Asian Journal of Law and Policy

Vol 4 No 1 (January 2024) eISSN: 2785-8979

Security Challenges in the Application of Blockchain Technology in Energy Trading

Karisma Karisma
Tunku Abdul Rahman University of Management and Technology, Malaysia
and
Faculty of Law, University of Malaya, Malaysia
karisma@tarc.edu.my
ORCID iD: 0000-0001-9783-9504
(Corresponding author)

ABSTRACT

This paper examines the interplay between blockchain technology and the energy sector, focusing on security limits, barriers, and challenges. The authors discusses the primary components of cyber risks, including threats, vulnerabilities, and impacts that plague blockchain systems and their application, network, and data layers. Further, anonymity is a key feature of blockchain, ensuring that blockchain users, nodes, and miners remain unidentifiable by any measure. Therefore, perpetrator-focused measures are not viable when assigning responsibility for dangerous and illegal conduct. There are concerns that the concealment of identity will broaden blockchain attack surfaces and pose risks to energy security. The authors also emphasises the need for a well-defined and consistent legal and regulatory framework to address the complexities of blockchain development in the energy sector and assert that the maturity of blockchain in this industry will depend on balancing security and user rights and suggest implementing ex-ante and ex-post measures. This paper is novel; the author seeks to provide an in-depth analysis of the security challenges faced by blockchain-based energy applications and offer practical solutions for mitigating these cybersecurity threats and vulnerabilities.

Keywords: Blockchain; Security challenges; Regulations; Energy security; Cyberattacks

Received: 4 Jan 2023, **Accepted:** 27 Apr 2023, **Published:** 31 Jan 2024

(2024) 1 Asian Journal of Law and Policy 51–75
https://doi.org/10.33093/ajlp.2024.3

Published by MMU Press. URL: https://journals.mmupress.com/ajlp

1. Introduction

Blockchain technology ('blockchain' unless specifically referred to) has taken centre stage in major industries at the dawn of a new era of digitalisation and revolution. Blockchain is gaining traction in different sectors, namely financial services, supply chains, manufacturing, energy, and telecommunications. Renewable energy generations, installations and infrastructures could be integrated with blockchain systems to optimize the development of decentralised and distributed energy systems and augment digitalisation.[1] Adopting digital technologies within the energy domain can drive new business models and facilitate a swift transition towards an era of the energy revolution. Many pioneer countries are involved in blockchain development with meritorious functionality of the technological application within the energy sector. The advent of blockchain-enabled energy initiatives and surging investments in blockchain-enabled platforms within these countries ensues from more favourable economic and technological landscapes.[2] These constitute vigorous impetuses towards systemic transitions from conventional energy systems to blockchain-enabled energy systems. On an organisational front, the domestication of blockchain and the emergence of new blockchain-based business models in these countries are prompting individuals and communities to attain greater control over their energy consumption and production.

Several countries have successfully mobilised or leveraged blockchain-enabled energy trading applications or are actively adopting such means. The United Kingdom (UK), Estonia, and Denmark are engaged in many business start-ups in Northern Europe. For instance, Electron is one of the many energy start-ups in the UK that uses blockchain-based platforms to allow prosumers and consumers to participate in local energy markets by enabling distributed and decentralised energy trading.[3] Estonia's WePower, an energy trading platform, is leveraging blockchain systems to engender a revolutionary change within the industry by tokenising energy data and uploading the data on a blockchain-backed platform.[4] Western Europe, Switzerland, France, the Netherlands, and Germany are

[1] Ying Wu and others, 'Digitalization and Decentralization Driving Transactive Energy Internet: Key Technologies and Infrastructures' (2021) 126 International Journal of Electrical Power & Energy Systems 106593 <https://doi.org/10.1016/j.ijepes.2020.106593>.

[2] Merlinda Andoni and others, 'Blockchain Technology in the Energy Sector: A Systematic Review of Challenges and Opportunities' (2019) 100 Renewable and Sustainable Energy Reviews 143–174 <https://doi.org/10.1016/j.rser.2018.10.014>.

[3] Melvyn Weeks, 'The Evolution and Design of Digital Economies' (2018) <https://fetch.ai/blog/fetch-ai-economics-white-paper>; Beom Suk Lee and others, 'Blockchain Architectures for P2P Energy Trading between Neighbors' (International Conference on Information and Communication Technology Convergence (ICTC), Korea, 2019) 1013–1017 <https://doi.org/10.1109/ICTC46691.2019.8939856>; Vikash Kumar Saini and others, 'Proof of Work Consensus Based Peer to Peer Energy Trading in the Indian Residential Community' (2023) 16 Energies 1253 <https://doi.org/10.3390/en16031253>.

[4] Zhitao Guan and others, 'Achieving Efficient and Privacy-Preserving Energy Trading based on Blockchain and ABE in Smart Grid' (2021) 147 Journal of Parallel and Distributed Computing 34–45 <https://doi.org/10.1016/j.jpdc.2020.08.012>; Md Moniruzzaman, Abdulsalam Yassine and Rachid Benlamri, 'Blockchain and Metaverse For Peer-to-peer Energy Marketplace: Research Trends and Open Challenges'

well-positioned with start-ups and companies deploying blockchain systems in the energy trading landscape. Blockchain-enabled energy solutions such as online energy marketplaces, decentralised peer-to-peer and wholesale energy trading and deployment of distributed flexibility infrastructures are adopted widely in Germany, not limited to Conjoule, Wuppertal Stadtwerke (Tal Markt), and Ponton, with copious amounts of other entrepreneurial business models.[5] In the Netherlands, Alliander and Spectral Energy are developing blockchain-enabled peer-to-peer energy trading platforms, open and accessible to prosumers and consumers, to facilitate distributed and decentralised energy transactions and optimise energy management.[6] Vandebron, an online trading platform connecting renewable energy prosumers and consumers directly in renewable energy trading, enabling the formation of local energy communities, is investigating blockchain in energy marketplaces.[7] SunChain in France and Quartierstrom in Switzerland utilise blockchain-enabled applications to track, secure and certify energy exchanges and improve energy efficiency.[8] Energy trading platforms, such as Power Ledger in Australia, and Brooklyn Microgrid in the United States, adopt blockchain systems to facilitate energy trade by matching demand and supply and allow real-time transaction settlements between buyers and sellers of energy.[9] Energy transaction data are stored and shared with all peers on the

(IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD), Morocco, 2022) <10.1109/ICTMOD55867.2022.10041871>.

[5] Ariana Polyviou, Pantelis Velanas and John Soldatos, 'Blockchain Technology: Financial Sector Applications beyond Cryptocurrencies' (2019) 28 Proceedings 7 <https://doi.org/10.3390/proceedings2019028007>; Pornpit Wongthongtham and others, 'Blockchain-enabled Peer-to-Peer Energy Tading' (2021) 94 Computers & Electrical Engineering 107299 <https://doi.org/10.1016/j.compeleceng.2021.107299>; Mario Pichler and others, 'Decentralized Energy Networks based on Blockchain: Background, Overview and Concept Discussion' (Business Information Systems Workshops: BIS 2018 International Workshops, Germany, 2019) 244–257 <https://doi.org/10.1007/978-3-030-04849-5_22>; Moein Choobineh and others, 'Blockchain Technology in Energy Systems: A State-of-the-Art Review' (2023) 3 IET Blockchain 35–59 <https://doi.org/10.1049/blc2.12020>; Chathuri Lakshika Gunarathna and others, 'Reviewing Global Peer-to-Peer Distributed Renewable Energy Trading Projects' (2022) 89 Energy Research & Social Science 102655 <https://doi.org/10.1016/j.erss.2022.102655>; Yihao Guo, Zhiguo Wan and Xiuzhen Cheng, 'When Blockchain Meets Smart Grids: A Comprehensive Survey' (2022) 2 High-Confidence Computing 100059 <https://doi.org/10.1016/j.hcc.2022.100059>.

