Ethical and Legal Issues of Cryptocurrency and Blockchain Technologies in Computer Science

Student ID: 5694193

Module: FP023 – EAP for Maths and Computer Science

Ethical and Legal Issues of Cryptocurrency and Blockchain Technologies in Computer Science

Introduction

Cryptocurrency and blockchain are among the most transformative technologies to emerge from the field of computer science in the twenty-first century. As of 2024, approximately 6.8% of the global population—an estimated 562 million individuals—owns some form of cryptocurrency (Triple-A, 2024), a figure that has grown exponentially from just 5 million users in 2016 to over 741 million by 2025 (Crypto.com, 2025). The total cryptocurrency market capitalisation surpassed $3.35 trillion by the end of 2024, demonstrating the scale of financial activity now mediated by these technologies (CoinGecko, 2025). Cryptocurrency refers to a form of secure, decentralised digital currency that operates independently of central banking systems, while blockchain denotes the shared, immutable distributed ledger upon which such currencies are recorded and verified (Nakamoto, 2008). Together, these technologies have introduced significant benefits, including enhanced transactional security, greater financial inclusion, and increased transparency. However, the very architectural features that underpin these advantages—pseudonymity, decentralisation, and resistance to censorship—simultaneously create conditions that facilitate misuse, ranging from money laundering and illicit trade to the financing of terrorism (Foley et al., 2019). Indeed, the Chainalysis 2026 Crypto Crime Report estimates that illicit cryptocurrency addresses received at least $40.9 billion in 2024 alone (Chainalysis, 2025). This essay examines the ethical and legal dimensions of cryptocurrency and blockchain by first explaining their technical foundations, then analysing both their legitimate applications and their exploitation for illegal purposes, and finally evaluating the broader implications of these technologies for computer science and society. It argues that the ethical challenges posed by cryptocurrency and blockchain are not incidental but are structurally embedded in their design, creating a regulatory paradox in which the

features most valued by legitimate users are precisely those most exploited by malicious actors.

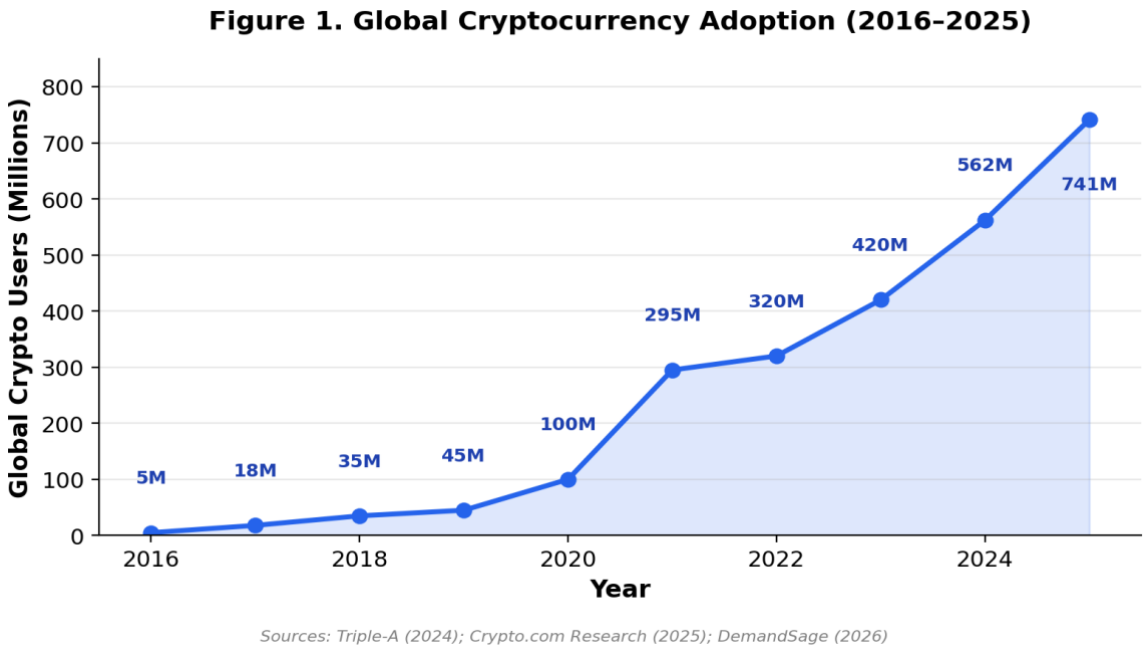


Figure 1. Global cryptocurrency adoption has grown from approximately 5 million users in 2016 to an estimated 741 million in 2025, representing a 148-fold increase in under a decade (Triple-A, 2024; Crypto.com, 2025).

