Cryptocurrency and Blockchain Technology

Subjects: Criminology & Penology | Law | Computer Science, Software Engineering

Contributor: Casey Watters

Cryptocurrency has exploded in popularity, with Bitcoin adopted as a national currency in two countries. The blockchain technology on which cryptocurrency is built is an important tool used not only to facilitate a medium of exchange but also in many industries, including healthcare and education. As with all technologies, blockchain is a tool and can be abused by malicious actors. However, the decentralised nature of the technology creates an obstacle to establishing jurisdiction in transnational crimes.

cryptocurrency Bitcoin crime blockchain fraud jurisdiction public key private key

1. Introduction

For Bitcoin and most cryptocurrencies, the association with cybercrime and fraud is not due to a lack of transparency but rather the ease of use in international transactions, something that increases the complexity of establishing jurisdiction. While Bitcoin and many cryptocurrencies are on public ledgers, transferring money between banks and across borders creates barriers to identifying the criminals, as it takes time for law enforcement to obtain information from each bank, which may require time-consuming processes in each country, and banks may even be owned by criminal actors (Levi 2002). If banks in any jurisdiction stop cooperating, the trail is lost (Hedayati 2012). In order to truly remain anonymous, cybercriminals could use stolen identities to transfer funds and eventually withdraw the cash, making them nearly untraceable. However, selecting a specific currency is inefficient for those engaging in cybercrime. Human time is valuable while running code is low cost. As such, cybercriminals play a numbers game allowing code to attack any computer with identified vulnerabilities or assume the identities of anyone whose information has become available, often through phishing attacks (Ghazi-Tehrani and Pontell 2021). Insisting on bank transfers in dollars would make sense in the US; however, if the victim's computer is located in Poland or China, a request to transfer dollars to a US bank account may pose a greater challenge and prevent the criminals from receiving some of the funds. As cryptocurrency is jurisdiction-non-specific, cybercriminals can establish a single demand message for a virus that can harm systems globally. Due to the global nature of cryptocurrency, which uses a distributed ledger system, the appropriate jurisdiction for those involved in crypto-related crime is not always clear.

2. Background of Cryptocurrency and Blockchain Technology

Bitcoin and other cryptocurrencies are a form of distributed ledger that use blockchain to record transactions (Soltani et al. 2022; Pinto et al. 2022; Gorbunova et al. 2022). As a record of assets, ledgers are ordinarily kept by one centralised person or entity, requiring trust in that entity. For example, when someone opens a bank account, the bank does not store physical money for the customer but rather maintains a ledger tracking how much money to which the customer is entitled. As a highly regulated sector, people trust that banks will maintain accurate ledgers instead of changing the amount in customer accounts (Cardona 2022). With cryptocurrencies, the ledger is stored across multiple nodes around the world and the blockchain functions to prevent improper changes to the record. The greater number of nodes and the greater the decentralisation, the more secure a cryptocurrency is. Startup projects may be susceptible to attack. However, Bitcoin has never been successfully hacked and, with around 15,000 full nodes, (Bailey and Warmke 2023) is a permissionless and trustless network. It is said to be permissionless in that anyone who holds Bitcoin can transfer it and create new wallets (like accounts) without the need for a bank or any other intermediary, and trustless in that the code is open source and the ledger is distributed so no one can make unauthorised changes to the ledger (Arote and Kuri 2022).

A new Bitcoin block is created approximately every 10 min, and the chain goes back to 2009, when Bitcoin was first created in response to irresponsible banking behavior causing the 2008 financial crisis (Aboura 2022). Although Bitcoin is good for international transfers, it is not ideal for most retail purchases due to the 10 min delay. As such, a second layer has been added, known as the lightning network (Divakaruni and Zimmerman 2023; Liu and Au 2022; van Dam and Kadir 2022). The lightning network facilitates nearly instant Bitcoin transactions at a fraction of a cent (Dylan LeClair 2022). In El Salvador, where Bitcoin was adopted as an official currency (Taylor 2022), the lightning network was used by the government to transfer Bitcoin to its citizens.

