

**Cryptography as Digital Sovereignty: An impact analysis of its uses,  
challenges, and modern applications**

**Maricarl C. Leño\***

Technological University of the Philippines  
Taguig City, Philippines  
Email: maricarlleano@gmail.com

**Josh Christian I. Bernabe**

Technological University of the Philippines  
Taguig City, Philippines  
Email: joshbernabe0829@gmail.com

**Mark Kent I. Del Rosario**

Technological University of the Philippines  
Western Taguig City, Philippines  
Email: delrosariomarkkent@gmail.com

**Edilyn P. Mallo**

Technological University of the Philippines  
Taguig City, Philippines  
Email: edilynmallo6@gmail.com

**Karl Jexel A. Talaba**

Technological University of the Philippines  
Taguig City, Philippines  
Email: karljexelt@gmail.com

**Pops V. Madriaga**

Technological University of the Philippines  
Taguig City, Philippines  
Email: pops\_madriaga@tup.edu.ph

---

\*Corresponding author

DOI: <http://doi.org/10.69651/PIJHSS0404494>

Recommended citation:

Leño, M. C., Bernabe, J. C. I., Del Rosario, M. K. I., Mallo, E. P., Talaba, K. J. A., & Madriaga, P. V. (2025). Cryptography as Digital Sovereignty: An impact analysis of its uses, challenges, and modern applications. Pantao (The International Journal of the Humanities and Social Sciences) 4 (4), 5337-5345.  
<http://doi.org/10.69651/PIJHSS0404494>

## ABSTRACT

Since it evolved from a secretive military tool, cryptography has been a potent instrument in the hands of governments, businesses, and individuals to administer infrastructure and protect the integrity of their systems. It has become an integral part of digital independence. Examples of these industries are e-commerce, finance, and healthcare. It also helps to design Blockchain, cryptocurrency, and innovative contract technologies. Cryptography supports the stability of operations in a digital environment by protecting data and its privacy, ensuring the security of exchanges, and confirming identities. For instance, the protection of financial transactions through the Internet is guaranteed by the encryption methods (SSL/TLS). The stability of communications is ensured by encryption methods (SSL/TLS), and digital signatures and certificates guarantee the reliability of communication. Likewise, using a cryptographic system to protect personal data in medical facilities would significantly boost privacy and responsibility. The real-life application examples show that an organization can use cryptography to secure and gain control over its internet-based resources. However, cryptography has a dark side. It is more sophisticated and targeted by cybercriminals. Moreover, cryptographic attack threats on the Internet keep improving. The issue of quantum computing endangers the encryption process embraced by traditional means, and there is a need to develop post-quantum cryptography and other more sophisticated systems. The above issues highlight that cryptography, although an essential tool, must not be the sole method of ensuring digital security. This study considers the practical benefits and limitations of cryptography for digital sovereignty. The findings show that cryptography protects digital systems, trust, and innovation. However, its integration with cybersecurity programs can be effective only when the regulatory systems are enforced and constantly improved. Cryptography strengthens digital independence by establishing a secure and dependable digital ecosystem, but it needs comprehensive strategic support to ensure resilience in a complicated environment.

**Keywords:** Cryptography, Digital Sovereignty, security, privacy, cybersecurity, digital infrastructure

Date Submitted: August 1, 2025

Date Accepted: September 4, 2025

Date Published: October 3, 2025

## INTRODUCTION

In an increasingly interconnected world, digital information has become one of the most valuable resources. The rise of global communication, e-commerce, and cloud services has heightened the need to secure data against theft, manipulation, and misuse. States, organizations, and individuals are responsible for exercising authoritative control over their digital systems, technologies, and data streams, which is referred to as digital sovereignty, and these developments have increased focus. Cryptography offers the tools needed to ensure confidentiality, authenticity, and integrity in the digital media world, which is currently considered a fundamental element of this study.

Cryptography is widely applied beyond conventional security. The cryptographic protocols, such as SSL/TLS, ensure the security of sensitive information, such as payment and banking information, during e-commerce and financial transactions. Digital signatures and authentication methods enhance the reliability of communication and governance systems, ensuring trust and accountability in any digital platform. Besides, due to the advent of Blockchain, cryptocurrencies, and smart contracts, cryptography has made it possible for new patterns of transparency and decentralization to transform economic and technological spaces.

Nonetheless, despite its transformative advantages, cryptography exists in changing issues. Cyberattacks are becoming increasingly complex in their approach to encryption systems, and sophisticated methods are being used to combat them. Meanwhile, the high rate of quantum computing advancement endangers the sustainability of modern cryptography algorithms, and it requires novel approaches, including post-quantum cryptography.