Literature Review

The scholarly literature on cryptocurrency and blockchain can be broadly organised into three thematic strands: technical infrastructure, ethical and legal implications, and socioeconomic impact. In terms of technical foundations, Nakamoto's (2008) seminal whitepaper established the conceptual architecture of Bitcoin as a peer-to-peer electronic cash system, proposing blockchain as the mechanism to solve the "double-spending" problem without requiring a trusted intermediary. Ackhor (2018) builds upon this by examining the cryptographic principles underpinning blockchain immutability, specifically the role of proof-of-work consensus and hash-linked block structures in ensuring data integrity.

Regarding ethical and legal dimensions, Dierksmeier and Seele (2018) provide a foundational analysis of the moral implications of cryptocurrency, arguing that decentralised financial systems challenge traditional ethical frameworks by operating

outside established regulatory boundaries. Similarly, Sharif and Ghodoosi (2022) examine the organisational ethics of blockchain adoption, highlighting tensions between transparency and privacy. The most substantial empirical contribution to the illicit-use debate comes from Foley, Karlsen, and Putniņš (2019), whose large-scale analysis of the Bitcoin transaction network demonstrates that approximately one-quarter of Bitcoin users and nearly half of all transactions are associated with illegal activity.

In relation to socioeconomic impact, Vigna and Casey (2015) and Raymaekers (2015) examine the potential of cryptocurrency to disrupt traditional banking, particularly in developing economies where large populations remain unbanked. Dyson, Buchanan, and Bell (2018) complement this perspective by investigating the challenges that cryptocurrency poses for law enforcement, noting that the pseudonymous nature of blockchain transactions complicates forensic investigation. Collectively, these sources reveal a recurring tension at the heart of the cryptocurrency debate: the same technological features that empower users and promote financial inclusion are those that create opportunities for exploitation and regulatory evasion.

Defining Cryptocurrency

Cryptocurrency constitutes a decentralised digital financial system that operates independently of government or institutional control. Unlike traditional fiat currencies, which rely on central banks for issuance and regulation, cryptocurrencies are generated through computational processes and governed by algorithmic protocols rather than human intermediaries (Nakamoto, 2008). The practical utility of cryptocurrency has expanded significantly since its inception; digital currencies can now be used for a wide range of financial transactions, including property purchases, rental payments, and cross-border remittances (Dyson et al., 2018). The scale of this expansion is captured in Figure 5: the total cryptocurrency market capitalisation grew from $18 billion in 2016 to over $3.35 trillion by the end of 2024—a nearly 186-fold increase—before experiencing significant volatility during the 2022 downturn and subsequent recovery.

