The Role of Cryptocurrency in Financial Privacy and Cybersecurity

Jason Pham

IT-104-B01

June 16, 2025

"By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on https://academicstandards.gmu.edu/wp-content/uploads/2023/08/George-Mason-University-Honor-Code-2023-2024-final-version-SaveasPDF.pdf and as stated, I as student member of the George Mason University community pledge not to cheat, plagiarize, steal, or lie in matters related to academic work. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of text, any material copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on http://copyright.gmu.edu/?page_id=301 web site."

The Role of Cryptocurrency in Financial Privacy and Cybersecurity

Introduction

In the past, when we were using a big computer to access the Internet, we are exploring and developing more digital technologies that we could think of. Now we are in an era when digital assets are a common thing. Individuals, companies and large organizations are also involved in digital assets like Cryptocurrency. In this digital world, cryptocurrencies are promising to enhance anonymity and decentralized control over financial transactions. According to the authors Alnıpak and Toraman, this blockchain technology offers many benefits for improving transactional efficiency, transparency and security as seen in applications ranging from supply chain logistics to international payments (Alnıpak & Toraman, 2024). However, this technology also has its bad side as well. This paper will be investigating all the roles of cryptocurrency in the financial privacy and cybersecurity aspects. As on-chain crime becomes increasing, the total value received by illicit cryptocurrency addresses reached an estimated $40.9 billion in 2024, this underscores the scale of the problem (Chainalysis, 2025, p.4). We will be exploring the features of blockchain technologies that protect the user privacy and how cryptocurrencies are used in illegal activities

This paper will provide all the aspects and argue that the cryptocurrency's blockchain technologies give to human society a benefit in financial efficiency and user control. The core features of pseudonymity, decentralization and the regulatory environment create risks for financial privacy as well as cybersecurity. These risks are not only in global fraud and money laundering operations but also involved in corporate/organizations wrongdoing. This paper will outline the technological promise of blockchain, then go deeper into the complex legal and ethical issues that we are currently facing. Finally, we will provide a detailed analysis of the security risks that cryptocurrencies pose to individuals, organizations, and the financial system.

Technology Overview: The Promise of a Decentralized Future

Blockchain technology is fundamentally a decentralized ledger system that stores transaction records across a distributed network, significantly reducing reliance on central authorities or intermediaries. Each transaction is cryptographically secured and added sequentially into blocks, which are immutable once added, thereby ensuring a high level of transparency and security. This decentralization not only streamlines processes but also minimizes risks associated with single points of failure or control, which are common in traditional centralized systems.

Moreover, blockchain's unique capability to create and enforce smart contracts has profound implications for automating complex transactions and agreements. Smart contracts execute automatically when predefined conditions are met, significantly reducing manual intervention and the potential for human error or fraud. Industries such as supply chain management, maritime logistics, and finance have already started adopting blockchain to enhance operational efficiencies and improve trust among participants (Alnıpak & Toraman, 2024).

The financial sector, in particular, has benefited significantly from blockchain technology by enabling faster and more secure cross-border transactions. Blockchain can drastically reduce transaction times from days to minutes, or even seconds, enhancing liquidity and reducing transaction costs. This capability is particularly appealing in international trade and financial services, where traditional payment processing involves multiple intermediaries and prolonged verification procedures.

However, despite the promising advantages, the widespread adoption of blockchain technology is still hindered by several technical and regulatory challenges. Technological barriers include scalability issues, high energy consumption, and the need for interoperability among diverse blockchain systems. Furthermore, the absence of global technical standards and comprehensive regulatory frameworks poses significant obstacles to its universal adoption and integration into existing financial systems (Mehta & Chawla, 2024).

Legal, Ethical, and Social Issues

With the rapid rise of cryptocurrencies, they also bring many problems and concerns. Especially with the legal, ethical and social aspects. Governments worldwide are trying to regulate this technology. The tension is palpable between the desire of some users for complete financial anonymity and the legal mandates for Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance imposed on traditional financial institutions to prevent illicit activities. With the pseudonymous nature of cryptocurrencies that brings privacy. It also creates challenges for law enforcement in finding cybercriminals and tax evaders.

To understand why cryptocurrency is a new way for criminal to conduct transactions. The authors Wang and Hsieh provide a useful criminological theory/framework known as the money laundering triangle to understand why cryptocurrencies are so attractive for illicit use. The framework posits that a crime occurs when there is a convergence of motivated offenders, suitable instruments, and inadequate guardianship. Cryptocurrency satisfies all three conditions.