This paper, *Cryptography as Digital Sovereignty: An Impact Analysis of Its Uses, Challenges, and Modern Applications*, seeks to analyze how cryptography strengthens digital sovereignty, explore its limitations in the face of emerging threats, and highlight its role in shaping the secure digital future.

### Statement of the problem

The study seeks to answer the central question: How does cryptography contribute to digital sovereignty amid its evolving uses, challenges, and modern applications? Specifically, it aims to address the following sub-questions:

1. What are the practical benefits of cryptography in enhancing digital security, privacy, and trust across sectors such as finance, healthcare, and communication?
2. What challenges and risks are associated with the widespread adoption of cryptographic technologies, including economic, technical, and ethical dimensions?
3. How do emerging innovations such as blockchain and quantum computing redefine the future implications of cryptography in sustaining digital sovereignty?
4. To what extent can cryptography, when integrated with broader cybersecurity and regulatory frameworks, strengthen the resilience and autonomy of digital infrastructures?

### METHODOLOGY

The study employed a qualitative and descriptive research design using an impact analysis framework to examine the multifaceted role of cryptography in the digital world. Rather than delving into the mathematical foundations of cryptographic algorithms, the research focused on real-life applications, particularly how blockchain technology shapes online communication, finance, and healthcare systems. This design allowed the researchers to provide an in-depth understanding of the social, economic, and technological implications of cryptography across different sectors while emphasizing its real-world significance.

To ensure the credibility and relevance of the information gathered, data were collected from a wide range of peer-reviewed studies, technical papers, and research articles. Most of these sources originated from blockchain-related research, with others focusing on healthcare

applications such as cryptography in electronic health records, e-business transaction protocols, and general cryptography concepts. These materials formed the basis of the group's analysis, offering diverse yet reliable perspectives on the topic. The collection process was designed to capture the breadth of existing literature while emphasizing studies that demonstrated practical applications of cryptographic systems.

Once the data were compiled, a rigorous screening and selection process was conducted to guarantee reliability and validity. Materials that were outdated, purely theoretical, or unrelated to the research objectives were excluded. Only studies that provided practical insights and reflected current trends in the use of cryptography were retained. This filtration process ensured that the resulting dataset accurately represented contemporary realities, thereby aligning the analysis with the study's goal of exploring cryptography's tangible effects in modern digital environments.

Following data screening, thematic categorization and analysis were employed to interpret the findings. The information was organized into three major themes: positive impacts, adverse effects, and future implications. The positive impacts highlighted the enhancement of data security and integrity facilitated by cryptographic systems, while the adverse effects underscored challenges such as high implementation costs and potential misuse by cybercriminals. The final theme centered on the emerging implications of quantum computing, which presents both risks to current encryption systems and opportunities for developing stronger, more resilient cryptographic techniques. This thematic framework allowed the researchers to balance the discussion between benefits and drawbacks while projecting the future trajectory of the field.

In the evaluation and interpretation phase, the findings demonstrated that cryptography plays a crucial role in maintaining confidentiality, integrity, and trust in communication, healthcare, and financial systems. The decentralized nature of blockchain emerged as a major advantage in promoting transparency and security, yet persistent challenges such as vulnerabilities, cybercrime, and key management continued to hinder optimal implementation. It was further observed that no single approach could comprehensively address these domain-specific issues. Finally, the emergence of quantum computing was identified as both the most significant threat and the most promising advancement for the future of digital security. The study thus concluded that the evolution of post-quantum cryptography will be central to sustaining trust and resilience in an increasingly digitalized world.

## RESULTS AND DISCUSSION

The study utilized a qualitative and descriptive research design grounded in an impact analysis framework to examine the real-world applications and consequences of cryptography across multiple domains. Although the study did not involve human participants, it relied extensively on secondary data gathered from peer-reviewed literature, research reports, and academic papers. These materials were selected through a careful screening process to ensure that only current, credible, and practically relevant sources were included. The analysis drew primarily from research on blockchain, with supplementary studies on healthcare, e-business, and general cryptographic principles. This methodological approach allowed for a

comprehensive and balanced understanding of cryptography's influence in promoting digital sovereignty, data security, and trust across industries.

### Research design and approach

Security and trust in the digital environment are fundamentally anchored in cryptography. The findings revealed that encryption protocols safeguard the integrity and confidentiality of communications while enabling secure verification processes and financial transactions. In the financial sector, cryptography facilitates the development of decentralized systems, ensuring transparency and protection against fraudulent activities. Within healthcare, it plays a pivotal role in securing confidential data, supporting telemedicine services, and maintaining regulatory compliance through the protection of electronic health records (EHRs). The analysis also identified scalability issues, energy demands, and key management challenges as major concerns in cryptographic applications. Nonetheless, blockchain technology—an extension of cryptographic innovation—was found to provide decentralization, transparency, and immutability, enhancing the integrity of digital infrastructures. These results indicate that cryptography not only enhances digital security but also stimulates innovation and promotes the balance between efficiency, robustness, and usability within digital ecosystems.