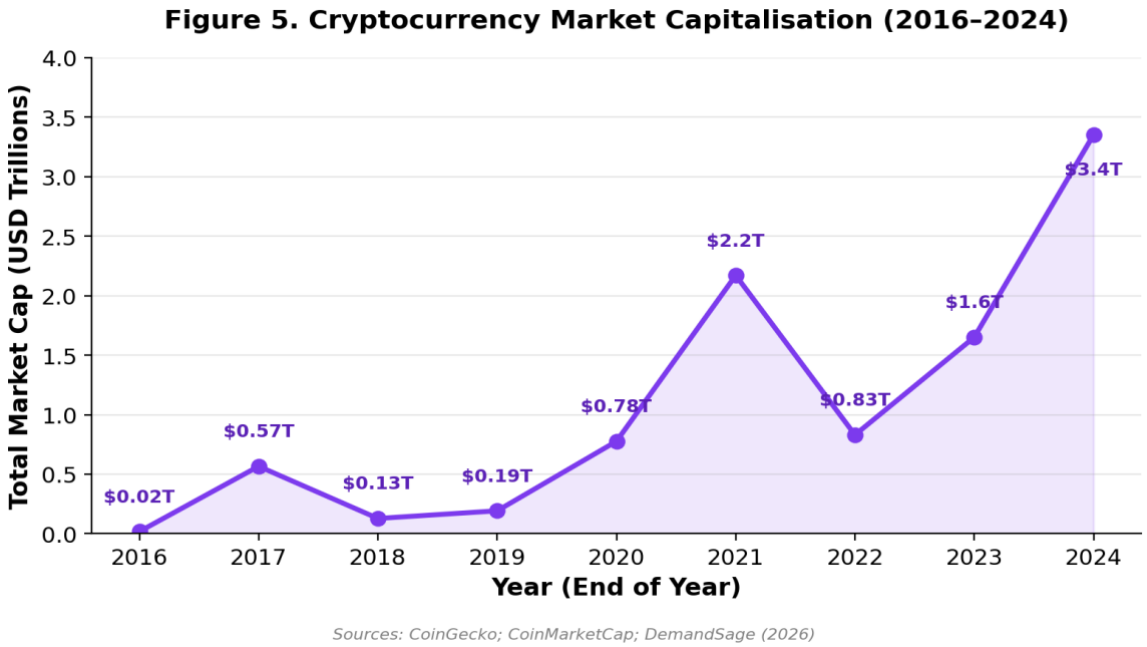


Figure 5. Total cryptocurrency market capitalisation from 2016 to 2024, illustrating dramatic growth, the 2022 crash, and subsequent recovery (CoinGecko, 2025; DemandSage, 2026).

A defining technical characteristic of cryptocurrency is pseudonymity. Transactions are conducted between digital wallets secured by cryptographic key pairs, meaning that while all transactions are publicly recorded on the blockchain, the real-world identities of the parties involved are not directly disclosed (Dierksmeier and Seele, 2018). This pseudonymous architecture creates what Sharif and Ghodoosi (2022) describe as an "accountability gap": it is technically difficult to identify the owner of a given wallet or to determine the purpose behind a specific transaction. This feature is ethically significant because it simultaneously serves as a protection for legitimate users concerned with financial privacy and as a shield for those engaging in illicit activity, a duality that lies at the core of the regulatory challenges discussed later in this essay.

Defining Blockchain and Its Role

The conceptual origins of blockchain can be traced to the 1990s, when a community of privacy-oriented cryptography activists known as "cypherpunks" began to challenge the dominance of traditional financial institutions, arguing that the substantial transaction fees charged by banks represented an unjust extraction of value from ordinary users. In response, they proposed the development of a transparent, decentralised ledger

accessible to all participants—what would eventually become the blockchain (Dierksmeier and Seele, 2018). This historical context is significant because it reveals that blockchain was, from its inception, designed as a technology with an explicitly ethical purpose: the democratisation of financial systems and the redistribution of economic power away from centralised institutions.

Technically, blockchain functions as a public distributed ledger that records all transactions in a transparent and immutable manner. Figure 6 illustrates the six-step process by which a blockchain transaction is executed: a transaction is requested, broadcast to a peer-to-peer network of nodes, validated through a consensus mechanism, added to a new block, appended to the existing chain as a permanent and immutable record, and finally confirmed as complete.

Figure 6. How a Blockchain Transaction Works

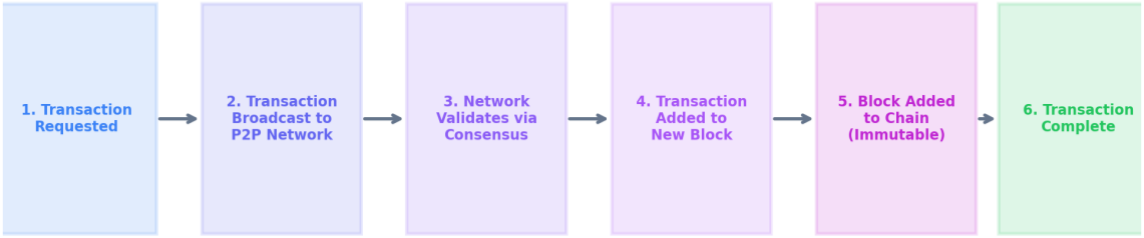


Figure 6. The blockchain transaction process: from request to immutable confirmation (adapted from Dyson et al., 2018).