[6] Ayman Esmat and others, 'A Novel Decentralized Platform for Peer-to-Peer Energy Trading Market with Blockchain Technology' (2021) 282 Applied Energy 116123 <https://doi.org/10.1016/j.apenergy.2020.116123>; 'Spectral and Alliander Launch Blockchain Based Energy Token at de Ceuvel' (Spectral, 2022) <https://spectral.energy/spectral-and-alliander-launch-blockchain-based-energy-token-at-de-ceuvel/>.

[7] Esteban A Soto and others, 'Peer-to-Peer Energy Trading: A Review of the Literature' (2021) 283 Applied Energy 116268 <https://doi.org/10.1016/j.apenergy.2020.116268>.

[8] Xin Lu and Zhitao Guan, 'A Blockchain-based Trading Matching Scheme in Energy Internet' (BSCI 2020: Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure, Co-located with AsiaCCS 2020, Taiwan, 2020) 142–150 <https://doi.org/10.1145/3384943.3409430>; Loai Nasrat and others, 'Review on Energy Trading of Community-Based Projects Around the World' (23rd International Middle East Power Systems Conference (MEPCON), Egypt, 2022) <https://doi.org/10.1109/MEPCON55441.2022.10021688>; Sławomir Bielecki and others, 'Electricity Usage Settlement System Based on a Cryptocurrency Instrument' (2022) 15 Energies 7003 <https://doi.org/10.3390/en15197003>.

blockchain network to enable effective interaction with prosumers and consumers.[10] Considering many peers on energy trading platforms, A blockchain-based energy landscape is apt considering many peers on energy trading platforms[11] Recognising the prevailing limits, barriers, and technological and legal challenges in the blockchain-enabled energy trading domain. This article explores the security risks and challenges surrounding blockchain-enabled energy trading applications and shifts the readers' perspective on the lack of regulation to address blockchain cyberattacks. The article then examines ex-post and ex-ante mitigation measures to address cybersecurity issues.

As blockchain is still in its infancy, it is more vulnerable to security attacks by malicious nodes that conspire to launch an attack and deny service to other nodes, thus facing the risk of failures when deployed on critical infrastructures such as energy systems. Security threats disrupt blockchain performance by engaging in coordinated attacks, imitating honest nodes, and generating multiple malicious identities to tamper with data content. This article provides in-depth discussions on security challenges which could impede vast blockchain uptake in peer-to-peer energy trading applications.

2. A Taxonomy of Security Issues in Blockchain-Enabled Energy Trading Landscapes

Blockchain outperforms centralised systems in terms of efficacy since trading parties will have an updated record of all energy transactions in real-time, coupled with the elimination of third-party intermediaries and reduction in operational costs.[12] In light of implementing renewable energy systems to achieve net zero targets, blockchain is useful where there is extensive multiplication of energy trading records and heightened energy data volumes.[13] Further, centralised ledgers fail to attain data transparency and immutability requisite sufficiently.[14] Even though numerous academics hail the benefits of blockchain as a breakthrough technology, the workings of blockchain expose participants to cybersecurity

[9] Alexandra Schneiders and David Shipworth, 'Energy Cooperatives: A Missing Piece of the Peer-to-Peer Energy Regulation Puzzle?' (British Institute of Energy Economics, 2018) <https://www.biee.org/resources/energy-cooperatives-a-missing-piece-of-the-peer-to-peer-energy-regulation-puzzle/>.

[10] Oliver Dzobo and others, 'Proposed Framework for Blockchain Technology in a Decentralised Energy Network' (2021) 6 Protection Control of Modern Power Systems 31 <https://doi.org/10.1186/s41601-021-00209-8>.

[11] Tahereh Nodehi and others, 'EBDF: The Enterprise Blockchain Design Framework and its Application to an e-Procurement Ecosystem' (2022) 171 Computers & Industrial Engineering 108360 <https://doi.org/10.1016/j.cie.2022.108360>.

[12] Sidique Gawusu and others, 'Renewable Energy Sources from the Perspective of Blockchain Integration: From Theory to Application' (2022) 52 Sustainable Energy Technologies and Assessments 102108 <https://doi.org/10.1016/j.seta.2022.102108>; Bokolo Anthony Jnr, 'Distributed Ledger and Decentralised Technology Adoption for Smart Digital Transition in Collaborative Enterprise' (2021) 17 Enterprise Information Systems 465–498 <https://doi.org/10.1080/17517575.2021.1989494>; Raphael Moser and others, 'Solar Prosumers in the German Energy Transition: A Multi-Level Perspective Analysis of the German "Mieterstrom" Model' (2021) 14 Energies 1188 <https://doi.org/10.3390/en14041188>.

[13] Anthony Jnr (n 12).

risks. This section primarily focuses on the risks culminating from blockchain applications. Many cybersecurity attacks endanger blockchain systems, influencing the operation and stability of peer-to-peer energy trading and energy communities.

That said, a thorough understanding of the cyber risks on the blockchain fora is crucial to strengthen blockchain architecture in cyberspace. With the appreciation of potential weaknesses, developing defence strategies is possible. The first part is purposefully descriptive, as the author charts the security vulnerabilities and threats surrounding blockchain systems and highlights the qualitative and quantitative impact on critical infrastructures due to the lack of oversight and accountability. The second part explores challenges concerning the (a) attribution of responsibility and (b) ex-post and ex-ante responses to cyber-attacks.

2.1 Energy Security and Cyber-Attacks on Blockchain Landscapes

Energy security inextricably merges with the nation's decentralised power systems and energy policies. The heterogeneity and diversification of market actors and energy infrastructures are conducive to augmenting energy security. The proper functioning of institutional and governance regimes can ensure that relevant mitigation measures are in place to address the common threats posed by the functionalities of energy systems.

With the growing economy, we face increasing energy supply shortages and excessive resource exploitation. Decentralised and digitalised energy systems play a catalytic role in leveraging renewable energy, eliminating fossil fuel dependence, and enhancing energy efficiency and security. In blockchain systems, energy security and cyber-security hinge on one another due to the high reliability and fault tolerance compared to conventional energy systems.[15] Blockchain maintains data integrity and immutability across all nodes. Further, the absence of intermediaries eliminates the risks of a single point of failure. Blockchain also increases energy trading adoption rates with the active participation of prosumers in local energy markets.[16] While boundless opportunities advanced by blockchain embolden prosumers, there are copious amounts of cybersecurity issues that reduce connectivity and automation potential.

All nations attach high value to energy security. While blockchain technology promotes the availability, affordability, accessibility, and acceptability of energy, security concerns hinder energy provisions in a socially reasonable and responsible manner.[17] Attackers thwart

[14] Cristian Hurtado, 'A Feasibility Analysis of Transactive Energy Systems in Ontario' (Master's dissertation, York University 2019) <http://hdl.handle.net/10315/36863>.

[15] Jiabin Bao and others, 'A Survey of Blockchain Applications in the Energy Sector' (2020) 15 IEEE Systems Journal 3370 <https://doi.org/10.1109/JSYST.2020.2998791>.

[16] Moser and others (n 12); Anthony Jnr (n 12).

[17] Bernd Teufel, Anton Sentic and Mathias Barmet, 'Blockchain Energy: Blockchain in Future Energy Systems' (2019) 17 Journal of Electronic Science and Technology 100011 <https://doi.org/10.1016/j.jnlest.2020.100011>; Nallapaneni Manoj Kumar, 'Blockchain: Enabling Wide Range of Services in Distributed Energy System' (2018) 7 Beni-Suef University Journal of Basic and Applied Sciences 701–704

blockchain-enabled energy systems, disrupting energy production and supply and posing challenging economic issues.