First, motivated offenders are constantly finding a new way to move and obscure funds. The Chainalysis (2025) reports highlights a diverse array of these actors, coming commonly from Cyberattack such as from the ransomware gangs, and including many cybercriminals that involved in darknet market vending and organized crime syndicates. Second, the cryptocurrency serves as a uniquely suitable instrument. Its decentralization means there is no central points of control, and the technologies gives the ability of pseudonymity that allows for a high degree of anonymity. Tools like crypto mixers and privacy coins are used to further obfuscate the trail of funds. For instance, after the $305 million hack of DMM Bitcoin, attackers used a Bitcoin CoinJoin Mixing Service before moving the funds through other services (Chainalysis, 2025, p.84). Third, the current global landscape provides inadequate guardianship. The gap in regulations allows criminals to exploit jurisdictional loopholes. This combination of factors, as Wang and Hsieh (2024) argue, makes cryptocurrency almost a perfect tool for modern money laundering, as well as a host of other types of crimes.

Security Aspects and Challenges

While cryptocurrencies offer new ways to handle money, they also bring a lot of security concerns for both users and the company/organization. Criminals have a new “legal” way to protect themselves from exposure because the pseudonymous nature of cryptocurrencies brings the privacy. Mehta and Chawla (2024) categorize these risks into “barriers” to legitimate use (such as technical complexity and lack of trust) and “illegal usage”. Their research confirms that criminals are using it for illegal activities like money laundering, and it is hard for authorities to follow the money compared to the traditional bank transfer. For normal users, keeping cryptocurrencies is something that we would think it is an easy task. However, this is also a favorite place for hackers to steal the funds. If you are not lucky and get your funds stolen, it is impossible to get them back because of the nature of the cryptocurrency’s technologies.

The anonymity of cryptocurrencies technologies has increased manipulative scams. An example is the “pig butchering” fraud, an incident that happens when criminals use social engineering to build long-term trust with the victim before convincing them to invest large sums of money into a fraudulent cryptocurrency platform (Burrell, 2025). In this attack, cryptocurrency is the primary tool for the final “butchering”, because of the pseudonymous nature of the transactions makes the stolen funds nearly impossible to recover. This example shows how cybercriminals use both human psychology and technology to cause the financial and mental harm. The “pig butchering scam”, which saw its revenue grow by nearly 40% year-over-year in 2024 (Chainalysis, 2025, p.58)

These scams also show a sophistication that emerging “scam as a service” ecosystem. Platforms like Huione Guarantee, a marketplace that tied to a Cambodian conglomerate, provide criminals with the tools they need to plan and execute these frauds at scale. These activities include selling targeted data lists, web hosting services, and even using Generative Artificial Intelligence software that could create a fake personas and realistic content to trick victims into making fraudulent investments (Chainalysis, 2025, p. 63-64). This type of fraud demonstrates a convergence of psychological manipulation and advanced technology, and it involves with cryptocurrency serving as the final, irreversible method of extraction.

The dangers of cryptocurrency are no longer limited to the digital side. The Chainalysis (2025) report a rise in cases where criminals use violence to force crypto transfer. These attacks fall into two categories: opportunistic street crimes, where a stolen phone reveals a crypto wallet, and targeted attacks on high-net-worth individuals. In one notable incident, seven members of a UK gang were sentenced for kidnapping and torturing a crypto investor over several months to extort his funds. In another incident, the co-founder of the hardware wallet brand Ledger was kidnapped from his home and held for ransom (Chainalysis, 2025, p.133). These incidents show that the perceived wealth stored in crypto wallets is making individuals physical targets, blurring the line between cybersecurity and personal safety.

Businesses and other institutions are not exception. They are also facing a lot of attacks. In 2024 alone, $2.2 billion was stolen from crypto platforms through hacking incidents (Chainalysis, 2025, p.75). These attacks are often carried out by state-sponsored groups, such as those from North Korea, who use stolen funds to finance weapons programs. As Nkambule et al. (2025) note, organizations struggle to develop a robust cybersecurity frameworks to defend against such threats, which often exploit vulnerabilities in smart contracts or through the compromise of private keys.

