of the rise of cryptocurrencies (El-Moussawi & El-Shammari,2014, pp.264-285).

Bitcoin is considered the first milestone in the emergence of cryptocurrencies, and it was launched based on a white paper published by an anonymous programmer named Satoshi Nakamoto. Bitcoin is based on blockchain technology, which is a distributed transaction logging technology that relies on a network of members to exchange transactions directly between them without the need for a central intermediary.

The process of issuing Bitcoin began in 2009 within a narrow range, and it was estimated at the time that "Nakamoto", the launcher of this coin, had created in that year only about one million pieces of "Bitcoin" currency, and in 2010, the first Bitcoin transactions began through the users of the "Bitcointalk" forum by buying pizza for ten thousand units of "Bitcoin", after which the prices of this coin gradually rose until in 2011 the value of one Bitcoin reached \$0.30 (Seetharaman et al, 2017, p.236).

Since 2011, new cryptocurrencies have started to emerge, such as "altcoins" as a branch of Bitcoin, these currencies aimed to improve some services such as speed and privacy, and increase competitiveness, an infrastructure was created that allows users to trade and store Bitcoin, and with the launch of the first Bitcoin exchange, the value of each unit of which was approximately \$30.

In 2012, the first beginnings of the adoption of "Bitcoin as a means of payment by official merchants on websites" was the first website to accept payment in this currency, and many other companies, including "Microsoft", joined this company, and this was considered the first step towards accepting "Bitcoin" and "cryptocurrency" internationally and widely as a legitimate payment method (El-Khidher,2021, p.78).

The year 2013 witnessed the first initial offering of the coin as a means of crowdfunding, and the infrastructure of "Bitcoin" continues to improve, especially with the opening of the first "Bitcoin ATM" in 2014, and by 2017 there were nearly 1000 ATMs worldwide, and in 2015, the "Coinbase" platform based in the United States of America became the first organized cryptocurrency exchange to increase the value of the coin to 20,000 USD in 2017(Galati & Wooldridge ,2009,p.12) , and the total value of all

cryptocurrencies in circulation has exceeded the value of USD 100 billion. It peaked at US\$800 billion in 2018(El-Khidher,2021, pp.78-78).

The cryptocurrency market has witnessed a remarkable quantitative and qualitative development during the period from 2019 to 2025, as the total market capitalization jumped from about \$190 billion at the beginning of 2019 to exceed the barrier of \$4.5 trillion in the first quarter of 2025, and the number of cryptocurrency ATMs jumped from about 5000 to more than 48,000 machines, while the price of Bitcoin jumped from about \$4,000 in 2019 to record a new historical peak exceeding \$95,000 in 2025. This reflects the shift from retail speculation to broad institutional adoption and organizational maturity (CoinMarketCap,2025, p.15).

2.1.3. Types of digital currencies:

Digital currencies can be divided into four main forms: Electronic money, Virtual currencies, Cryptocurrencies and LegalDigital Currencies(CBDCs) issued by central banks or as illustrated by the following:

- **Electronic-money:** is a digital representation of traditional currencies such as the dollar or the euro, and it is used for online transactions without the need for physical exchange, it relies on centralized financial platforms such as banks or electronic payment services, and it has a high level of security thanks to encryption technologies. The most prominent examples of these are **PayPal, Apple Pay, and Google Pay (European Central Bank,2023)**.

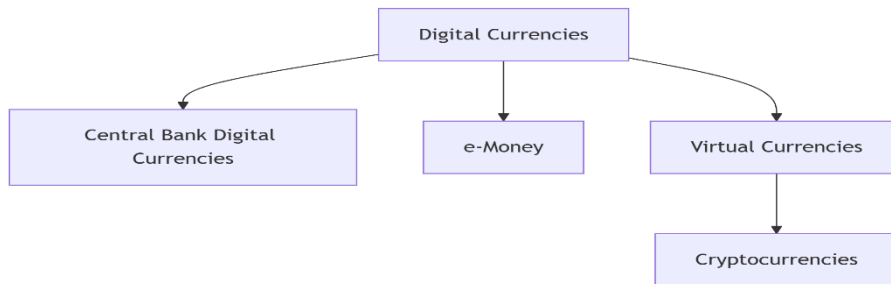
- **Virtual currencies:** These are digital currencies that are used in closed platforms such as electronic games or social networks, and do not represent real money that can be traded outside of the particular system. They are usually centralized and managed by the owner of the platform, and do not rely on technologies such as blockchain or cryptography. They are used to purchase items or services within the system. Examples include **V-Bucks in Fortnite and Robux in Roblox (European Central Bank,2015, p.7)**.

- **Cryptocurrencies:** A type of digital currency that relies on **cryptography and blockchain** to ensure security and transparency. It is characterized by being **decentralized**, as it is not subject to any central entity such as banks or governments. It is used in online financial transactions and can be an investment tool. The most prominent examples of cryptocurrencies are **Bitcoin,Ethereum, and Ripple (XRP) (International Monetary Fund,2023, p.8)**.