### Data collection

The collected data were derived from diverse sources, as reflected in the distribution of studies analyzed. Most of the literature focused on blockchain and its cryptographic underpinnings, highlighting the substantial academic and industrial attention devoted to decentralized systems. Research on healthcare applications, though fewer in number, offered critical insights into the complexities of encrypting data for telemedicine and the protection of electronic health records. In contrast, e-business studies concentrated on digital trust and transaction protocols, providing perspectives on how cryptography supports online commercial interactions. General studies on cryptographic concepts complemented these specialized applications by establishing a theoretical foundation for the overall analysis. This distribution demonstrated that while blockchain remains the most extensively studied area, integrating literature from other domains created a balanced and credible understanding of cryptography's cross-sectoral influence.

### Data screening and selection

The screening process was instrumental in ensuring the credibility and accuracy of the study's findings. Outdated, purely theoretical, or redundant materials were excluded, and only those demonstrating contemporary and practical cryptographic applications were retained. This process emphasized the necessity of filtering information in a rapidly evolving field where obsolete data could easily compromise research validity. By refining the dataset to include only recent and relevant publications, the researchers ensured that the study reflected current industry standards and technological developments. The data screening outcomes affirmed that the

selected sources were consistent, timely, and aligned with the study's objectives of examining cryptography's real-world impact on digital security and sovereignty.

### Categorization and thematic analysis

Through thematic analysis, three major themes emerged—positive effects, adverse effects, and future implications. The positive effects underscored cryptography's contribution to enhancing data protection, secure communication, and digital trust. It has fortified security systems across multiple sectors by ensuring authenticity and integrity in data exchange. However, the analysis also revealed several drawbacks, including the high cost of implementation, the technical complexity of key management, and the potential misuse of encryption by cybercriminals. Meanwhile, the future implications highlighted the rise of quantum computing as both a risk and an opportunity. Quantum technology could render current encryption methods obsolete but also pave the way for more advanced, quantum-resistant cryptographic systems. Collectively, these findings depict cryptography as a double-edged tool—offering immense benefits for security while presenting formidable challenges that shape its evolution.

### Positive impacts

The study found that cryptography serves as a cornerstone for the protection of digital sovereignty by maintaining secrecy, integrity, and authentication across diverse sectors. In finance and e-commerce, SSL/TLS protocols were shown to safeguard online transactions and mitigate fraud, reinforcing consumer trust and economic stability. In healthcare, encryption technologies strengthened the privacy and accountability of electronic health records, improving patient data protection and confidentiality. Governmental and communication systems also benefited through the use of digital signatures and authentication methods, which enhance transparency and legitimacy in digital governance. Blockchain technology further advanced these developments by introducing decentralized systems that made digital records tamper-proof and less dependent on intermediaries. Collectively, these positive impacts confirm cryptography's central role in fostering secure, trustworthy, and transparent digital environments.

### Negative impacts

Despite its advantages, cryptography also poses considerable challenges. One major issue identified was the high cost of implementation, which can hinder smaller organizations from adopting advanced cryptographic infrastructures. The technology's complexity also leads to difficulties in key management and vulnerability to human error, thereby affecting overall efficiency. Furthermore, encryption—while designed for protection—can be exploited by malicious actors to conceal cybercrimes, such as ransomware attacks and data breaches. These findings reveal that cryptography, though vital, cannot single-handedly ensure cybersecurity. It must function as part of a broader, integrated system of digital protection that includes regulation, policy, and user awareness.

## Future implications

Looking ahead, the study emphasized the dual nature of quantum computing as both a challenge and a catalyst for innovation in cryptography. Current encryption systems such as RSA and elliptic curve (EC) cryptography may become ineffective once quantum computers reach operational maturity, as their computational power could easily decrypt traditional ciphers. However, this same technological advancement offers a new frontier through post-quantum cryptography—an emerging field focused on developing encryption systems that can resist quantum attacks. The pursuit of such research underscores the adaptability and resilience of cryptographic science, ensuring its continued relevance in securing future digital infrastructures.

## Discussion

The findings reaffirm the effectiveness of the qualitative-descriptive research design in exploring cryptography's impact across sectors. By focusing on real-world applications rather than algorithmic complexity, the study successfully illustrated the multifaceted role of cryptography in decentralization, governance, healthcare, and finance. The combination of varied data sources—balanced among blockchain, healthcare, e-business, and general cryptography—provided a robust and credible basis for interpretation. The filtering process further enhanced data integrity, ensuring that only high-quality, contemporary sources were analyzed.