Corporate and Institutional Risk

Beyond external threats from criminals, cryptocurrency and blockchain technology also introduce internal and institutional risks. Luo, Fang, Li, and Chen (2024) identify a form of "managerial opportunism," where companies may adopt blockchain technology not for its functional benefits but using to capitalize on market "hype." By announcing a pivot to blockchain, managers can potentially inflate their stock price and mask poor underlying performance, thereby increasing corporate default risk and misleading investors.

For legitimate organizations, they are also trying to protect their digital environment against these new threats is a difficult task. As explored by Nkambule, van Vuuren, and Leenen (2025), institutions face challenges in developing robust cybersecurity frameworks to protect sensitive data. With the rise of malware and phishing attacks that add another layer of complexity, it is

requiring a level of user knowledge and institutional awareness about the current digital criminal world, which as Mehta and Chawla (2024) note, is often lacking.

Conclusion

We cannot deny the benefits of cryptocurrency that brings to human society and solves many problems in traditional financial institutions. However, it also has their negative aspects in financial privacy and cybersecurity. We are already exploring blockchain technologies that provide users with pseudonymity and control over their financial data, and this also creates more opportunities for more illegal activities for criminals. We also discussed that these risks include not only those from individuals or groups but also from companies/organizations that use cryptocurrencies for illegal activities. It requires more development of robust institutional cybersecurity frameworks and enhanced digital knowledge for all users. Without acknowledging and having a proactive solution for these problems, we risk allowing the transformative potential of cryptocurrency to be overshadowed by the threats that cybercrime poses.

References

Alnıpak, S., & Toraman, Y. (2024). Analysing the intention to use blockchain technology in payment transactions of Turkish maritime industry. *Quality and Quantity*, 58(3), 2103-2123. https://doi.org/10.1007/s11135-023-01735-3

This article explores the potential benefits that blockchain adoption within the complex maritime industry. Using a Technology Acceptance Model (TAM) framework. The authors survey industry professionals in Turkey to gauge their intention to use blockchain for payment transactions. This article highlights the benefits of blockchain technology for payment transactions. However, this technology is still not relevant for non-technical users, and it requires some knowledge in digital technologies.

Burrell, D. N. (2025). Mental health impacts of cybercrime. Reading: *Academic Conferences International Limited*. Retrieved from http://mutex.gmu.edu/login?url=https://www.proquest.com/conference-papers-proceedings/mental-health-impacts-cybercrime/docview/3202190860/se-2

This paper is important to my research because it helps me understand more from the cybercrimes perspective, including how they are using cryptocurrency as their primary tool for perpetrating large-scale financial fraud. The paper also explores cybersecurity aspects, like how cybercriminals use psychology when employing social engineering tactics on their targets. The authors research details how cryptocurrency serves as the primary tool for large scale financial frauds due to its anonymity and the difficulty of recovery. This source providing a powerful example of how its technological features are weaponized that affect human.

Chainalysis. (2025, February). *The 2025 crypto crime report*. https://www.chainalysis.com/reports/2025-crypto-crime-report/

This annual industry report from a leading blockchain analysis firm provides extensive data and analysis on the use of cryptocurrency in illicit activities. The report details trends in scams, ransomware, money laundering, and organized crime, quantifying the monetary value and identifying the primary methods criminals use. It uses on-chain data to trace the flow of illicit funds, offering an evidence-based overview of the professionalization of the crypto crime landscape, including the use of AI and the rise in physical violence. This source provides concrete statistics and real-world case studies to substantiate claims about the scale and nature of illegal activities. It serves as a credible, data-driven source that grounds the paper's theoretical discussion in current, empirical evidence.

Luo, Y., Fang, M., Li, A., & Chen, S. (2024). Opportunity or opportunism? Blockchain technology adoption and corporate default risk. *Humanities & Social Sciences Communications*, 11(1), 1360. https://doi.org/10.1057/s41599-024-03727-6

This scholarly article investigates the internal corporate risks associated with the adoption of blockchain technology. The authors argue that some companies engage in "managerial opportunism," adopting blockchain not for its functional benefits but to capitalize on market hype, mislead investors, and mask poor performance. Their analysis shows that such strategic disclosures can actually increase a company's default risk. This source is vital for expanding the paper's scope beyond external criminal threats to include internal, corporate-level risks. It demonstrates that the challenges of cryptocurrency are not just about illegal usage but also about how the technology can be misused within legitimate but unethical corporate strategies.