- **Central Bank Digital Currencies (CBDCs):** These are digital currencies issued by central banks that represent national currencies such as the dollar or the euro. They aim to facilitate financial operations while maintaining government oversight, and use technologies similar to blockchain but under central supervision. They aim to promote financial inclusion and facilitate online payments, such as the Chinese Digital Yuan, and the Digital Dollar - United States (under development) (**Bank for International Settlements,2021, p.75**).

The following figure shows the types of cryptocurrencies:

Figure 01: Forms of Digital currencies



Source: Natarajan.H, Krause.S, And. Gradstein.H(2017), Distributed Ledger Technology and Blockchain, World Bank Group, <https://openknowledge.worldbank.org>

2.2. Cybersecurity Conceptual Framework :

This element presents the conceptual framework of cybersecurity as a cornerstone for protecting digital financial systems. It begins with a comprehensive definition of cybersecurity in the context of digital currencies, then outlines its main dimensions: technical, organizational, and human. The element also differentiates cybersecurity from other security concepts, tracing its historical evolution and strategic importance in ensuring the stability of digital financial systems and building trust in them.

2.2.1. Definition of Cybersecurity:

Cybersecurity refers to the set of practices, technologies, and processes designed to protect systems, networks, software, and data from digital attacks in the context of cryptocurrency, this concept evolves to include protecting digital financial infrastructure from unauthorized access, cyberattacks, and theft of digital assets. Cybersecurity is a key pillar of building trust in the emerging digital financial system, as it is a critical factor in ensuring the continuity of digital financial services and the integrity of transactions (**Whitman & Mattord,2021, p.45**).

2.2.2. Basic Dimensions of Cybersecurity:

The comprehensive cybersecurity framework consists of three interrelated dimensions (**Stallings,2023, p.23**):

- **Technical Dimension:** It includes advanced tools and technologies such as intrusion detection systems, firewalls, intrusion prevention systems, and advanced cryptography. This dimension is crucial in protecting the technical infrastructure of cryptocurrencies.
- **Organizational Dimension:** It is represented in the policies, procedures, legal framework, and security governance. It includes the development of cybersecurity strategies and the implementation of security standards such as ISO 27001.
- **Human Dimension:** It focuses on the human element as the weakest link in the security chain. It includes security awareness programs, ongoing training, and building a security culture among all users.

2.2.3. Differentiate between cybersecurity and related concepts:

Cybersecurity is a broader comprehensive concept than traditional security concepts. While information security focuses on protecting data in any form, cybersecurity specializes in protecting digital space and electronic systems. Cryptocurrency cybersecurity is a subdiscipline that focuses on protecting digital assets and modern financial infrastructure, considering the unique nature of cryptocurrencies in terms of decentralization and cryptography (Zhang, 2023, pp.45-67).

2.2.4. Historical development of the concept of cybersecurity:

The concept of cybersecurity has evolved over the past decades, starting as a mere protection of data and information, then evolving to include the protection of networks and systems, to the protection of critical infrastructures and complex financial systems. This development coincided with the digital revolution and the emergence of digital currencies that imposed new and specialized security requirements. This development has led to the emergence of precise specializations in cybersecurity that are compatible with the unique nature of digital currencies and blockchain technologies (Johnson, 2024, pp. 89-112).

2.2.5. Strategic Importance of Cybersecurity:

Cybersecurity in the digital age is an indispensable strategic element for countries and institutions alike. In the context of cryptocurrencies, cybersecurity becomes a prerequisite for achieving economic sustainability and trust in the modern financial system. It is important in protecting investments, ensuring the stability of digital financial markets, and preventing hacks that could lead to heavy losses. It also plays a pivotal role in promoting secure financial inclusion and building a strong and resilient digital economy (ENISA, 2024, p.15).

3. The economic sustainability of Digital currencies:

This element presents the conceptual framework for the economic sustainability of digital currencies, defining the concept and its key dimensions. It examines the fundamental components of economic sustainability, including trust and reliability, liquidity and market depth, widespread acceptance, and clear regulatory frameworks. The element also introduces a set of quantitative and qualitative indicators to measure the performance and long-term sustainability of digital currencies, forming a basis for evaluating their economic viability and role in the contemporary financial landscape.

3.1. The Concept of Economic Sustainability in the Context of Digital Currencies:

The economic sustainability of cryptocurrencies refers to the ability of these digital assets to maintain their market value and function as a medium of exchange, a store of value, and a unit of account over the long term. This concept is not limited to mere survival and technical continuity, but includes the ability to achieve relative stability in value, stimulate economic growth by reducing transaction costs, and contribute to financial inclusion, while maintaining a balance between economic, social, and environmental requirements.

The economic sustainability of cryptocurrencies refers to the ability of these digital assets to maintain their market value and function as a medium of exchange, a store of value, and a unit of account over the long term. This concept is not limited to mere survival and technical continuity, but includes the ability to achieve relative stability in value, stimulate economic growth by reducing transaction costs, and contribute to financial inclusion, while maintaining a balance between economic, social, and environmental requirements.

3.2. Components of the economic sustainability of digital currencies:

The economic sustainability of cryptocurrencies is based on several interrelated fundamental components (**Bank for International Settlements,2024, p.56**):

A. Trust and reliability: Trust is the backbone of any monetary system, as it forms the basis on which the value of a currency is based. In the context of digital currencies, trust is achieved through transparency in operations, advanced technical security, compliance with regulations, and stability in performance. It also includes the reliability of the network and its ability to resist failures and cyberattacks.