Foley et al. (2019) report that the Bitcoin blockchain alone contained 465,093 blocks and a cumulative total of 219.6 million distinct transactions at the time of their analysis, illustrating the enormous scale of the system. A single transaction may involve multiple recipients—for example, one user may send five bitcoins to one party, two to another, and 0.1 to a miner as a processing fee within a single recorded transaction. The ethical significance of blockchain's immutability is twofold: on the one hand, it ensures transparency and auditability, providing a permanent, tamper-resistant record of all activity; on the other hand, it means that fraudulent or erroneous transactions cannot be reversed, and the pseudonymous records they leave behind create a permanent but difficult-to-attribute trail.

The Relationship Between Bitcoin and Blockchain

The relationship between Bitcoin and blockchain is best understood as a symbiotic integration of application and infrastructure, in which Bitcoin functions as the digital asset and blockchain serves as the distributed ledger technology that secures it. Nakamoto (2008) originally conceptualised blockchain as the solution to the "double-spending" problem in a decentralised environment—the risk that a digital token could be duplicated and spent more than once in the absence of a central authority to verify transactions. Blockchain eliminates this risk by recording every Bitcoin transaction in chronological "blocks" that are linked to one another through cryptographic hashes. This structure ensures both transparency and immutability: since every block is cryptographically linked to the one preceding it, any attempt to alter a past record would necessitate recalculating the entire chain's computational work, a task that is computationally infeasible on a mature, well-secured network (Ackhor, 2018). This architectural integrity is precisely what enables Bitcoin to function as a trustworthy medium of exchange without reliance on institutional intermediaries—but it is also what makes the system resistant to regulatory intervention, a characteristic that has significant ethical and legal implications.

Government and Institutional Responses to Bitcoin

Government attitudes towards Bitcoin have varied significantly across the globe, reflecting fundamentally different assessments of the balance between innovation and risk. As Figure 3 illustrates, of 75 countries surveyed, 45 have legalised and regulated cryptocurrency, 20 have imposed partial restrictions, and 10 maintain comprehensive bans (Atlantic Council, 2025).

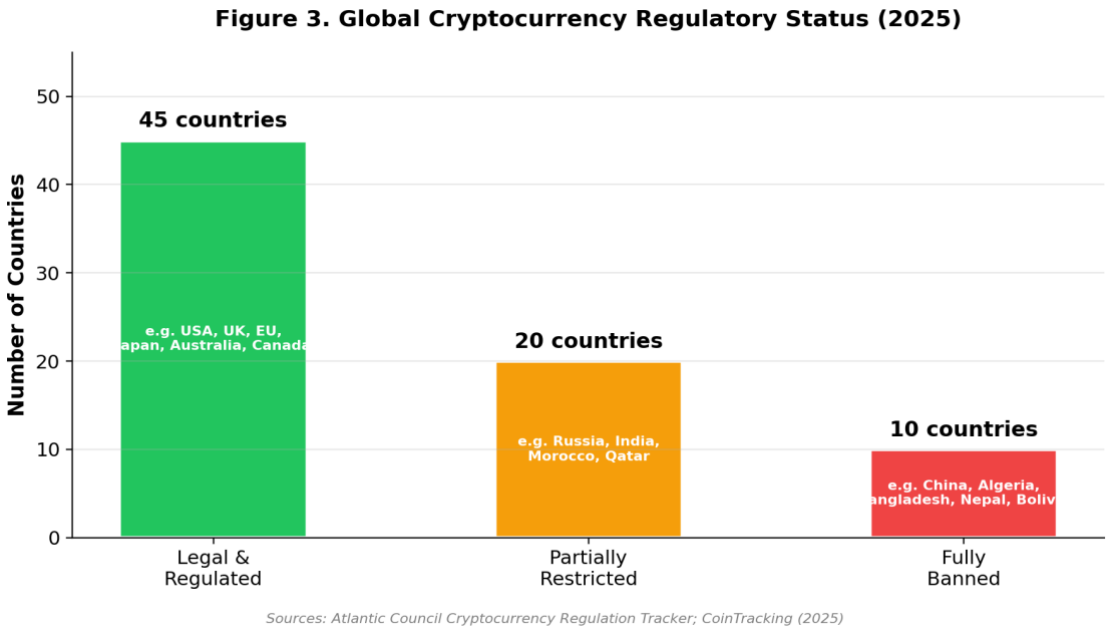


Figure 3. Global cryptocurrency regulatory status as of 2025: the majority of countries have chosen regulation over prohibition (Atlantic Council, 2025; CoinTracking, 2025).