Further, the heightened reliance on blockchain-enabled prosumer-centric activities triggers sophisticated cyber-attacks due to larger attack surfaces resulting in a malfunction of local energy markets. In this instance, the growing cyberattacks in blockchain systems embroil active customers in a conflict, given that engaging in peer-to-peer energy trading on decentralised systems is fraught with imperilment and jeopardy. Cyberattacks hamper the development of socially equitable and acceptable energy services and pose challenges toward universal electrification and sustainable supply. Denial of service attacks (DDoS) and 51% attacks, which are explained and discussed in detail below, are likely to significantly interrupt the energy supply, affecting the growth and performance of countries. Under the DDoS attack, the perpetrator engulfs the network or server with disruptive traffic flow and overloads the bandwidth, perpetuating a service disruption of any intensity.[18] While systems with a single point of failure are usually vulnerable to DDoS attacks, decentralised and distributed blockchain platforms are not entirely resistant to such attacks. In such instances, it is difficult to assess the likelihood of DDoS attacks on blockchain systems as blockchain implementation, design, and security measures embedded within the systems play a key role when assessing blockchain vulnerabilities to such attacks. DDoS attacks are performed on the application layer and can compromise the entire blockchain infrastructure, defeating any prospects of serving the genuine request of the network.[19] There are many real-world examples of DDoS attacks in blockchain landscapes. In May 2021, Polygon Network, a blockchain platform, was attacked, resulting in congestion, delay in processing time, and build-up of network traffic that overloaded the system.[20] Subsequently, in June 2021, Solana's network was the target of DDoS attacks causing network disruptions with malicious attackers flooding the system with high Internet traffic.[21] In April 2020, Binance Exchange suffered a DDoS attack where malicious attackers overloaded the servers resulting in delay and disruption of network performance.[22] Further, multiple DDoS attacks affected the Ethereum Network, Bitmex, a blockchain-based cryptocurrency exchange, causing system stability issues and potential revenue losses.[23]

<https://doi.org/10.1016/j.bjbas.2018.08.003>.

[18] Sharyar Wani and others, 'Distributed Denial of Service (DDoS) Mitigation Using Blockchain: A Comprehensive Insight' (2021) 13 Symmetry 227 <https://doi.org/10.3390/sym13020227>; Kanneganti Jahnavi, 'The Blockchain Technology and Attacks on It' (2021) 12 Turkish Journal of Computer and Mathematics Education 571–581 <https://doi.org/10.17762/turcomat.v12i13.8338>.

[19] Wani and others (n 18); Jahnavi (n 18).

[20] Andrew Thurman, 'Polygon Under Accidental Attack From Swarm of Sunflower Farmers' (*CoinDesk*, 2022) <https://www.coindesk.com/tech/2022/01/06/polygon-under-accidental-attack-from-swarm-of-sunflower-farmers/>.

[21] Alex Hulubas, 'Solana Network Goes Through Another DDoS Attack' (*Cryptorobin.com*, 2022) <https://cryptorobin.com/solana-network-goes-through-another-ddos-attack/>.

[22] Milka Trajcevski, 'Binance Suffered Series of DDoS Attacks' (*DailyCoin*, 2020) <https://dailycoin.com/binance-suffered-series-of-ddos-attacks/>.

As for the 51% attacks, it occurs when the attackers manage to obtain majority mining power or hash rate of 50% or more. In such instances, successful attackers can rewrite the transaction history, obstruct genuine mining operations, and block the confirmation of new transactions, leading to double spending issues, chain splitting, and revenue losses.[24] For example, in 2018 and 2019, malicious attackers executed 51% of attacks on Ethereum Classic and Monacoin, resulting in revenue losses.[25]

Although cybersecurity attacks are yet to manifest in blockchain-enabled energy trading landscapes, this does not guarantee that they will not happen in the future. Energy trading platforms are inherently vulnerable to security risks, disrupting and affecting the proper functioning of trading platforms, therefore, requiring increased security measures that keep in stride and protect these platforms from potential threats.

2.2 Blockchain Security Threats, Vulnerabilities, and Impact

While it is beyond the scope of this dissertation to generate comparatively detailed discussions on distinct cyber risk definitions observed by scholars and organizations, it is pertinent to espouse a workable and pragmatic definition from academic literature having appraised blockchain designs, use cases, and capabilities.[26] The United States National Institute of Standards and Technology defines risk as the (a) probability that a particular security threat will 'trigger' or 'exploit' system vulnerability and (b) resulting adverse impact on the occurrence of such circumstance or event on organisational operations and assets.[27] Similarly, the International Organisation for Standardisation and International Electrotechnical Commission defines information security risk as the likelihood of a threat exploiting system vulnerabilities, causing harm to an organization.[28] The author adopts this broad and encapsulating definition which comprises three elements, namely 'vulnerability', 'threat' and 'impact', which can be taken as a starting point to aid the reader's understanding of the author's trajectory.

[23] Sead Fadilpašić, 'BitMEX Explains the Attack to Doubting Customers; Refunds BTC 40' (*Cryptonews*, 2020) <https://cryptonews.com/news/bitmex-explains-the-attack-to-doubting-customers-refunds-btc-6048.htm>.

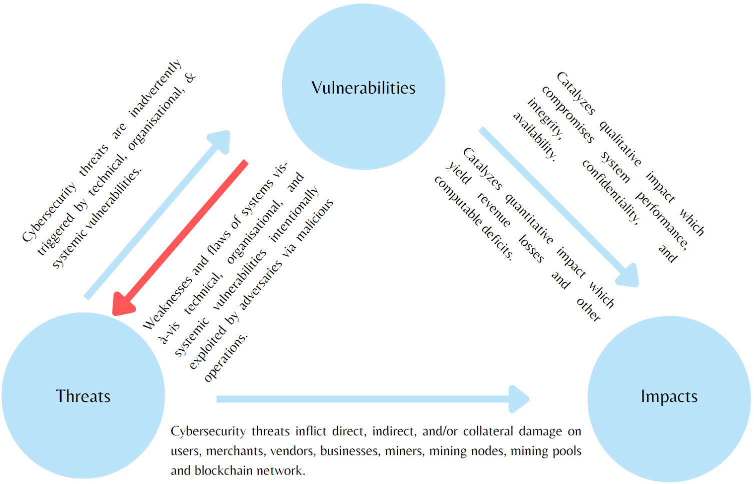
[24] Congcong Ye and others, 'Analysis of Security in Blockchain: Case Study in 51%-attack Detecting' (5th International conference on dependable systems and their applications (DSA), China, 2018) 15–24 <https://doi.org/10.1109/DSA.2018.00015>.

[25] Zack Voell, 'Ethereum Classic Hit by Third 51% Attack in a Month' (*CoinDesk*, 2020) <https://www.coindesk.com/markets/2020/08/29/ethereum-classic-hit-by-third-51-attack-in-a-month/>; Alyssa Hertig, 'Blockchain's Once-Feared 51% Attack Is Now Becoming Regular' (*CoinDesk*, 2018) <https://www.coindesk.com/markets/2018/06/08/blockchains-once-feared-51-attack-is-now-becoming-regular>.

[26] Cyber risk is defined by the Geneva Association as 'Any risk emerging from the use of information and communication technology that compromises the confidentiality, availability or integrity of data or services': Organisation for Economic Co-operation and Development, *Enhancing the Role of Insurance in Cyber Risk Management* (OECD Publishing 2017) <https://doi.org/10.1787/9789264282148-en>.

[27] National Institute of Standards and Technology, 'Computer Security Resource Centre' <https://csrc.nist.gov/glossary/term/risk>.