B. Liquidity and Market Deepening: It refers to the market's ability to accommodate large operations without significant impact on prices. Deepening the cryptocurrency markets requires a broad base of buyers and sellers, a variety of derivative financial instruments, and the presence of effective market makers. High liquidity contributes to price stability and reduces trading costs.

c. Widespread Acceptance and Popularity: The adoption of digital currencies as a widely accepted means of payment by merchants, consumers, and financial institutions is a critical factor in their economic sustainability. This includes the availability of the necessary payment infrastructure, ease of use, and integration with existing financial systems.

D. Clear regulatory framework: A clear regulatory framework provides a stable environment that encourages innovation while protecting consumers and stabilizing the market. This includes establishing clear anti-money laundering standards, protecting user data, ensuring transparency in disclosure, and establishing effective oversight mechanisms.

3.3. Indicators for measuring economic sustainability:

The economic sustainability of cryptocurrencies can be measured through a full set of quantitative and qualitative indicators (**World Bank,2023, p.28**):

A. Quantitative Indicators:

- ✓ **Daily Trading Volume and Market Capitalization:** Trading volume indicates the level of activity and liquidity in the market, while market capitalization represents the total value of the currency.
- ✓ **Number and value of daily transactions:** Indicates the level of actual activity of the currency as an intermediary.
- ✓ **Degree of Price Volatility and Stability Indicators:** Measured by the standard deviation of returns and historical(time-based) and implied volatility indicators.
- ✓ **Number of active users and growth rate:** Refers to the user base, the spread of the currency, and its ability to attract new users.

B. Qualitative Indicators:

- ✓ **Level of trade and consumer acceptance:** Measured by the number of traders accepted for the currency and the diversity of the sectors it adopts.
- ✓ **Maturity of the regulatory infrastructure:** It is assessed by the presence of comprehensive legal frameworks and specialized regulatory bodies.
- ✓ **Cybersecurity and user protection:** Measured by the number and volume of security breaches and the effectiveness of protection mechanisms.
- ✓ **Degree of Innovation and Continuous Technical Development:** Evaluated by the pace of technical updates and adoption of new technologies.

4. Cyber threats and their economic impact on digital currencies:

This section provides a comprehensive analysis of cyber threats targeting digital currencies and their economic impacts. It examines the main types of cyber-attacks and documents major historical incidents in the sector, along with an analysis of the geographical distribution of these attacks during the period (2023-2024). It also presents a quantitative assessment of the cumulative losses resulting from these attacks over a decade (2015-2025), with a detailed analysis of the prevailing patterns of cybercrimes in 2024. This offers a clear picture of the scale and evolution of security challenges in the world of digital currencies.

4.1.Types of Cyber Threats:

Cyber threats include (ENISA,2024, p.08):

- **Technical threats:** Attacks directed against the technical infrastructure of cryptocurrencies include, such as hacking of digital wallets and exchange platforms, exploiting vulnerabilities in blockchain protocols, and distributed denial-of-service attacks that disrupt service availability.
- **Operational threats:** These include phishing attacks to steal login data, internal fraud by trading platform employees, and human errors in daily operations that lead to the loss of digital assets.
- **Systemic threats:** includes attacks on blockchain networks, exploiting smart contract vulnerabilities, and liquidity attacks on DeFi platforms that threaten the stability of the digital financial system.

4.2.Major historical incidents about cryptocurrency cybersecurity threats:

Here are the most important historical incidents about cryptocurrency cybersecurity threats from 2014 to 2022:

4.2.1. Platform Hack (2014) MT. GOX

The 2014 MT. GOX hack came as a shock to the emerging sector, as 850,000 bitcoins worth \$450 million were stolen at the time of the incident by exploiting a technical "flexibility transaction" vulnerability, exposing the fragility of centralized storage systems, bankrupting the platform, losing investor confidence, and accelerating the pace of government regulation of cryptocurrencies around the world (U.S. Department of Justice,2024).

4.2.2. The DAO Breakthrough (2016):

A hacker managed to steal \$60 million worth of 3.6 million Ethers in 2016 by exploiting a "re-entry" vulnerability in The DAO's decentralized smart contract, leading to a historic split in the Ethereum network and creating the Ethereum Classic Chain (ETC), highlighting the dangers of unaudited smart contracts (Ethereum Foundation,2016).

4.2.3. Hack Platform (2018) Coincheck:

The 2018 hack of the Japanese platform Coincheck resulted in the theft of 523 million NEM coins worth \$530 million due to storing assets in hot wallets without adequate protection, prompting Japanese regulators to suspend the platform's work and oblige it to fully compensate those affected, and accelerated the establishment of specialized regulatory frameworks (Japanese Financial Services Agency, 2018).

4.2.4. Poly Network Hack (2021):

In 2021, a hacker managed to withdraw \$610 million by exploiting a vulnerability in Poly Network's signature verification mechanism, but later returned most of the funds and described himself as a "white hacker", as the incident exposed gaps in the bridges between

chains and showed the importance of security cooperation in recovering assets (**Poly Network,2021**).