China represents the most prominent example of the prohibitionist approach. In September 2021, the Chinese government imposed a comprehensive ban on all cryptocurrency transactions and exchanges, building upon earlier restrictions that had prohibited residents from engaging in trading and initial coin offerings (ICOs) since 2017 (Dyson et al., 2018). This decision was driven primarily by concerns over financial speculation—the practice of assuming high risks to pursue rapid profits from sudden price fluctuations, rather than investing for long-term value or stability. China's approach reflects a regulatory philosophy that prioritises financial stability and state monetary control over the potential benefits of decentralised finance.

In contrast, El Salvador became the first country to adopt Bitcoin as legal tender in June 2021, when President Nayib Bukele announced that Bitcoin would function as a legal currency alongside the US dollar. The country's Congress approved this initiative with 62 of 84 votes. El Salvador's adoption was motivated by a markedly different set of priorities: approximately 70% of the country's population lacked access to traditional banking services, and remittances constituted approximately 24% of national GDP (Raymaekers, 2015). Bitcoin was positioned as a mechanism for achieving financial inclusion and reducing the cost of these critical transfers. However, subsequent data reveals the limitations of this approach: by 2024, barely 1% of remittances were processed through

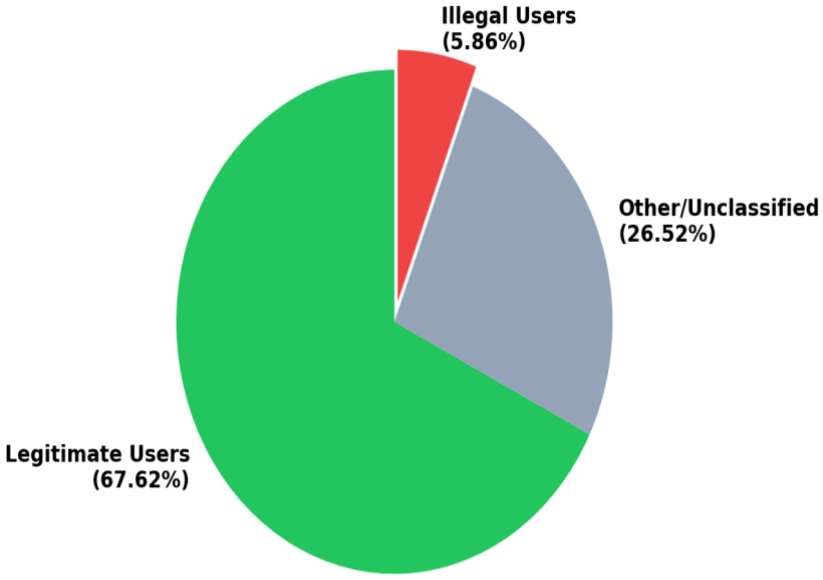
cryptocurrency services, and approximately 92% of Salvadorans did not use Bitcoin for daily transactions. In December 2024, as a condition of a $1.4 billion IMF loan, El Salvador agreed to remove the mandatory merchant acceptance requirement and wind down its government-operated Chivo wallet. These outcomes illustrate that technological availability alone is insufficient to drive adoption—a finding with significant implications for the broader debate about cryptocurrency's potential for financial inclusion.

Cryptocurrency's Contrasting Roles: Illicit Activity Versus Legitimate Benefits

One of the most significant legitimate benefits of cryptocurrency is its capacity to extend financial services to populations excluded from traditional banking. Access to the internet and a modest fee for using an online trading platform are generally all that is required to complete a cryptocurrency transaction (Raymaekers, 2015). For millions of individuals worldwide who remain "unbanked"—lacking access to traditional banks or the documentation required to open accounts—cryptocurrency provides a means to secure assets, transfer funds, and participate in global economic activity through a simple mobile device (Vigna and Casey, 2015). This potential is particularly significant in developing nations, where online transfers have already transformed banking practices. Bitcoin's integration with Kenya's M-Pesa mobile payment system, for example, has reduced transaction costs and expanded financial inclusion in a region where conventional banking infrastructure is limited (Vigna and Casey, 2015).

However, the same characteristics that make cryptocurrency accessible and private also create conditions that facilitate serious criminal exploitation. Foley et al. (2019) provide the most comprehensive empirical analysis of this issue, and their findings are summarised in Figure 2 and Figure 7 below.