Bitcoin uses a distributed consensus mechanism commonly referred to as “mining” to confirm transactions and update the blockchain. Encrypted numbers with 64 digits act as digital fingerprints, called hashes, which are used to secure the system (Allenotor and Oyemade 2021). Miners use the hash from the previous block and try to calculate the next hash. This connection of the hashes is what creates the chain between blocks, preventing someone from altering the ledger (Wezza et al. 2022). Proof of work, where miners use large amounts of computing power to secure the blockchain, is a useful tool for securing the blockchain and has been proposed for other things, including preventing denial of service attacks on email servers (Soria Ruiz-Ogarrio 2022). However, it has been criticised for its high degree of energy consumption (Wendl et al. 2023), largely within the context of ESG (Rudd 2023). As such, many other projects have opted for a consensus mechanism called proof of stake. In proof of stake, holders of a cryptocurrency can “stake” their currency to give a validator the authority to confirm transactions (Ibañez and Rua 2023). The theory is that those who own the currency have a stake in ensuring the security and accuracy of the system. In some cryptocurrencies, the stakers will lose their staked currency if the validator where they stake misbehaves.

In order to transact on the blockchain, users have two items, a public key and a private key (Liu et al. 2017). The public key is like an email address on the blockchain, and others can use it to send cryptocurrency to that address. The private key is like a password and allows the user to send from any address to which they have the private key. Therefore, only the person with a private key can move funds on the blockchain. This both ensures the

security of the blockchain and means that if a user loses their private key, they lose access to their cryptocurrency. To simplify the process, digital wallets are used to store the private key and streamline transactions (Suratkar et al. 2020). These wallets are said to “hold” the cryptocurrency, but they only display the user’s account balance (which is public on the blockchain) and hold the private key. All cryptocurrency is on the decentralized blockchain, not on the wallet or any one device.

Aside from assets like Bitcoin that are meant as a permissionless and decentralised medium of exchange, digital assets can be divided into multiple asset classes, including:

1. Stable coins, which are pegged to the value of a specific asset, often the US dollar (Ante et al. 2023);

2. Governance tokens, which allow the holder to vote on decisions for a decentralised project (Fan et al. 2022; Makridis et al. 2023); and

3. Smart contract-capable digital assets, an important part of web3, can be used for a variety of purposes including securing patient records in healthcare (Aloini et al. 2023; Ghosh et al. 2023; Kaur et al. 2023; Wenhua et al. 2023) and increasing efficiency in the energy sector (Mololoth et al. 2023; Zanghi et al. 2023; Khezami et al. 2022).

Despite the many benefits of the technology, cryptocurrency has been criticised for energy usage1 (Truby 2018; Rudd 2023) and the perceived risk of money laundering (Mahalaxmi and Srinivas 2022; Sun et al. 2022; Anthony 2022b; Hossain 2023), fraud (Scharfman 2023b; Sanz-Bas et al. 2021), tax evasion (Mezquita et al. 2023; Noked 2018), and use in the drug trade (Mezquita et al. 2023). Some jurisdictions banned or heavily regulated cryptocurrencies while others have sought to embrace digital assets as a source of innovation (Novak 2020). To date, El Salvador (Alvarez et al. 2022; Analytica 2021; Kshetri 2022b; Sparkes 2022) and the Central African Republic (Katterbauer et al. 2022; Kshetri 2022a; Neti 2022) even adopted Bitcoin as legal tender within the countries. However, the Central African Republic later repealed its law.

Decentralised digital assets lack a clear regulatory framework in most countries. To address this and in response to Executive Order 14067, the US Department of Justice (DOJ) issued a report on crimes related to digital assets (DOJ 2022). In this report, the DOJ expresses concerns over the use of cryptocurrency in crimes including sanctions evasions. The report calls for greater cooperation, both internationally and between government departments, and discusses the current state of the law, which lacks a comprehensive regulatory framework specific to decentralised digital assets, but where enforcement actions have nevertheless been taken. In spite of the fact that the US does not recognise cryptocurrency as legal tender, 18 U.S.C. § 1960, which prohibits “unlicensed money transmitting businesses” has been held to apply to cryptocurrency transmitting businesses.