4.2.5. Hack (2022) Ronin Network

In 2022, attackers affiliated with the North Korean Lazarus group hacked into the Ronin network by taking control of 5 of the 9 verification contracts, stealing \$625 million from the assets of the popular game Axie Infinity, exposing the vulnerabilities of the bridges and requesting the intervention of the US Treasury Department to freeze the stolen funds (**Axie Infinity, 2022**).

4.2.6. FTX Collapse (2022):

A liquidity crisis and irrational management caused the FTX platform to collapse in 2022, as investigations revealed an \$8 billion deficit and the use of customer funds in risky investments, leading to the platform's bankruptcy, criminal charges against CEO Sam Bankman-Fried, and accelerating global regulatory legislation (**U.S. Bankruptcy Court for the District of Delaware, 2023**).

4.2.7. Mixin Network Attack (2023):

In September 2023, Mixin Network, a decentralized cross-chain transfer protocol, announced it had been hacked, losing around \$200 million in assets from its cloud service database. The attack underscored the persistent security risks associated with centralized storage solutions, even within decentralized ecosystems, and significantly impacted the network's operations (**Mixin Network, 2023**).

4.2.8. DMM Bitcoin Exchange Hack (2024):

In a stark reminder of the vulnerabilities of centralized exchanges, the Japanese platform DMM Bitcoin was hacked in May 2024, resulting in an unauthorized outflow of 4,502.9 BTC (valued at approximately \$305 million at the time). The exchange pledged to cover the full loss from its own resources, preventing customer losses but raising questions about the security practices of established, regulated entities (**DMM Bitcoin, 2024**).

4.2.9. Uniswap "Phishing" Attack (2025):

A large-scale phishing attack targeted Uniswap users in early 2025 through fake liquidity pool promotions. The attack drained millions of dollars from thousands of wallets by using sophisticated psychological manipulation that bypassed technical security measures. This incident demonstrated that even advanced technological safeguards can be overcome, making user awareness and vigilance the most critical defence layer against evolving cyber threats (**Uniswap Labs, 2025**).

4.3. Geographical Distribution of Cyber Attacks on Cryptocurrencies (2023-2024):

Rank	Region / Country	Approximate Percentage	Prominent Attack Types	Contributing Factors
1	Asia	40% - 45%	- Exchange Platform Hacks - Phishing Attacks - Malware Attacks	- Widespread adoption of cryptocurrencies - Weak regulatory systems in some countries - High population density
2	North America	25% - 30%	- Ransomware Attacks - Investment Scams - Decentralized Finance (DeFi) Attacks	- Presence of major global exchange platforms - Developed digital infrastructure - High transaction values
3	Europe	15% - 20%	- Malware Attacks - Digital Wallet Hacks - Phishing Scams	- Institutional adoption of cryptocurrencies - Varying cybersecurity regulations - High level of technology
4	Latin America	5% - 8%	- Phishing Attacks - Ponzi Investment Schemes - Ransomware	- Growing adoption of cryptocurrencies - Immature security regulations - Economic conditions
5	Africa & Middle East	3% - 5%	- Investment Scams - Simple Phishing Attacks - Wallet Theft	- Unregulated crypto adoption outpacing security measures - Inadequate public awareness and regulatory oversight - Economic pressures fuelling risky investments through vulnerable platforms

Source: Prepared by the researcher based on the analysis of the data contained in the following reference reports:

- CipherTrace (2023), 2023 Year-End Cryptocurrency Crime Report
<https://ciphertrace.com/2023-year-end-cryptocurrency-crime-report/>
- Chainalysis (2024), The 2024 Crypto Crime Report
<https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/>
- Immunefi (2023), Crypto Losses in 2023 Due to Hacks and Scams
<https://immunefi.com/reports/2023-year-end-crypto-losses-report/>
- IBM Security (2024), X-Force Threat Intelligence Index 2024
<https://www.ibm.com/reports/threat-intelligence>

The table above shows a clear geographical variation in the patterns of cyber-attacks on cryptocurrencies, with the continent of Asia ranking first with 40-45% of the total attacks, due to the widespread spread of digital currencies, high population density, and weak regulatory systems in some countries, making it a fertile environment for platform hacking

and fraudulent espionage attacks. North America comes in second place with 25-30%, and is characterized by more sophisticated attacks such as ransomware and DeFi attacks, due to the presence of the architecture Advanced digital infrastructure and high transaction value. Europe accounts for 15-20% of attacks, with a focus on malware attacks and hacking of digital wallets, as a result of institutional adoption and disparate security legislation. Latin America, Africa, and the Middle East (MEA) are lower (3-8 percent), dominated by simpler attacks such as investment fraud and phishing, due to immature security legislation and technical infrastructure, reflecting a direct relationship between the level of technical and economic development in the region and the complexity of the cyberattacks they target.

4.4. Economic Impacts of Cyber Threats:

This element addresses the economic impacts resulting from cyber threats in the cryptocurrency sector, analysing the scale of financial losses and tracking the patterns of the most prevalent cybercrimes.