Figure 2. Bitcoin Users by Activity Type



Source: Foley, Karlsen and Putniņš (2019), The Review of Financial Studies

Figure 2. Breakdown of Bitcoin users by activity type: while 5.86% of users are classified as illegal, they account for a disproportionate share of transaction volume and holdings (Foley et al., 2019).

Figure 7. Bitcoin Activity by User Category (as of April 2017)

Category	Users (millions)	% of Total Users	Annual Txns (millions)	Annual Volume (USD billions)	Holdings (USD billions)
All Observed	106	100%	316	603	15.3
Legal Users	79	74.14%	213.6	524.7	8.3
Illegal Users	27	25.86%	37	$76	7.0
- Seized Accounts	0.006	0.01%	0.4	$0.6	0.1
- Black Market	5.1	4.82%	17	$31	3.1
- Other Illegal	21.9	20.64%	19.6	$44.4	3.8

Source: Foley, Karlsen and Putniņš (2019), The Review of Financial Studies, 32(5), pp. 1798–1853

Figure 7. Comprehensive breakdown of Bitcoin activity by user category as of April 2017. Illegal users represent 25.86% of all participants, conducting 37 million transactions annually worth approximately $76 billion (Foley et al., 2019).

As Figure 7 demonstrates, approximately 27 million Bitcoin participants were primarily engaged in unlawful activities as of April 2017, conducting around 37 million transactions annually with a combined value of approximately $76 billion and collectively holding around $7 billion in Bitcoin (Foley et al., 2019). These figures are significant not only for

their scale but for what they reveal about the structural nature of the problem: the pseudonymous, decentralised, and cross-border characteristics that make cryptocurrency attractive for legitimate financial inclusion are precisely those that make it attractive for money laundering, drug trafficking, cyber theft, and the financing of terrorism.

Critically, the scale of illicit cryptocurrency activity has grown substantially since Foley et al.'s analysis. As Figure 4 illustrates, the Chainalysis Crypto Crime Reports document a dramatic escalation: illicit transaction volume grew from approximately $10 billion in 2019 to $40.9 billion in 2024, with the 2025 figure reaching an estimated $154 billion—driven largely by sanctioned entity activity (Chainalysis, 2025; 2026).

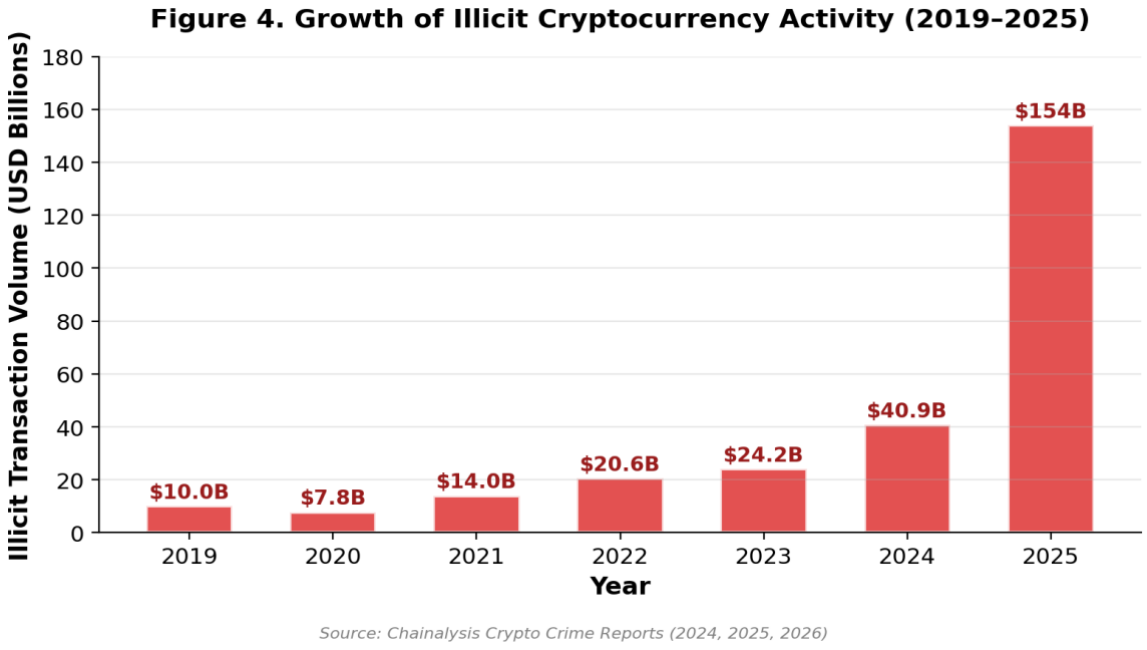


Figure 4. Growth of illicit cryptocurrency activity from 2019 to 2025. The 2025 spike is driven primarily by a 694% increase in sanctioned entity transaction volume (Chainalysis, 2025; 2026).