[28] ISO/IEC 27005:2011, 'ISO/IEC 27005:2011(en) Information Technology — Security Techniques — Information Security Risk Management' <https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-2:v1:en>.


Vulnerabilities
Cybersecurity threats are inadvertently triggered by technical, organisational, & systemic vulnerabilities.
Weaknesses and flaws of systems vis-à-vis technical, organisational, and systemic vulnerabilities intentionally exploited by adversaries via malicious operations.
Catalyzes qualitative impact which compromises system performance, integrity, confidentiality, and availability.
Catalyzes quantitative impact which yield revenue losses and other computable deficits.
Threats
Impacts
Cybersecurity threats inflict direct, indirect, and/or collateral damage on users, merchants, vendors, businesses, miners, mining nodes, mining pools and blockchain network.

Source: Author's own

2.3 Vulnerabilities

By design, blockchain represents a system inherently resistant to cybersecurity attacks. Considering blockchain systems' security vulnerabilities, academic literature has focused on fending off such attacks and upholding data integrity. Primary components under the umbrella of vulnerability are technical, organisational, and systemic:[29]

(a) 'Technical vulnerability' refers to generating undesired effects when blockchain infrastructures, hardware or software are susceptible to attacks vis-à-vis misconfiguration, defects in system design or implementation, security flaws in the code and weak cryptographic implementation, amongst others.[30]

(b) 'Organisational vulnerability' refers to the weakness in security and operation policies and practices, including but not limited to personnel and management factors vis-à-vis the acute shortage of blockchain developers, lack of elaborate skills, knowledge, and expertise in blockchain software development and the inability of organisations to scale up training of personnel.

(c) 'Systemic vulnerability' refers to linkages and mutually dependent connectivity among different systems and subsystems where the exposure of one system in peril spreads to other systems, resulting in widespread impact, thereby destabilising, and diminishing the exposed system(s).[31]

[29] Feja Lesniewska and others, 'In the Eye of a Storm: Governance of Emerging Technologies in UK Ports Post Brexit' (2019) Living in the Internet of Things 1 <https://doi.org/10.1049/cp.2019.0165>.

[30] ibid.

[31] Giada Limongi and Adriana Galderisi, 'Twenty years of European and International Research on Vulnerability: A Multi-faceted Concept for Better Dealing with Evolving Risk Landscapes' (2021) 63 International Journal of Disaster Risk Reduction 102451 <https://doi.org/10.1016/j.ijdrr.2021.102451>.

Blockchain architecture comprises the following layers, including but not limited to the Application, Network, and Data Layers. These layers are predisposed to security vulnerabilities. While some scholars attribute security vulnerabilities to technological and structural immaturity causing unanticipated catastrophic cyber-attacks, others ascribe the lacunae to the foundations of blockchain infrastructure itself, 'being built by people, people who are making decisions that will impact the operation and success of the new infrastructure'.[32] These high-stakes decisions are technical, policy, economic and risk assessments.[33] In a blockchain network, regarding developers with a 'position of power', the magnitude of their power varies with their corresponding role.[34] Key developers shape blockchain by testing and reviewing the codes and implementing policy and technical measures.

For example, a group of developers leveraged their 'position of power' in the 2016 Decentralised Autonomous Organisation (DAO) attack, also known as the reentrancy attack that impacted the entire Ethereum platform.[35] These actors aligned their interests to the detriment of their victims, who invested in the DAO by initiating a hard fork to recover $50 million of stolen funds.[36] In reversing the DAO attack, they set up salient terms in the blockchain domain through code to reflect and map collective values and policy and technical choices. This section assesses the vulnerabilities associated with the blockchain layers and the resulting problematic implications toward energy policy goals which could perversely exacerbate trust, compromising democratic participation in the energy market.

The Application layer forms the topmost layer of blockchain infrastructures, comprising decentralised applications (dApps), smart contracts, application program interfaces (APIs), and user interfaces.[37] It facilitates consumer interactions with existing systems as a vital blockchain component. Consumers can leverage the application layer to communicate with peers on energy networks and conduct efficient energy transactions. Despite tethering the Application layer to security and privacy features, it is susceptible to DAO, user wallet and blockchain network attacks, which undermine the resiliency and reliability of blockchain

[32] Angela Walch, 'In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains' in Philipp Hacker and others (eds), *Regulating Blockchain: Techno-Social and Legal Challenges* (Oxford University Press 2019) 58–82 <https://doi.org/10.1093/oso/9780198842187.003.0004>.

[33] ibid.

[34] ibid.

[35] The DAO (or reentrancy) attack allows the malicious attackers to draw out funds using the recursive call function. Noama Fatima Samreen and Manar H Alalfi, 'Reentrancy Vulnerability Identification in Ethereum Smart Contracts' (2020 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE), 2020) 22–29 <https://doi.org/10.1109/IWBOSE50093.2020.9050260>.

[36] Quinn DuPont, 'Experiments in Algorithmic Governance: A History and Ethnography of "The DAO," A Failed Decentralized Autonomous Organization' in Malcolm Campbell-Verduyn (ed), *Bitcoin and Beyond* (Routledge 2017) 157–177 <https://www.taylorfrancis.com/chapters/oa-edit/10.4324/9781315211909-8/experiments-algorithmic-governance-quinn-dupont>.

[37] Khizar Hameed and others, 'A Taxonomy Study on Securing Blockchain-based Industrial Applications: An Overview, Application Perspectives, Requirements, Attacks, Countermeasures, and Open Issues' (2022) 26 Journal of Industrial Information Integration 100312 <https://doi.org/10.1016/j.jii.2021.100312>.

applications and impair the performance of blockchain systems.[38] Besides, user wallet attacks bring about cyber espionage and malicious exchanges. We will likely observe an increase in cybersecurity attacks on blockchain Application layers, affecting all connected energy applications, networks, and services due to increased attack surfaces from higher complexity and connectivity. This situation may eventually engender the sustained inability to conduct localised energy transactions, thus contributing to the decline of prosumerism and interruptions in energy operations.

The Data layer is the pivot of the blockchain, performing a salient role in the development of the architecture by operating as a data structure. This layer organises and maintains transactional data with a unique identifier known as a hash function. Timestamped and cryptographically linked data is recorded within a string of blocks and tethered to the Data layer.[39] However, some systems may be susceptible to burgeoning transaction privacy leakages. Malicious adversaries are likely to exploit the weakness of the architecture and infer linkability between transactions.[40] Such privacy leakages can affect data integrity and result in data protection violations. While private cryptographic keys are identity and security mechanisms the user retains on blockchain systems, common security challenges include the leakage or theft of private keys. A private key with a larger entropy and increasing randomness is more secure than a weak key with a lesser entropy. Scholars have ascertained the vulnerability in the Elliptic Curve Digital Signature Algorithm that fails to generate 'enough randomness' of private keys.[41] In what follows, data-related harm emerges from stolen private keys without sufficient legal recourse in decentralised landscapes.[42] Security preservation and enhancement mediums are necessary for every facet of the Data layer. As such, the codification of safety engineering and security by design can increase security by assigning responsibility to blockchain developers to construct tamper-proof and secure blockchain components.

The Network layer demonstrates a detailed mapping of blockchain operations. It plays a prominent role in data dissemination to facilitate communication and engagement between all participating nodes on the network.[43] The Network layer is salient to develop consensus and allow for block propagation. Communication is the Network layer's fulcrum, so it

[38] Muneeb Ul Hassan, Mubashir Husain Rehmani and Jinjun Chen, 'Differential Privacy in Blockchain Technology: A Futuristic Approach' (2020) 145 Journal of Parallel Distributed Computing 50–74 <https://doi.org/10.1016/j.jpdc.2020.06.003>.

[39] Hameed and others (n 37).