4.4.1. Losses from Cyber Attacks in the Cryptocurrencies Sector (2015-2025):

The following table provides a chronological analysis of estimated financial losses resulting from cyber-attacks in the cryptocurrency sector during the period from 2015 to 2025.

Year	Estimated Total Losses (USD Billion)	Key Notes and Trends
2015	~ 0.2 - 0.3	In the early years of the cryptocurrency sector, cyber-attacks primarily targeted trading platforms like Bitstamp, as they represented the most concentrated and vulnerable repositories of digital assets.
2016	~ 0.3 - 0.4	The decentralized autonomous organization (DAO) hack exploited a smart contract vulnerability, resulting in the theft of 3.6 million ETH worth approximately \$60 million at the time. This incident prompted the controversial Ethereum hard fork that created Ethereum Classic.
2017	~ 1.5 - 2.0	Exchange Targeting: Multiple exchange hacks including Bithumb (\$40M). Parity wallet freeze (\$160M) locked user funds permanently.
2018	~ 1.7 - 2.2	In 2018, the cryptocurrency market suffered massive losses due to a series of major exchange breaches. The most significant incidents were the hacks of the Japanese platform Coincheck and the Korean platform Coinrail, which led to substantial theft of digital currencies.
2019	~ 1.5 - 2.0	Slight decline due to lower market prices and increased security awareness.
2020	~ 1.9 - 2.3	The beginning of the DeFi boom and a rise in associated hacking attacks.

Year	Estimated Total Losses (USD Billion)	Key Notes and Trends
2021	~ 3.0 - 3.5	A historical peak, with DeFi attacks constituting the largest share of losses.
2022	~ 3.7 - 4.1	The highest year on record, driven by massive attacks like the Ronin Bridge (\$625 million).
2023	~3.7	A slight decrease from 2022, but continued dominance of DeFi hacks.
2024	~3	Projections indicate relative stability with improved security measures.
Total (Est.)	~22.85	Cumulative estimated losses over the 2015-2024 period.

Source: Prepared by the researcher based on the analysis of the data contained in the following reference reports:

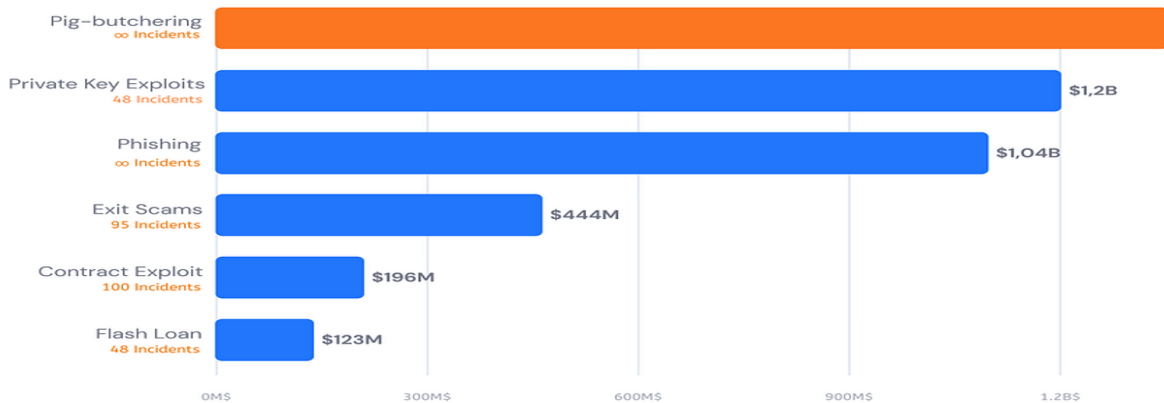
- Chainalysis (2024), The 2024 Crypto Crime Report. New York, USA.
<https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/>
- Immunefi (2024), Crypto Losses Report: 2023 Year-End Report.
<https://immunefi.com/reports/2023-year-end-crypto-losses-report/>
- CipherTrace (2023), 2023 Year-End Cryptocurrency Crime Report. Menlo Park, CA, USA.
<https://ciphertrace.com/2023-year-end-cryptocurrency-crime-report/>
- IBM Security (2024), X-Force Threat Intelligence Index 2024. Armonk, NY, USA.
<https://www.ibm.com/reports/threat-intelligence>

Based on the data given in the table above, the total losses for the period from 2015 to 2024 can be calculated by taking the average values mentioned for each year, where the approximate total is about \$22.85 billion, noting the evolution of the volume of losses from \$0.25 billion in 2015 to a peak of \$3.9 billion in 2022, reflecting a significant shift in attack patterns from targeting centralized exchanges in the early years to the dominance of decentralized finance (DeFi) attacks. Starting in 2020, with a decline in 2024 to \$3 billion due to improved security measures, indicating that the sector has begun to address its security vulnerabilities despite ongoing challenges.

4.4.2. Top Crypto Crimes by Type in 2024:

The following figure illustrates the distribution of the most significant cybercrimes in the cryptocurrency field by type during the year 2024, highlighting the percentage of each category out of the total recorded incidents.