On the regulatory front, the Financial Action Task Force (FATF), a 39-member body that establishes standards aimed at preventing money laundering, identifying funds related to the illicit drug trade, and terrorist financing, issued its recommendations on regulating digital assets (FATF 2021; de Koker et al. 2022). The FATF adopts the terms “virtual assets” (VAs) and “virtual asset service providers” (VASPs) in their recommendations. As a

developing technology, whether something is considered a VASP under the recommendations may not always be clear. The focus of the recommendations is information collection and monitoring, with mandatory disclosure requirements, such as the ‘travel rule’ and information sharing central to these recommendations. Although the recommendations are not law, FATF recommendations set global standards that usually lead to broad adoption.

References

1. Levi, Michael. 2002. Money laundering and its regulation. The Annals of the American Academy of Political and Social Science 582: 181–94.
2. Hedayati, Ali. 2012. An analysis of identity theft: Motives, related frauds, techniques and prevention. Journal of Law and Conflict Resolution 4: 1–12.
3. Ghazi-Tehrani, Adam Kavon, and Henry N. Pontell. 2021. Phishing evolves: Analyzing the enduring cybercrime. Victims & Offenders 16: 316–42.
4. Soltani, Reza, Marzia Zaman, Rohit Joshi, and Srinivas Sampalli. 2022. Distributed Ledger Technologies and Their Applications: A Review. Applied Sciences 12: 7898.
5. Pinto, Filipe, Catarina Ferreira da Silva, and Sergio Moro. 2022. People-centered distributed ledger technology-IoT architectures: A systematic literature review. Telematics and Informatics 70: 101812.
6. Gorbunova, Maria, Pavel Masek, Mikhail Komarov, and Aleksandr Ometov. 2022. Distributed ledger technology: State-of-the-art and current challenges. Computer Science and Information Systems 19: 65–85.
7. Cardona, Mercedes. 2022. Lessons Learned: Andrew Gray. Journal of Financial Crises 4: 613–16.
8. Bailey, Andrew M., and Craig Warmke. 2023. Bitcoin is King. In Cryptocurrency: Concepts, Technology, and Issues. Edited by J. Liebowitz. London and New York: Taylor & Francis, pp. 175–97.
9. Arote, Prerna, and Joy Kuri. 2022. ZCC: Mitigating Double-spending Attacks in Micropayment Bitcoin Transactions. Paper presented at 2022 Fourth International Conference on Blockchain Computing and Applications (BCCA), San Antonio, TX, USA, September 5–7.
10. Aboura, Sofiane. 2022. A note on the Bitcoin and Fed Funds rate. Empirical Economics 63: 2577–603.
11. Divakaruni, Anantha, and Peter Zimmerman. 2023. The Lightning Network: Turning Bitcoin into Money. Finance Research Letters 52: 103480.