Thematic insights drawn from the study reinforce the duality of cryptography as both a protective and disruptive force. It strengthens accountability, transparency, and trust through technologies like blockchain and digital signatures but also introduces challenges such as implementation cost, technical limitations, and cyber misuse. The looming threat of quantum computing adds another dimension to this balance, emphasizing the urgency for adaptive solutions such as post-quantum encryption.

Ultimately, the research demonstrates that cryptography remains one of the most critical pillars of digital sovereignty. It empowers nations, organizations, and individuals to maintain control over their digital assets while promoting privacy, security, and innovation. However, its success depends on continuous collaboration between technology developers, cybersecurity experts, and policymakers to mitigate risks and ensure sustainable digital independence. Cryptography, therefore, should be understood not as an isolated safeguard but as an integral component of a larger, evolving cybersecurity ecosystem that shapes the future of digital trust and autonomy.

## CONCLUSION

The most imperative aspect of the system of digital modernity is cryptography, which is the most effective tool in protecting and maintaining information and creating the notion of digital sovereignty. Cryptography has changed the financial account, healthcare team, and governance department, introducing transparency, authenticity, and decentralization. These steps will enable individuals, institutions, and governments to protect their information to enhance

information confidence, invention, and liberty over the net. Cryptography will create an autonomous digital realm, technical, social, economic, political, and inhale the forces. The sophisticated factors can be associated with the issue of cryptography, regardless of the benefits of the technology. Classified cybernetic systems eat up and expend giant finances and technical expertise in servicing and system setup. The process of creating encrypted systems is not controllable. It cannot be discussed as unvulcanifiable, as the technologies that contribute to the high level of safety were applied and can be shifted to the wrong individuals and used to organize crimes. These factors infringe on the legality and law of encrypting its use and receipt. These contradictions give birth to the concept of cryptography, which is a two-polar phenomenon to aid the formation of the implication of sovereignty of the digital, which cannot be standardized and can be governed, resurrected, and reanimated.

The other issue that should be brought up is the implementation of quantum computing. The vision of quantum technologies threatens the classical cryptographies of the domicile and the producers of the block mechanisms of the vast majority of all digital beings in the world. The team is also developing post-quantum encryption and its inclusion in the security program. A collective initiative of research, regulation, and innovations in evading this issue is the primary means of providing communication systems that will never be vulnerable to further attacks.

Even today, when there is still no viable money on digital security, cryptography is not that magic that has no remedy, yet has no ills. It is among the most desirable building blocks. The cryptographic innovation was not the only concept required to make the world more digitalized and secure. At this level, government, versatility, and cooperation will also be considered internationally. These will all be prepared to seize the sovereignty of digital liberties as well as the ability of civilizations to pick up a shield in the globalized world.

## REFERENCES

Schneier, B. (2015). *Applied cryptography: Protocols, algorithms, and source code* in C. Wiley.

Internet Society. (n.d.). Navigating digital sovereignty and its impact on the Internet. <https://www.internetsociety.org/>

Paar, C., & Pelzl, J. (2010). *Understanding cryptography: A textbook for students and practitioners*. Springer.

Rescorla, E. (2000). *SSL and TLS: Designing and building secure systems*. Addison-Wesley.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126. <https://doi.org/10.1145/359340.359342>

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. <https://bitcoin.org/bitcoin.pdf>



European Union Agency for Cybersecurity (ENISA). (2024). Cybersecurity threat trends 2024. ENISA. <https://www.enisa.europa.eu/>

Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009). Post-quantum cryptography. Springer.

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, 41(10), 1027–1038. <https://doi.org/10.1016/j.telpol.2017.09.003>

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Security techniques for the electronic health records. *Journal of Medical Systems*, 41(8), 127. <https://doi.org/10.1007/s10916-017-0778-4>

Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson.

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on post-quantum cryptography. National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8105>

National Institute of Standards and Technology (NIST). (2023). Cryptographic standards and guidelines. NIST. <https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines>

European Union Agency for Cybersecurity (ENISA). (2023). Cryptography in the digital era. ENISA. <https://www.enisa.europa.eu/publications/>

Kshetri, N. (2021). Cryptography and security in the age of digital transformation. *IEEE IT Professional*, 23(2), 67–72. <https://doi.org/10.1109/MITP.2021.3058663>

Cloud Security Alliance (CSA). (2022). Future of cryptography. CSA Reports. <https://cloudsecurityalliance.org/>