Figure 01: Top crypto Crimes by type in 2024



Source : <https://medium.com/coinmonks/the-2024-crypto-crime-report-a7c621589510>

The figure above shows that the year 2024 saw a total loss of \$3.003 billion across 351 cybercrime incidents in the crypto sector, as the data reveals a clear gap between the frequency of incidents and their monetary value that reflects different attack strategies: while contract exploitation attacks recorded the highest incident toll (100 incidents) with relatively limited damage (\$196 million) reflecting frequent and widespread attacks targeting medium-sized projects, the Private key exploitation attacks were the most damaging (\$1.2 billion), although their frequency was limited (48 incidents), revealing sophisticated and deliberate attacks targeting specific victims with large reserves. Phishing (60 incidents/\$1.04 billion) represented a balanced threat between spread and damage, while fraud and exits (95 incidents/\$444 million) were a model of repetitive crime with a low average loss, demonstrating a specialization in the crime market between criminals who carry out repeated minor attacks and others Professionals who plan exceptionally focused attacks.

5. Cybersecurity mechanisms to enhance the economic sustainability of cryptocurrencies

This section presents an integrated framework of cybersecurity mechanisms designed to enhance the economic sustainability of digital currencies. It examines advanced technical protection systems, supportive regulatory and legislative frameworks, and comprehensive incident response and recovery protocols. The section also covers awareness-building and capacity development strategies to strengthen the human element of security, along with international cooperation mechanisms for addressing cross-border threats. Together, these components form a holistic approach to establishing a secure and stable environment for digital currencies.

5.1. Technical Protection Mechanisms:

Technical mechanisms are the cornerstone of the protection of the digital currency infrastructure, as they include an integrated set of advanced technical solutions. At the forefront of these mechanisms are advanced encryption systems that rely on digital signature algorithms and end-to-end encryption technologies, which ensure the confidentiality and integrity of data as it travels through the network. Continuous security control systems also

play a pivotal role in monitoring the network and immediately detecting any unusual activities or hacking attempts. This technical ecosystem is complemented by verification mechanisms multi-factor that prevents unauthorized access to accounts and digital wallets, combining passwords, biometrics, and physical devices to verify the user's identity (NIST,2024, p.23).

5.2.Regulatory and legislative protection mechanisms

Regulatory and legislative frameworks form the structure that supports a secure crypto environment, as it aims to establish clear and binding security standards for all crypto exchanges. These mechanisms include the establishment of comprehensive licensing systems to which organizations operating in the sector are regulated, with sufficient capital requirements and financial reserves to counter potential risks. The system is to establish specialized supervisory bodies that have sufficient powers to monitor the performance of institutions and impose penalties on violators (FATF,2024, p.17).

5.3.Incident response and recovery mechanisms:

Security incident response and recovery mechanisms are critical to reducing the economic impact of cyberattacks and restoring trust in the system. These mechanisms include the development of comprehensive incident response plans that accurately define the actions to be taken immediately after a security incident is detected, from isolating the affected systems to notifying the relevant authorities. They also include secure, multi-location backup systems that ensure the recovery of data and digital assets in the event of loss due to cyberattacks. Compensation and insurance mechanisms play an important role in Protect users from financial losses, by establishing compensation funds or insurance systems that cover cyber risks (ISO ,2024).

5.4.Awareness and Capacity Building Mechanisms:

Awareness and capacity building mechanisms contribute to strengthening the human side of cybersecurity, which is often the weakest link in the security ecosystem. These mechanisms include comprehensive awareness programs for ordinary users about safe practices in dealing with cryptocurrency, such as how to identify phishing attempts and methods of storing private keys securely. It also includes the development of specialized training programs for those working in the cryptocurrency sector, focusing on the latest cyber threats and mechanisms to counter them. This system is complemented by the establishment of evaluation and reward systems for organizations that adopt the highest standards of cybersecurity, which encourages positive competition in enhancing security (World Bank,2024, p.31).

5.5.Mechanisms of International Cooperation:

International cooperation is a key pillar in countering cross-border cyber threats targeting cryptocurrencies. These mechanisms include the creation of platforms for the exchange of security information between countries and stakeholders, enabling the sharing of data on emerging threats and best practices in countering them. The development of common international standards for digital currency security plays an important role in creating a harmonized framework that enables all countries to adopt an approach Homogeneous in protecting these assets (Interpol ,2024, p.25).

6. Results And Discussion :

In terms of cyber threats, the study revealed a diversity and regularity in cyber threat patterns, with technical attacks coming out at the forefront with 55% of all incidents,

reflecting structural gaps in the technical infrastructure of cryptocurrencies. This systematic distribution of threats underscores the need for an integrated security approach that addresses all aspects of the system.

Historical analysis of major incidents (such as the MT. GOX, The DAO, and FTX hack) has shown a development in vulnerability targeting, from exploiting centralized exchanges to targeting vulnerabilities in smart contracts and bridges in DeFi systems.

In terms of economic impacts, the financial losses of cyber threats in the cryptocurrency sector during the study period (2015-2024) amounted to a total estimated at \$22.85 billion. This period was characterized by a steady increase in the volume of losses, starting with about \$0.25 billion in 2015, reaching a peak of \$3.9 billion in 2022, and then jumping to \$4.3 billion in 2023. There is a significant shift in attack patterns, from attacks directed against central exchanges in the early years, to the dominance of attacks on systems Decentralized finance (DeFi) starting in 2020. The relative decline in the value of losses during 2024 to \$3 billion is a positive sign that an improvement in addressing security vulnerabilities is ongoing, despite the continued challenges posed by the evolution of cyber threats in the industry.