[40] N Deepa and others, 'A Survey on Blockchain for Big Data: Approaches, Opportunities, and Future Directions' (2022) 131 Future Generation Computer Systems 209–226 <https://doi.org/10.1016/j.future.2022.01.017>.

[41] Hartwig Mayer, 'ECDSA Security in Bitcoin and Ethereum: A Research Survey' (*CoinFaabrik*, 2016) <https://www.coinfabrik.com/wp-content/uploads/2016/06/ECDSA-Security-in-Bitcoin-and-Ethereum-a-Research-Survey.pdf>; Xiaoqi Li and others, 'A Survey on the Security of Blockchain Systems' (2020) 107 Future Generation Computer Systems 841–853 <https://doi.org/10.1016/j.future.2017.08.020>.

[42] Li and others (n 41).

[43] Hassan, Rehmani and Chen (n 38).

should be delicately engineered. The Network layer is susceptible to security attacks, generating qualitative and quantitative social and economic impacts. These attacks include distributed denial of service (DDoS), transaction malleability, routing, time jacking, and Sybil attacks. The malicious attackers on the network layer can subjugate honest nodes, thus gaining prejudicial and illegitimate control over the entire network and perpetuating a service disruption. There are parallel and growing concerns amongst participating nodes on the revenue losses and ramifications toward data integrity.

On the one hand, we explore the issue of blockchain developers who need more competence, integrity, and credibility. A poorly developed blockchain system could expose it to security attacks. For instance, a blockchain developer's decisions involving blockchain system configurations and programming codes may reflect a lack of foresight or incomplete information. These may lead to political, societal, and economic implications. Blockchain developers should assume responsibility and adopt security and risk management measures to mitigate such cyber threats by introducing changes to blockchain protocols and improving network functionalities after conducting due diligence and consulting experts. Generally, it is the role and responsibility of energy regulators to ensure that peer-to-peer energy trading systems are safe and secure for blockchain participants. In such instances, their powers include enforcing regulations and acting against developers who develop and implement insecure trading systems. Notably, regulators could consider institutionalising ex-post oversight, reviews and accountability mechanisms or even regulate norms to guide the behaviour of developers, engineers, and operators. However, considering the early warning signs of the disruptive impact of blockchain-enabled energy systems, it is crucial to adopt ex-ante pre-emptive and accountability measures to nip cybersecurity attacks in the bud. For instance, introducing certification mechanisms can alleviate negative externalities and information asymmetry and heighten confidence and trust among prosumers. Through such schemes, regulators can determine the adherence of blockchain to specific security requirements and ban blockchain products, services, and processes that fail to meet such requirements.

On the other hand, while many rigorous safeguards are embedded in the blockchain architecture to prevent security attacks, complete reliance on such mechanisms precipitates bias. Developers may regard blockchain as a silver bullet in establishing and maintaining security across the network, resulting in excessive trust in the technology. Such circumstances may affect decision-making processes as developers encapsulate complacency in developing the front-end and back-end of blockchain interfaces.

Blockchain developers or programmers may be tempered by laxness or unwitting neglect when developing blockchain layers, triggering technical, organisational, and systemic vulnerabilities. While holding blockchain developers accountable ex-post through institutional and normative oversight mechanisms is important, regulators should collectively mitigate such challenges at national and international levels through ex-ante regulations, such as safety standards and certification mechanisms.

2.4 Threats

As a starting point, malicious actors can use benign blockchain-based software as an attack surface to augment existing attacks or launch new attacks.[44] For instance, building new interfaces with improved features or enhancing existing applications can culminate in a larger attack surface, increasing susceptibility to security threats and attacks. While blockchain has made significant strides since its introduction as a tamper-evident system, it correspondingly entails concerns regarding the risk of security threats as malicious entities coordinate attacks based on new strategies and tactics to compromise and damage the blockchain network.

Such intrusions comprise two (2) categories: internal and external attacks. External attacks originate from the exterior areas of the network. In contrast, internal attacks relate to adversarial attacks by malicious entities that form a 'legitimate and authorised' part of the system.[45] Internal attacks leverage the privileges of the network by adding malicious nodes to the system to increase consensus power. Here, adversaries launch security attacks, such as Distributed Denial of Service (DDoS), with no difficulty, considering the high adversarial hashing that compromises the system.[46] Generally, in a decentralised system, a smidgen of malicious nodes does not compromise the systems, as honest nodes constantly surpass more than 51% of computational network power.[47] However, this does not eliminate security attacks, as malicious actors that leverage a large portion of computational resources can launch 51% of attacks by tampering with and falsifying the contents of blocks. Hence, it is precarious to use blockchain as adversaries can mount attacks and dictate the outcomes of transactions added to the ledger, which may lead to interruptions in the power supply. Another internal attack that generates profound ramifications is the Sybil attack which creates multiple malicious identities on the network to gain disproportionate influence and out-vote legitimate nodes. Adversaries disconnect honest nodes, gaining prejudicial and illegitimate control over the entire network.

The Sybil impinges network performance and restricts engagement between honest nodes, thus compromising energy transactions and allowing adversaries to mount selfish mining attacks where they withhold mined blocks without intentionally broadcasting them to the blockchain network to generate a fork.[48]

[44] Muhammad Saad and others, 'Exploring the Attack Surface of Blockchain: A Comprehensive Survey' (2020) 22 IEEE Communications Surveys & Tutorials 1977–2008 <https://doi.org/10.1109/COMST.2020.2975999>.

[45] Noshina Tariq, Farrukh Aslam Khan and Muhammad Asim, 'Security Challenges and Requirements for Smart Internet of Things Applications: A Comprehensive Analysis' (2021) 191 Procedia Computer Science 425–430 <https://doi.org/10.1016/j.procs.2021.07.053>.

[46] Dusica Marijan and Chhagan Lal, 'Blockchain Verification and Validation: Techniques, Challenges, and Research Directions' (2022) 45 Computer Science Review 100492 <https://doi.org/10.1016/j.cosrev.2022.100492>.

[47] Ashish Rajendra Sai and others, 'Taxonomy of Centralization in Public Blockchain Systems: A Systematic Literature Review' (2021) 58 Information Processing & Management 102584 <https://doi.org/10.1016/j.ipm.2021.102584>.

[48] Maisevli Harika, Sandi Rahmadika and DR Ramdania, 'Blockchain Technology for Managing an Architectural Model of Decentralized Medical Record' (2019) 1402 Journal of Physics: Conference Series 077027

In the case of external attacks, perpetrators can compromise nodes with high stakes on the network to initiate a denial of service and double spending attacks. External attackers can launch user-wallet attacks, such as dictionary attacks, to misappropriate users' security credentials. Further, blockchain users are prone to hot and cold wallet attacks, where adversaries maliciously obtain the private keys of victims on blockchain servers by hacking or exploiting a bug in the system.

On a broader scale, internal and external attacks relate to the 'unauthorized access, modification, misuse,' and destruction of blockchain networks to pursue illegal and illegitimate objectives, which can compromise the system.[49] Such attacks could lead to cascading effects and catastrophic failures within the energy network and affect the security and stability of energy access.

The lack of coordinated policies and standards on blockchain cyber security across different firms and industries can create barriers hamper blockchain development.[50] Indeed, it is necessary to develop congruous national and global governance structures as a measure of preparedness to avert crisis instead of fragmented structures that affect the viability and operability of blockchain. These security challenges necessitate proper governance responses to reduce vulnerabilities and participants' exposure to adversarial attacks. It is pertinent to develop security norms to (a) counter shortcomings, (b) improve the detection of malicious activities, (c) remove opportunities for adversaries with malicious motives, and (d) evaluate the employment of defensive and preventive measures.[51]

On the one hand, developers can design validating mechanisms that hinder security threats and vulnerabilities and are resilient to node failures and man-in-middle attacks. On the other hand, platform operators deploying blockchain-enabled energy processes can conduct red-teaming exercises. Red teaming involves assessing the susceptibility and vulnerability of blockchain infrastructure to security threats and attacks by stimulating cyberattacks within such systems. As a result, while various security measures and procedures can be adopted to strengthen the security layer of blockchain infrastructures, they could be more foolproof solutions.