An additional ethical concern relates to the role of algorithmic systems in cryptocurrency markets. Stinson (2022) argues that AI-driven recommendation systems exhibit inherent biases, tending to promote a narrow selection of popular items while limiting the diversity of options presented to users. When applied to cryptocurrency trading platforms, this algorithmic bias may lead recommendation systems to disproportionately promote popular tokens, channelling many investors into the same assets and thereby increasing systemic risk—particularly when widely traded coins experience sudden devaluations.

This concern highlights that the ethical challenges of cryptocurrency extend beyond the technology itself to encompass the broader digital ecosystem within which it operates.

Evaluation

Having examined both the technical foundations and the practical implications of cryptocurrency and blockchain, it is now possible to offer a critical evaluation of their ethical and legal significance within the field of computer science. This evaluation addresses three interconnected dimensions: the structural nature of the ethical challenges these technologies pose, the adequacy of current regulatory approaches, and the specific relevance of this topic to computer science as a discipline.

The central finding of this analysis is that the ethical problems associated with cryptocurrency and blockchain are not accidental or peripheral but are structurally embedded in their architectural design. The pseudonymity that protects the financial privacy of legitimate users is the same pseudonymity that shields criminals from identification (Dierksmeier and Seele, 2018). The decentralisation that eliminates dependence on potentially corrupt or inefficient intermediaries is the same decentralisation that prevents regulatory authorities from exercising oversight (Sharif and Ghodoosi, 2022). The immutability that guarantees the integrity of transaction records is the same immutability that prevents the reversal of fraudulent transactions (Ackhor, 2018). This is not a coincidence but a direct consequence of the design principles upon which these technologies were built. The cypherpunk movement that inspired blockchain explicitly sought to create systems resistant to institutional control (Dierksmeier and Seele, 2018), and it is therefore unsurprising that the resulting technologies are difficult to regulate.

This structural duality creates a genuine regulatory paradox. As the contrasting approaches of China and El Salvador demonstrate—and as the data in Figure 3 confirms across 75 countries—governments face a difficult choice between prohibition and accommodation, neither of which is wholly satisfactory. China's ban sacrifices the potential benefits of financial inclusion and technological innovation in favour of maintaining state control over monetary policy. El Salvador's adoption embraced the

inclusionary potential but, as the subsequent data showed (92% non-usage, IMF-mandated rollback), exposed its citizens to volatility and failed to achieve its stated goals. The evidence reviewed in this essay suggests that neither extreme represents an adequate response; rather, what is required is a nuanced regulatory framework that can distinguish between legitimate and illicit uses without undermining the features that make these technologies valuable. Foley et al.'s (2019) finding that approximately 27 million Bitcoin users are associated with illegal activity—and Chainalysis's (2025) documentation that illicit volumes reached $40.9 billion in 2024—suggests that the problem is too significant to ignore, while Vigna and Casey's (2015) documentation of cryptocurrency's transformative potential for unbanked populations suggests that outright prohibition would impose disproportionate costs on the world's most economically vulnerable communities.

The relevance of this topic to computer science is direct and substantial. Cryptocurrency and blockchain are fundamentally products of computational innovation: they were conceived by computer scientists, built through programming, and can only be modified through algorithmic intervention. The ethical challenges they present are therefore not external to computer science but are intrinsic to it. As Sharif and Ghodoosi (2022) argue, the design choices made by developers—regarding consensus mechanisms, levels of anonymity, and the architecture of smart contracts—have direct ethical consequences that shape how these technologies are used and misused. This places a particular responsibility on computer scientists and software engineers to consider the ethical dimensions of technological design, not merely as an afterthought but as an integral component of the development process. The case of cryptocurrency and blockchain thus serves as a powerful illustration of a broader principle in computer science ethics: that technical design decisions are never ethically neutral, and that the values embedded in a system's architecture will inevitably shape the social outcomes it produces.