Mehta, K., & Chawla, S. (2024). Illuminating the dark corners: A qualitative examination of cryptocurrency's risk. *Digital Policy, Regulation and Governance*, 26(2), 188-208. doi:https://doi.org/10.1108/DPRG-10-2023-0147

This scholarly journal paper provides a very good explanation that helps me to understand how Cryptocurrency technologies also have a dark side. It shows me how illegal activities around these digital asset technologies are very concerning. Also, with advanced technologies like Cryptocurrency, many regular users are at risk from this digital asset, so I think that everyone is still lacking knowledge of these technologies. Through in-dept interviews, the authors categorize the downsides into two main areas: barriers to legitimate adoption and direct illegal usage. This source provides the foundational structure for the paper's discussion on security challenges, distinguishing between usability issues and criminal exploitations.

Nkambule, M., van Vuuren, J. J., & Leenen, L. (2025). Identifying cybersecurity elements for a cybersecurity framework in higher education. Reading: *Academic Conferences International Limited*. Retrieved from http://mutex.gmu.edu/login?url=https://www.proquest.com/conference-papers-proceedings/identifying-cybersecurity-elements-framework/docview/3202190627/se-2

This conference paper details the challenges that complex organizations, specifically higher education institutions, face in creating robust cybersecurity frameworks. The authors discuss the need for a holistic approach that integrates governance, technical controls, and data protection systems to defend against a rising tide of cyber threats. While focused on academia, the paper's findings are broadly applicable to any large organization trying to protect sensitive data. This source is important for the "Corporate and Institutional Risk" section, as it provides a practical perspective on the defensive struggles of legitimate organizations. It highlights the resource-intensive nature of cybersecurity and underscores why the new threats posed by cryptocurrency are so difficult for many institutions to manage effectively.

Wang, H., & Hsieh, M. (2024). Cryptocurrency is new vogue: a reflection on money laundering prevention. *Security Journal*, 37(1), 25-46. https://doi.org/10.1057/s41284-023-00366-5

This article gives me a perspective on the cryptocurrency and money laundering, how cryptocurrency technologies provide anonymity, decentralization, and its contribution/impact to the use in illegal activities. The authors also discuss the challenges to anti-money laundering. The paper discusses the significant challenges these features pose to traditional anti-money laundering (AML) efforts. This source is fundamental to the paper's "Legal, Ethical, and Social Issues" section, providing a clear theoretical model to explain *why* cryptocurrency is so effective

for illicit use. Overall, this paper helps me understand how the technologies that affect financial privacy, and there are security challenges that cryptocurrencies present.

Appendix: Use of AI in the Research and Writing Process

I was using ChatGPT to help me brainstorm for my "The Role of Cryptocurrency in Financial Privacy and Cybersecurity. "Research paper.

The use of ChatGPT was integrated into several distinct phases of the writing process:

Phase 1: Initial Draft Review and Structural Refinement

Prompt/Task: The initial draft of the paper was presented to ChatGPT with a request for high-level feedback on its structure, argumentation, and academic tone.

AI Contribution: The AI provided feedback that helped me revised structure of the paper. It suggested strengthening the introduction with a clear, argumentative thesis statement and organizing the body of the paper into more distinct, thematic sections (e.g., Technology Overview, Legal/Ethical Issues, Security Aspects, and Corporate Risk). This moved the paper from a general overview to a more focused argument.

Phase 2: Source Integration and Synthesis

Prompt/Task: Using AI for quickly review of the sources

AI Contribution: It assisted in integrating the "money laundering triangle" framework from Wang and Hsieh (2024) into the "Legal, Ethical, and Social Issues" section.

It helped connect the concept of "pig butchering" from Burrell (2025) with the technological features of cryptocurrency described by other authors, strengthening the "Security Aspects and Challenges" section.

It assisted in positioning the arguments of Mehta & Chawla (2024) on "illegal usage" and Luo et al. (2024) on "managerial opportunism" as distinct but related facets of cryptocurrency risk.

This process involved transforming the author's understanding of the sources into fluid, integrated, and properly cited evidence within the paper's main argument.

Phase 3: Grammatical Correction and Tone Polishing

Prompt/Task: I requested to check my grammar issues.

AI Contribution: The AI performed a line-by-line review to correct grammatical errors, including subject-verb agreement, verb tenses, pluralization, and punctuation. It also helped shift the tone from being somewhat conversational