<10.1088/1742-6596/1402/7/077027>; Dac-Nhuong Le and others (eds), *Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies* (John Wiley & Sons 2019) <https://doi.org/10.1002/9781119488330>; Choobineh and others (n 5).

[49] Vinod Kumar Mishra, 'Cyber Security in Blockchain based System' (2019) 1 Cybernomics 13–15 <https://www.cybernomics.in/index.php/cnm/article/view/8>.

[50] Shubhani Aggarwal and others, 'Blockchain for Smart Communities: Applications, Challenges and Opportunities' (2019) 144 Journal of Network and Computer Applications 13–48 <https://doi.org/10.1016/j.jnca.2019.06.018>.

[51] Muzammil Hussain and others, 'Blockchain-Based IoT Devices in Supply Chain Management: A Systematic Literature Review' (2021) 13 Sustainability 13646 <https://doi.org/10.3390/su132413646>; Jennifer J Xu, 'Are Blockchains Immune to All Malicious Attacks?' (2016) 2 Financial Innovation 25 <https://doi.org/10.1186/s40854-016-0046-5>; Eva C Uribe and others, *Paradigms and Challenges for Deterrence in Cyberspace* (2019) <https://doi.org/10.2172/1762337>.

There are hurdles in governing this domain due to the heterogeneity and complexity of blockchain. A significant setback that hinders the adoption of proper governance structures includes the need for systemic engagement between multi-stakeholders, namely the government, blockchain developers, and platform providers, on cybersecurity risks, leaving blockchain participants and honest nodes in precarious positions. Besides that, the absence of centralised control over a blockchain network and the inability to identify perpetrators raises questions on the attribution of liability for cyber-attacks within the blockchain domain.[52] As such, the anonymity of blockchain technology is used as a tool or shield for malicious actors to conduct illegal activities.

In essence, various security attacks surface from integrating blockchain technology within energy systems and characterise the same based on blockchain network attacks, user wallet attacks, smart contract attacks, mining pool attacks and transaction verification mechanism attacks. Regulators should explore a viable range of governance solutions by considering (a) the interplay and engagement of formal and informal institutions, (b) the role and agency of key actors (state and non-state), (c) diversity and connectivity of multi-level interactions, and (d) hierarchical, market and network governance structures.[53]

2.5 Impact

Having accessed the vulnerabilities and threats emanating from blockchain systems, we explore the potency of impact. Cyber-attacks impose considerable societal and technological impact (specifically towards blockchain's viability, operability, and effectiveness). There is a tendency to overstate or understate the impact of system vulnerabilities and cyber threats, mainly when (a) some impacts take a longer time to manifest than others and (b) the continuous development of technical solutions.

Amid an unclear trajectory of societal and technological impact, regulators adopt wait-and-see policies due to the rapidly evolving nature of blockchain. However, adopting wait-and-see policies may raise serious concerns, particularly if passivity engenders widespread cyber-attacks. Indeed, the stakes are too high to afford the wait-and-see policies, more so when the potential for abuse is great, expecting blockchain participants, already experiencing significant qualitative and quantitative impact, to continue bearing its burden without sufficient recourse to justice.

We explore the qualitative and quantitative impacts that undermine blockchain-enabled energy systems. In terms of qualitative impact, blockchain participants may be denied legitimate access to the blockchain network due to the overload of the network with spurious requests and attack traffic. System inefficiencies also directly impact or harm them ,

[52] Yan Teng, 'Towards trustworthy blockchains: normative reflections on blockchain-enabled virtual institutions' (2021) 23 Ethics and Information Technology 385–397 <https://doi.org/10.1007/s10676-021-09581-3>.

[53] Claudia Pahl-Wostl, 'A Conceptual Framework for Analysing Adaptive Capacity and Multi-level Learning Processes in Resource Governance Regimes' (2009) 19 Global environmental change 354–365 <https://doi.org/10.1016/j.gloenvcha.2009.06.001>.

slowing down network performance and computing power.[54] Besides that, through various cyber-attacks, adversaries alter, tamper, or falsify transaction history, compromising data integrity on the blockchain ledger.[55] Long-lasting reputational damage on blockchain systems is commonplace, with multiple cyber-attacks launched continuously, affecting users' trust in such systems and technological apathy.

In terms of quantitative impact, victims of cyber-attacks incur a loss of revenue due to (a) network downtime, (b) malicious reversals or alterations of blockchain transactions, (c) double-spending attacks, (d) waste of computational power, and (e) cost of recovery from attacks which can prove untenable for businesses and individuals.[56] Considering the blockchain applications' widespread security vulnerabilities and threats (as discussed above), their prospects of success in the energy sector need to be revised and more obscure. The complexity and novelty of blockchain raise intrinsic and extrinsic cybersecurity concerns, which could consequentially produce cascading and catastrophic failures when employed in critical infrastructures. Cybersecurity concerns in blockchain ecosystems can influence energy security resulting in interrupted supplies and energy vulnerabilities and hampering the continued operations of energy infrastructures. It is salient to devise legal norms, institutional policies, and regulatory frameworks to effectively circumvent these externalities and remain resilient to potential energy disruptions.

In the preceding section, the author revisits the security threats, vulnerabilities, and impacts on the blockchain infrastructure. Even though blockchain technology can enhance security capabilities in its multi-domain environment, it is not entirely resistant to cyberattacks as it can disconnect and disrupt legitimate users and nodes. A reliable energy system design is fundamental to prevent disastrous consequences such as interruptions in the power supply. The extent and severity of the cybersecurity risks depend on the architecture and operation of the blockchain network. The essential facets include the number of nodes on a blockchain network, authorisation requirements of the system, efficiency and reliability of consensus mechanisms and encryption strength.

3. The Veil of Anonymity and Attribution of Responsibility: Perpetrator-Focused Legislation

The operational feature of blockchain is its anonymity. Blockchain preserves anonymity by ensuring nodes and miners remain unidentifiable through any measure, concealing real-world addresses with digitally generated addresses.[57] While blockchain privacy and transaction unlinkability are generally accountable to anonymity, malicious attackers exploit

[54] Wani and others (n 18); Jahnavi (n 18).

[55] Chenhao Xu and others, 'A Light-Weight and Attack-Proof Bidirectional Blockchain Paradigm for Internet of Things' (2021) 9 IEEE Internet of Things Journal 4371–4384 <https://doi.org/10.1109/JIOT.2021.3103275>; Firdous Kausar and others, '6G Technology and Taxonomy of Attacks on Blockchain Technology' (2021) 61 Alexandria Engineering Journal 4295–4306 <https://doi.org/10.1016/j.aej.2021.09.051>.

[56] Divya Guru, Supraja Perumal and Vijayakumar Varadarajan, 'Approaches Towards Blockchain Innovation: A Survey and Future Directions' (2021) 10 Electronics 1219 <https://doi.org/10.3390/electronics10101219>.

this feature by launching cyber-security attacks on the network under pretenses. The lack of linkage and parallelism between the malicious actor's identity on the blockchain network and his real-world identity makes it impossible to ascertain the perpetrator. Hence, while anonymity is a key feature of blockchain, it results in dangerous and illegal behaviour, posing threats to the network and its users. There are concerns that the concealment of identity can implicate cybersecurity risks. Pervasive forms of exploitation and attacks prompt safety concerns and deter the stability of critical infrastructures, such as energy sectors.[58] As such, blockchain systems provide considerable latitude for disorderly conduct.