12. Liu, Mengling, and Man Ho Au. 2022. Practical Anonymous Multi-hop Locks for Lightning Network Compatible Payment Channel Networks. Paper presented at Network and System Security: 16th International Conference (NSS 2022), Denarau Island, Fiji, December 9–12.
13. van Dam, Gijs, and Rabiah Abdul Kadir. 2022. Hiding payments in lightning network with approximate differentially private payment channels. Computers & Security 115: 102623.
14. Dylan LeClair, Sam Rule. 2022. The State Of Lightning Network Adoption. Bitcoin Magazine, June 10.
15. Taylor, Luke. 2022. The World's First Bitcoin Republic. Amsterdam: Elsevier.
16. Allenotor, David, and D. A. Oyemade. 2021. An Optimized Parallel Hybrid Architecture for Cryptocurrency Mining. Available online: https://www.isteams.net/_files/ugd/185b0a_6f88b82981424f87850d11fea3f52e1b.pdf (accessed on 27 February 2023).
17. Wezza, May, M. M. El-Gayar, and Ahmed AboElfetoh. 2022. A Novel Model for Securing Seals Using Blockchain and Digital Signature Based on QR Codes. Available online: https://assets.researchsquare.com/files/rs-2031413/v1_covered.pdf?c=1662660250 (accessed on 27 February 2023).
18. Soria Ruiz-Ogarrio, Jorge Jesús. 2022. Mining Incentives in Proof-of-Work Blockchain Protocols. Helsinki: Publications of the Faculty of Social Sciences/Department of Political and Economic Studies, University of Helsinki.
19. Wendl, Moritz, My Hanh Doan, and Remmer Sassen. 2023. The environmental impact of cryptocurrencies using proof of work and proof of stake consensus algorithms: A systematic review. Journal of Environmental Management 326: 116530.
20. Rudd, Murray A. 2023. 100 Important Questions about Bitcoin's Energy Use and ESG Impacts. Challenges 14: 1. Available online: https://www.mdpi.com/2078-1547/14/1/1 (accessed on 27 February 2023).
21. Ibañez, Juan Ignacio, and Francisco Rua. 2023. The Energy Consumption of Proof-of-Stake Systems: A Replication and Expansion. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4324137 (accessed on 27 February 2023).
22. Liu, Yi, Ruilin Li, Xingtong Liu, Jian Wang, Lei Zhang, Chaojing Tang, and Hongyan Kang. 2017. An efficient method to enhance Bitcoin wallet security. Paper presented at 2017 11th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID), Xiamen, China, October 27–29.
23. Suratkar, Saurabh, Mahesh Shirole, and Sunil Bhirud. 2020. Cryptocurrency wallet: A review. Paper presented at 2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP), Chennai, India, September 28–29.

24. Ante, Lennart, Ingo Fiedler, Jan Marius Willruth, and Fred Steinmetz. 2023. A Systematic Literature Review of Empirical Research on Stablecoins. FinTech 2: 34–47. Available online: https://www.mdpi.com/2674-1032/2/1/3 (accessed on 27 February 2023).
25. Fan, Sizheng, Tian Min, Xiao Wu, and Cai Wei. 2022. Towards understanding governance tokens in liquidity mining: A case study of decentralized exchanges. World Wide Web, 1–20.
26. Makridis, Christos A., Michael Fröwis, Kiran Sridhar, and Rainer Böhme. 2023. The rise of decentralized cryptocurrency exchanges: Evaluating the role of airdrops and governance tokens. Journal of Corporate Finance 79: 102358.
27. Aloini, Davide, Elisabetta Benevento, Alessandro Stefanini, and Pierluigi Zerbino. 2023. Transforming healthcare ecosystems through blockchain: Opportunities and capabilities for business process innovation. Technovation 119: 102557.
28. Ghosh, Pranto Kumar, Arindom Chakraborty, Mehedi Hasan, Khalid Rashid, and Abdul Hasib Siddique. 2023. Blockchain Application in Healthcare Systems: A Review. Systems 11: 38.
29. Kaur, Arpneek, Sandhya Bansal, and Vishal Dattana. 2023. Blockchain in Healthcare: A Systematic Review and Future Perspectives. In Deep Learning for Healthcare Decision Making. London: Routledge.
30. Wenhua, Zhang, Faizan Qamar, Taj-Aldeen Naser Abdali, Rosilah Hassan, Syed Talib Abbas Jafri, and Quang Ngoc Nguyen. 2023. Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends. Electronics 12: 546.
31. Mololoth, Vidya Krishnan, Saguna Saguna, and Christer Åhlund. 2023. Blockchain and Machine Learning for Future Smart Grids: A Review. Energies 16: 528.
32. Zanghi, Eric, Milton Brown Do Coutto Filho, and Julio Cesar Stacchini de Souza. 2023. Collaborative smart energy metering system inspired by blockchain technology. International Journal of Innovation Science.
33. Khezami, Nadhira, Nourcherif Gharbi, Bilel Neji, and Naceur Benhadj Braiek. 2022. Blockchain Technology Implementation in the Energy Sector: Comprehensive Literature Review and Mapping. Sustainability 14: 15826. Available online: https://www.mdpi.com/2071-1050/14/23/15826 (accessed on 27 February 2023).
34. Truby, Jon. 2018. Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies. Energy Research & Social Science 44: 399–410.
35. Mahalaxmi, G., and T. Aditya Sai Srinivas. 2022. Data Analysis with Blockchain Technology: A Review. IUP Journal of Information Technology 18: 7–23.