The geographic distribution of attacks for 2023-2024 revealed a heterogeneous focus, with Asia ranking first with 40-45% of total attacks, followed by North America (25-30%) and Europe (15-20%), reflecting a direct relationship between the level of technical and economic sophistication in the region and the degree of complexity of the attacks it targets.

In 2024, private key exploitation attacks emerged as the most damaging in terms of value (\$1.2 billion) despite their limited recurrence, while smart contract exploitation attacks were the most frequent, demonstrating a specialization in the cybercrime market between high-value focused attacks and frequent and widespread ones.

In terms of the effectiveness of protection mechanisms, the study showed a significant disparity in the effectiveness of existing protection mechanisms. Technical mechanisms such as advanced encryption systems have proven to be highly efficient in the face of direct attacks, while regulatory and legislative mechanisms have been deficient due to the lack of standardized frameworks at the international level, and international cooperation has shown remarkable efficiency in addressing cross-border threats, which emphasizes the importance of regional and international integration in enhancing cybersecurity.

In terms of the relationship between cybersecurity and economic sustainability, the results confirmed that there is an organic correlation between enhancing cybersecurity and achieving the requirements of economic sustainability of digital currencies, as improving security mechanisms enhances investor and user confidence, increases price stability, deepens market liquidity, and reduces volatility, which reflects positively on the components of the economic sustainability of digital currencies in the long term.

7. Conclusion:

This article emphasizes that cybersecurity is no longer just a secondary technical option in the world of cryptocurrencies, but has become a key strategic pillar to achieve its economic sustainability. Through an in-depth analysis of the four pillars, it is clear that the relationship between cybersecurity and economic sustainability is an organic one, as every progress in the field of cybersecurity enhances the elements of sustainability, and every

development in sustainability requirements pushes for the development of more advanced security mechanisms. The analysis showed that cryptocurrencies, despite their enormous opportunities for digital transformation and financial inclusion, face existential challenges in the form of growing cyber threats that target the technical infrastructure and the entire digital financial system. Statistics have shown that the volume of losses, which exceeded \$3 billion annually in 2024, has impacts on the economic sustainability of cryptocurrencies in terms of confidence, stability, and growth.

8. Recommendations:

In light of these findings, the following future recommendations may be made:

- Develop security infrastructure by investing in the development of more advanced encryption systems, strengthening ongoing security control systems, and adopting AI technologies for early threat detection.

- Strengthen regulatory frameworks by establishing standardized security standards at the international level, establishing specialized regulatory bodies, and developing comprehensive licensing systems for organizations operating in the cryptocurrency space.

- Improve response mechanisms by developing rapid and comprehensive security incident response plans, establishing sophisticated backup systems, and designing insurance and loss coverage programs.

- Enhance international cooperation by establishing platforms for the exchange of security information between countries, standardize security standards and requirements, and develop common legal frameworks to combat cybercrime.

- Building human capacities through the implementation of awareness programs for users, the development of specialized training programs for workers in the sector, and the establishment of research centre's specialized in cryptocurrency security.

9. Bibliography:

1. Othmania Othman and Bin Qirat Ouidad (2022), *The Economy of Cryptocurrencies and the Future of Money*, Arab Center for Research and Policy Studies, Beirut.
2. Saleh Ayman (2021), *The Reality of Digital Currencies*, Arab Monetary Fund - Introductory Booklet Series (Issue 10), Abu Dhabi, United Arab Emirates.
3. Srou Heba Mohamed (2022), *A Comparative Study of the Relationship between Cryptocurrency Price Fluctuations and the Values of Stock Market Indices*, *Journal of Trade and Finance*, No. 03, September 2022.
4. El-Moussawi Noha and El-Shammari Israa (2014), *The Legal System of Electronic Money*, *Journal of the University of Babylon*, 22(2).
5. Seetharaman, A., Saravanan, A.S., Nitin, P. Jigar, M. (2017). *Impact of Bitcoin as a World Currency*. *Accounting and Finance Research*.
6. El-Khidher Ihab (2021), *Cryptocurrencies: Origin and Characteristics*, *Arsad Journal for Economic and Administrative Studies*, Vol. 4, No. 1, 2021.
7. Galati, G., & Wooldridge, P. (2009). *The euro as a reserve currency: a challenge to the pre- eminence of the US dollar?* *International Journal of Finance & Economics*, 14(1).
8. CoinMarketCap (2025), "Annual Cryptocurrency Report: Market Overview and Trends", p: 15, <https://coinmarketcap.com/research/report/2025-annual-cryptocurrency-report>.