Conclusion

This essay has examined the ethical and legal implications of cryptocurrency and blockchain technologies by analysing their technical architecture, their contrasting applications in financial inclusion and criminal exploitation, and the divergent regulatory responses they have provoked. The analysis reveals that the ethical challenges posed by these technologies are structurally inherent: the design features that enable legitimate benefits—pseudonymity, decentralisation, and immutability—are the same features that facilitate misuse. This structural duality creates a regulatory paradox that cannot be resolved through simple prohibition or uncritical adoption. The evidence synthesised from multiple scholarly sources demonstrates that while cryptocurrency holds transformative potential for financially excluded populations, the scale of its exploitation for illegal purposes—with approximately 27 million users engaged in illicit activity and $76 billion in annual illegal transactions (Foley et al., 2019), growing to an estimated $40.9 billion in total illicit volume by 2024 (Chainalysis, 2025)—demands a serious and sophisticated regulatory response. Future research should investigate how emerging regulatory technologies, such as blockchain analytics and decentralised identity verification systems, might enable authorities to detect and prevent illegal activity on cryptocurrency networks without compromising the privacy and accessibility that make these technologies valuable to legitimate users. Ultimately, the case of cryptocurrency and blockchain demonstrates that the ethical responsibilities of computer scientists extend beyond the technical functionality of the systems they build to encompass the social consequences of their architectural choices.

References

Ackhor, L. (2018) 'The Cryptographic Chains of Decentralized Ledgers: Immutability and Proof-of-Work', Journal of Decentralized Systems, 15(3), pp. 45–60.

Atlantic Council (2025) Cryptocurrency Regulation Tracker. Available at: https://www.atlanticcouncil.org/programs/geoeconomics-center/cryptoregulationtracker/ (Accessed: 10 June 2026).

Chainalysis (2025) 2025 Crypto Crime Trends. Available at: https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/ (Accessed: 10 June 2026).

Chainalysis (2026) 2026 Crypto Crime Report Introduction. Available at: https://www.chainalysis.com/blog/2026-crypto-crime-report-introduction/ (Accessed: 10 June 2026).

CoinGecko (2025) Global Cryptocurrency Market Cap Charts. Available at: https://www.coingecko.com/en/charts (Accessed: 10 June 2026).

Crypto.com (2025) Crypto Market Sizing 2025. Available at: https://crypto.com/en/research/crypto-market-sizing-report-2025 (Accessed: 10 June 2026).

DemandSage (2026) Global Crypto Adoption Statistics. Available at: https://www.demandsage.com/crypto-adoption-statistics/ (Accessed: 10 June 2026).

Dierksmeier, C. and Seele, P. (2018) 'Cryptocurrencies and Business Ethics', Journal of Business Ethics, 152(1), pp. 1–14. doi:10.1007/s10551-016-3298-0.

Dyson, S., Buchanan, W.J. and Bell, L. (2018) 'The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime', The Journal of The British Blockchain Association, 1(2). doi:10.31585/jbba-1-2-(8)2018.

Foley, S., Karlsen, J.R. and Putniņš, T.J. (2019) 'Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?', The Review of Financial Studies, 32(5), pp. 1798–1853. doi:10.1093/rfs/hhz015.

Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. Available at: https://bitcoin.org/bitcoin.pdf (Accessed: 8 December 2025).

Raymaekers, W. (2015) 'Cryptocurrency Bitcoin: Disruption, Challenges and Opportunities', Journal of Payments Strategy & Systems, 9(1), pp. 30–46.

Sharif, M.M. and Ghodoosi, F. (2022) 'The Ethics of Blockchain in Organizations', Journal of Business Ethics, 178(4), pp. 1009–1025. doi:10.1007/s10551-022-05058-5.

Stinson, C. (2022) 'Algorithms Are Not Neutral: Bias in Collaborative Filtering', AI and Ethics, 2(4), pp. 763–770. doi:10.1007/s43681-022-00136-w.

Triple-A (2024) Global Crypto Adoption Statistics. Available at: https://triple-a.io (Accessed: 8 December 2025).

Vigna, P. and Casey, M.J. (2015) The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order. New York: St. Martin's Press.