Blockchain broadens the attack surface and increases the likelihood of adversaries initiating attacks for malicious purposes. The high level of anonymity in the blockchain space poses cyber security risks, emerging as a driver for perpetrators to leverage blockchain and conduct illicit activities. Perpetrator-focused governance frameworks deter offenders from committing criminal acts by (a) advancing stringent legislation, (b) prioritising retributive justice and accountability, (c) increasing the risk of legal and administrative sanctions, and (d) improving detection, investigation, forensics, and enforcement systems. At the crux of cybercrime laws across jurisdictions are perpetrator-focused governance responses to thwart cyberattacks. These laws criminalise unauthorised or unlawful access, modification, impairment, manipulation, and interception of computer data, systems, or networks. However, the veil of anonymity renders perpetrator-focused frameworks ineffectual and nugatory. As a result, the legislative frameworks do not completely deter perpetrators from committing the offending behaviour through an incognito mode. For instance, in June 2016, an anonymous attacker hacked the Decentralised Autonomous Organisation on the Ethereum blockchain platform by exploiting the vulnerabilities underlying the Decentralised Autonomous Organisation's code, siphoning more than $50 million worth of ether. In 2017, about 4700 bitcoins amounting to $63.92 million were stolen by anonymous hackers on Nicehash, a third-party Bitcoin mining platform, causing it to halt payment and mining operations worldwide.[59] In 2018, blockchain-based cryptocurrencies, once hailed as foolproof networks and anonymous havens, namely Coincheck, Coinrail, Bitcoin Gold, and BitGrail, suffered cybersecurity attacks leading to the loss of millions of

[57] Aisha Zahid Junejo and others, 'RZee: Cryptographic and Statistical Model for Adversary Detection and Filtration to Preserve Blockchain Privacy' (2022) 34 Journal of King Saud University-Computer and Information Sciences 7885–7910 <https://doi.org/10.1016/j.jksuci.2022.07.007>.

[58] Charithri Yapa and others, 'Survey on Blockchain for Future Smart Grids: Technical Aspects, Applications, Integration Challenges and Future Research' (2021) 7 Energy Reports 6530–6564 <https://doi.org/10.1016/j.egyr.2021.09.112>; Hao Xu and others, 'Blockchain-enabled Resource Management and Sharing for 6G Communications' (2020) 6 Digital Communications and Networks 261–269 <https://doi.org/10.1016/j.dcan.2020.06.002>; Gregor Dorfleitner, Franziska Muck and Isabel Scheckenbach, 'Blockchain Applications for Climate Protection: A Global Empirical Investigation' (2021) 149 Renewable and Sustainable Energy Reviews 111378 <https://doi.org/10.1016/j.rser.2021.111378>.

[59] Jim Finkle and Jeremy Wagstaff, 'Hackers Steal $64 million from Cryptocurrency Firm NiceHash' (*Reuters*, 2017) <https://www.reuters.com/article/us-cyber-nicehash-idUKKBN1E10AQ>; Samuel Gibbs, 'Bitcoin: $64m in Cryptocurrency Stolen in "Sophisticated" Hack' (*The Guardian*, 2017) <https://www.theguardian.com/technology/2017/dec/07/bitcoin-64m-cryptocurrency-stolen-hack-attack-marketplace-nicehash-passwords>.

dollars.[60] In 2019, there was an increase in blockchain attacks. Unidentified hackers initiated 51% of attacks on blockchain-based cryptocurrency platforms, generating a recorded loss of over $292 million for investors and blockchain users and the collapse of many cryptocurrency exchanges.[61] Malicious attackers continue to outpace security embedded in blockchain networks. In 2020, blockchain attacks on cryptocurrency exchanges and wallets surged, with a recorded figure of 122 attacks and a loss of $3.78 billion.[62] In 2021, several blockchain attacks occurred, such as the 51% attack, ransomware attack, and Sybil attack, which allowed anonymous attackers to create fake identities and manipulate blockchain platforms.[63]

The anonymous and untraceable nature of malicious attackers on blockchain platforms impedes the investigation of blockchain-based attacks. The lack of effective governance responses presents unprecedented risks and challenges to the safety and security of blockchain users, honest nodes, and miners.

Further, considering the new cyber normalcy, distributed, decentralised and borderless blockchain transactions are not constrained to specific geographical locations and zones. This conflicts with the traditional construction of regulatory boundaries. Borderless operations allow malicious adversaries to mount attacks. Besides that, borderless paradigms function as a shield to avoid attracting regulatory scrutiny. The new cyberspace domain triggers questions on the attribution of responsibility and liability, considering the new attack vectors prompted by blockchain-based systems.

4. Ex-ante and Ex-post Mitigation Measures in Addressing Blockchain Security Attacks

4.1 Ex-ante Cybersecurity Risk Mitigation

Based on the preceding sections, blockchain technology faces many unique challenges, limitations, and barriers. The absence of specific safety requirements augments regulatory gaps and intensifies risks and vulnerabilities in the nation's critical energy infrastructure.

Cyber-resilient policy postures can mitigate unauthorised access, operations, and modifications that disrupt, manipulate, and impair blockchain systems and networks and ensure technology sturdiness to stem and steer blockchain in favourable directions. As such, the success of secure blockchain implementation in the energy sector lies in the quality of

[60] Christina Comben, '$1 Billion Dollar's Worth of Cryptocurrency Stolen in 2018' (*CCN*, 2021) <https://www.ccn.com/1-billion-dollars-worth-of-cryptocurrency-stolen-in-2018/>.

[61] Kausar and others (n 55).

[62] AIT News Desk, 'Blockchain Hackers Stole $3.8 Billion in 122 Attacks in 2020' (*AIThority*, 2021) <https://aithority.com/technology/blockchain/blockchain-hackers-stole-3-8-billion-in-122-attacks-in-2020/>.

[63] Herman Hayes, 'What is a Sybil Attack in Blockchain and Types of Sybil Attacks' (*BitKan*, 2022) <https://bitkan.com/learn/what-is-a-sybil-attack-in-blockchain-and-types-of-sybil-attacks-2798>; Anna Baydakova, 'Ransomware Payouts Declined in 2022: Crystal Blockchain' (*CoinDesk*, 2022) <https://www.coindesk.com/consensus-magazine/2022/12/22/ransomware-payouts-declined-in-2022-crystal-blockchain/>.

security governance and risk assessment, management, and mitigation measures. Further, preliminary checks and tests, internal control assessments, incident reporting protocols, threat assessments, standardisation and certification measures, security patching, and continuity planning demonstrate necessary safeguards and technical procedures for effective cybersecurity frameworks.[64] Therefore, aligning blockchain architecture, deployment, and operations with mitigation tools and modalities can prevent, detect, and form responses to escalating threats.

Risk assessment frameworks hinder cybersecurity attacks by identifying, assessing, and implementing security responses to minimise risks. Existing legal frameworks are aligned with centralised, top-down systems and need revision for a decentralised and distributed architecture.[65]

4.2 Standardisation and Certification Mechanisms Are Pertinent Ex-ante Mitigation Measures

In developing human-centred blockchain applications and shaping governance efforts, the relevance of standards and certification schemes for reliable quality assessments and advancement of ethical practices are noteworthy. Blockchain-enabled energy trading advances prospects of setting standards to circumvent cybersecurity risks and vulnerabilities. Industry standards provide benchmarks and metrics that level the playing field in blockchain development. Setting standards is not a straightforward task in a dense and diverse domain.