36. Sun, Nigang, Yuanyi Zhang, and Yining Liu. 2022. A Privacy-Preserving KYC-Compliant Identity Scheme for Accounts on All Public Blockchains. Sustainability 14: 14584.
37. Anthony, Nicholas. 2022b. Warren Targets Financial Privacy in Wake of FTX Fall. Available online: https://www.cato.org/blog/warren-targets-financial-privacy-wake-ftx-fall (accessed on 27 February 2023).
38. Hossain, Mohammad Belayet. 2023. Acquiring an awareness of the latest regulatory developments concerning digital assets and anti-money laundering. Journal of Money Laundering Control.
39. Scharfman, Jason. 2023b. The Cryptocurrency and Digital Asset Fraud Casebook. Cham: Springer Nature.
40. Sanz-Bas, David, Carlos del Rosal, Sergio Luis Náñez Alonso, and Miguel Ángel Echarte Fernández. 2021. Cryptocurrencies and Fraudulent Transactions: Risks, Practices, and Legislation for Their Prevention in Europe and Spain. Laws 10: 57. Available online: https://www.mdpi.com/2075-471X/10/3/57 (accessed on 27 February 2023).
41. Mezquita, Yeray, Dévika Pérez, Alfonso González-Briones, and Javier Prieto. 2023. Cryptocurrencies, Survey on Legal Frameworks and Regulation Around the World. Paper presented at International Congress on Blockchain and Applications, Guimaraes, Portugal, July 12–14.
42. Noked, Noam. 2018. Tax Evasion and Incomplete Tax Transparency. Laws 7: 31. Available online: https://www.mdpi.com/2075-471X/7/3/31 (accessed on 27 February 2023).
43. Novak, Mikayla. 2020. Crypto-friendliness: Understanding blockchain public policy. Journal of Entrepreneurship and Public Policy 9: 165–84.
44. Alvarez, Fernando E., David Argente, and Diana Van Patten. 2022. Are Cryptocurrencies Currencies? Bitcoin as Legal Tender in El Salvador. Cambridge: National Bureau of Economic Research.
45. Analytica, Oxford. 2021. El Salvador bitcoin experiment comes with risks. Expert Briefings, July 12.
46. Kshetri, Nir. 2022b. El Salvador’s bitcoin gamble. Computer 55: 85–89.
47. Sparkes, Matthew. 2022. El Salvador Revamps Bitcoin System. Amsterdam: Elsevier.
48. Katterbauer, Klemens, Hassan Syed, and Laurent Cleenewerck. 2022. The impact of the legalization of Bitcoin in the Central African Republic—A legal analysis. Cuadernos de Economía 713: 746.
49. Kshetri, Nir. 2022a. Bitcoin’s Adoption as Legal Tender: A Tale of Two Developing Countries. IT Professional 24: 12–15.

50. Neti, Lavanya V. 2022. Exploring the Implications of Cryptocurrencies in Selected Developing Countries. Working Paper, University of Pennsylvania Scholarly Commons. Available online: https://repository.upenn.edu/cgi/viewcontent.cgi?article=1044&context=spur (accessed on 27 February 2023).
51. DOJ. 2022. The Report of the Attorney General Pursuant to Section 8(b)(iv) of Executive Order 14067; Washington, DC: U.S. Department of Justice.
52. FATF, ed. 2021. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Paris: FATF.
53. de Koker, Louis, Talha Ocal, and Pompeu Casanovas. 2022. Where's Wally? FATF, virtual asset service providers, and the regulatory jurisdictional challenge. In Financial Technology and the Law: Combating Financial Crime. Edited by Doron Goldbarsht and Louis De Koker. Cham: Springer Nature, pp. 151–83.