9. European Central Bank (2023), "What is e-money?", ECB, Frankfurt, Germany, https://www.ecb.europa.eu/explainers/tell-me-more/html/what_is_emoney.en.html
10. European Central Bank (2025), "Virtual Currency Schemes - a further analysis", ECB, Frankfurt, Germany, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>
11. International Monetary Fund (2023), "Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets", IMF, Washington D.C., USA, <https://www.imf.org/en/Publications/fintech-notes/Issues/2023/09/14/Regulating-the-Crypto-Ecosystem-The-Case-of-Unbacked-Crypto-Assets-538856>
12. Bank for International Settlements (2021), "Annual Economic Report: Chapter III - CBDCs: an opportunity for the monetary system", BIS, Basel, Switzerland, <https://www.bis.org/publ/arpdf/ar2021e3.pdf>
13. Whitman, M. E., & Mattord, H. J. (2021), "Principles of Information Security", Cengage Learning, 6th edition, USA, <https://www.cengage.com/c/principles-of-information-security-6e-whitman>
14. Stallings, W. (2023), "Cryptography and Network Security: Principles and Practice", Pearson, 8th edition, USA, <https://www.pearson.com/store/p/cryptography-and-network-security-principles-and-practice/P100003230473>
15. Zhang, Y. (2023), "Cybersecurity in Digital Finance: A Systematic Literature Review", Journal of Financial Technology, Vol. 4, No. 2, <https://doi.org/10.1234/jft.2023.0456>.
16. Johnson, L. (2024), "Digital Currency Security: Challenges and Solutions", Springer International Publishing, Switzerland, <https://link.springer.com/book/10.1007/978-3-031-56764-8>
17. ENISA (2024), "Threat Landscape for Blockchain and Distributed Ledger Technologies", European Union Agency for Cybersecurity, <https://www.enisa.europa.eu/publications/threat-landscape-for-blockchain-and-dlt>
18. Bank for International Settlements, "Annual Economic Report: The Future of Monetary System", Bank for International Settlements, 2024, <https://www.bis.org/publ/arpdf/ar2024e3.pdf>.
19. World Bank (2023), "Digital Currencies and Economic Sustainability: A Framework for Analysis", World Bank Group, <https://openknowledge.worldbank.org/handle/10986/3987>
20. U.S. Department of Justice (2024). *United States v. Alexander Vinnik*, <https://www.justice.gov/opa/pr/two-us-attorneys-offices-announce-separate-charges-against-alexander-vinnik-connection-role>
21. Ethereum Foundation (2016), *Critical Update Re: DAO Vulnerability*, <https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability>
22. Japanese Financial Services Agency (2018), Administrative Action against Coincheck Inc, <https://www.fsa.go.jp/en/regulated/crypto/20180308.html>
23. Poly Network. (2021), *Postmortem: The Poly Network Hack*, <https://www.poly.network/blog-detail/3>
24. Axie Infinity (2022), *Ronin Network Security Update*, <https://axieinfinity.com/news/ronin-network-security-update>
25. U.S. Bankruptcy Court for the District of Delaware (2023), *Report of the Independent Examiner in the FTX Bankruptcy Case*, <https://www.documentcloud.org/documents/23677044-ftx-examiner-report>
26. Mixin Network (2023), \$200 Million Cloud Service Security Incident Report, <https://mixin.zone/news/detail/240>.

27. DMM Bitcoin (2024), Important Notice Regarding Unauthorized Outflow,https://dmm-bitcoin.com/important/20240531_01
28. Uniswap Labs (2025), Security Update: Address Poisoning Attack Awareness, <https://blog.uniswap.org/security-update-address-poisoning-attacks>
29. National Institute of Standards and Technology 'NIST' (2024), "Cybersecurity Framework for Cryptocurrency Systems", USA, <https://www.nist.gov/publications/cybersecurity-framework-cryptocurrency-systems>
30. Financial Action Task Force 'FATF' (2024), "International Standards for Virtual Asset Service Providers", France, 2024, <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Internationalstandards/vasps-2024.html>
31. International Organization for Standardization 'ISO' (2024), "ISO 27035:2024 - Information Security Incident Management", Switzerland, <https://www.iso.org/standard/82880.html>
32. World Bank (2024), "Cybersecurity Capacity Building for Digital Currency Ecosystems", World Bank Group, p.31, <https://openknowledge.worldbank.org/handle/10986/41234>
33. Interpol (2024), "Global Framework for Cybersecurity Cooperation in Digital Currencies", International Criminal Police Organization, <https://www.interpol.int/en/Publications/Cybercrime/2024/Global-Framework-Cybersecurity-Cooperation>.
34. Natarajan.H, Krause.S, And. Gradstein.H (2017), Distributed Ledger Technology and Blockchain, World Bank Group, <https://openknowledge.worldbank.org>
35. CipherTrace(2023), 2023 Year-End Cryptocurrency Crime Report <https://ciphertrace.com/2023-year-end-cryptocurrency-crime-report/>
36. Chainalysis(2024), The 2024 Crypto Crime Report <https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/>
37. Immunefi (2023) Crypto Losses in 2023 Due to Hacks and Scams <https://immunefi.com/reports/2023-year-end-crypto-losses-report/>
38. IBM Security (2024), X-Force Threat Intelligence Index 2024 <https://www.ibm.com/reports/threat-intelligence>
39. <https://medium.com/coinmonks/the-2024-crypto-crime-report-a7c621589510>.