Standards ensure a stronger consensus on technical solutions that augment efficacy and functionality as they contribute to the interoperability and interactions between multiple blockchain platforms and technological solutions.[66] As more institutional authorities or standard-setting organisations define cybersecurity standards, best practices, strategies, and guidelines, it can contribute to improving blockchain-enabled energy trading systems. Further, the standards develop specifications to measure, analyse, and evaluate the quality, security, and effectiveness of blockchain products, services, processes, procedures, and entities.

The author highlights some of the more prominent international, regional, and national standardization organisations that explore and provide a framework and guiding principles for the development and use of blockchain. The IEEE Standards Association (IEEE SA) is a globally recognised standard-setting-entity and consensus-building organisation within the

[64] Alana Maurushat and Kathy Nguyen, 'The Legal Obligation to Provide Timely Security Patching and Automatic Updates' (2022) 3 International Cybersecurity Law Review 437–465 <https://doi.org/10.1365/s43439-022-00059-6>.

[65] Ahmed Alketbi, Manar Abu Talib and Qassim Nasir, 'Blockchain Security Framework for Government Private Blockchain Consortium' in Muhammad Habib ur Rehman and others (eds), *Trust Models for Next-Generation Blockchain Ecosystems* (Springer 2021) 225–249 <https://doi.org/10.1007/978-3-030-75107-4_9>.

[66] Liping Di and Berk Üstündağ, *Agro-Geoinformatics: Theory and Practice* (Springer Nature 2021) <https://doi.org/10.1007/978-3-030-66387-2>.

IEEE that develops and publishes technical standards.[67] IEEE SA engages in an open process and joins forces with global, regional, and national organisations, industry players, stakeholders, and the global community to ensure the development of such standards with effectiveness and high visibility. IEEE SA is actively involved in blockchain standardisation efforts in multiple sectors. However, compliance with the IEEE Standards does not equate to conformity with or abidance by legal and regulatory instruments.[68]

Besides that, the International Organisation for Standardisation, a worldwide federation of national standards bodies, develops and publishes a series of standards in a voluntary and consensus-based manner. The ISO established a Technical Committee, ISO/TC 307, to standardise blockchain and distributed ledger technology (DLT). Seven working groups and four advisory working groups constitute the ISO/TC 307, which has to date published several blockchain and DLT standards, including (a) ISO/TR 23455 on the overview and interactions between smart contracts in blockchain and DLT systems, (b) ISO/TR 23244 on privacy and personally identifiable information considerations, (c) ISO/TR 23576 on security management of digital asset custodians, and (d) ISO/TS 23635 on the fulfilment of governance, specifically risk and regulatory contexts.[69] However, ISO/DTR 23245 on security risks, threats, and vulnerabilities was not ripe for publication and subsequently deleted. Relatedly, exploring many standards, such as ISO/IEC 27000, in terms of information security management may be persuasive and can indirectly have a considerable pull in the realm of blockchain and DLT.

Further, the European Committee for Standardisation (CEN) and European Committee for Electrotechnical Standardisation (CENELEC) devised a Focus Group on blockchain and distributed ledger technology to reinforce the work conducted by ISOs in developing and defining voluntary standards, ascertaining potential standardisation needs and demands in the blockchain fora, and offering strategies and recommendations. A report by the Focus Group recommended a standardisation framework for information security to bolster overall security assurance. Following the recommendation presented in the report, CEN-CLC/JTC 19, a joint technical committee was established to identify and adopt international standards for blockchain and DLT at the European level, having appraised regional legislative and policy requirements and specificities.[70]

The British Standards Institution is UK's national standards body that develops standards for diverse products and services. The British Standards Institution recognises

[67] Xiaofeng Chen and others, 'Applications Oriented Technical Ecology for the Standardization of Blockchain in IEEE' (IEEE 9th International Conference on Cyber Security and Cloud Computing (CSCloud)/2022 IEEE 8th International Conference on Edge Computing and Scalable Cloud (EdgeCom), China, 2022) 43–49 <https://doi.org/10.1109/CSCloud-EdgeCom54986.2022.00017>.

[68] IEEE Blockchain, 'Standards' <https://blockchain.ieee.org/standards>.

[69] International Organisation for Standardisation, 'ISO/TC 307 Blockchain and distributed ledger technologies' <https://www.iso.org/committee/6266604.html>.

[70] CEN-CENELEC, *Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies* (2018) <https://www.cencenelec.eu/media/CEN-CENELEC/Areas%20of%20Work/CEN%20sectors/Digital%20Society/Emerging%20technologies/fg-bdlt-white_paper-version1-2.pdf>.

security threats and vulnerabilities circumjacent to blockchain and distributed ledger technologies. Further, BSI highlights the need for standardisation to ensure the efficacy and reliability of blockchain applications.[71]

On the other hand, certification schemes attest to the conformity of (a) products, (b) services, (c) processes, and (d) entities developing and programming blockchain systems to one or more standards. Blockchain developers that certify their energy products, services, or processes under voluntary certification mechanisms are prudent in cybersecurity measures to add value to the blockchain landscape and pre-empt the cost burden. Against this backdrop, the author argues that credible cybersecurity certification systems are a proactive catalyst to reduce the negative externalities of blockchain systems. Certification schemes send clear policy signals and facilitate the integration of secure blockchain systems in the energy sector, thereby increasing trust in decentralised and distributed digital ledger technology for trading electricity. Such schemes can potentially transform product development strategies as they provide a significant competitive advantage to blockchain platforms with quality, safety, and reliability. For instance, the legislative arm of Malta enacted the Innovative Technology Arrangements and Services Act to establish a voluntary certification process to demonstrate that their Innovative Technology Arrangements and Services meet the standards of law and bears the seal of approval of the Malta Digital Innovation Authority, the primary governmental authority.[72] The certification measures are in place to (a) foment confidence and trust amongst blockchain users and (b) procure institutional support for the viability, operability, and effectiveness of the Innovative Technology Arrangements and Services. The Malta Digital Innovation Authority may certify the Technology Arrangements and Services for the following 'specified purpose(s)' concerning the (a) qualities, (b) features, (c) attributes, (d) behaviours, or (e) aspects as specified in the Innovative Technology Arrangements and Services Act.[73] Issuing a certificate for one or more of the abovementioned purposes shall not operate as a certification for a different purpose. This requirement includes certifying that IT security considerations and system configurations and processes are advanced sufficiently by developers or owners of Innovative Technology Arrangements and Services. While obtaining such certification is at this stage, voluntary, a blockchain developer may want to procure certification to vouch for the quality or standards of their Innovative Technology Arrangements and Services and gain endorsement value in the national and international fora.[74]

Security patching is a defence mechanism involving the application of patches or issuance of system updates upon notification, identification, or discovery of security

[71] British Standards Institution, 'BSI: Unlocking Blockchain Benefits for your Business' <https://www.bsigroup.com/en-GB/Innovation/blockchain/>.

[72] Innovative Technology Arrangements and Services Act 2018.

[73] ibid.

[74] Rasim Alam, *A Policymaker's Guide to Blockchain Technology Implementation and Innovation* (UCTAD, 2020) <https://unctad.org/system/files/non-official-document/CSTD2020-21_ISP_T2_c02_Ralam_Harvard_en.pdf>.

vulnerabilities in products and systems.[75] Security patching must be a clearly defined legal requirement under cyber-security laws in many jurisdictions.[76] The failure to fill governance gaps exacerbates and perpetuates existing system vulnerabilities and heightens security risks for blockchain users.

Continuity planning minimises the impact of cyber incidents, generating greater resilience and agility when disaster strikes.[77] In critical infrastructure, the immediate disruption to the energy service can cause massive power outages. Thus, legal, and regulatory frameworks that impose continuity planning obligations provide additional safeguards to mitigate security ramifications and insulate blockchain-enabled energy applications against catastrophic safety failures.[78]

Incident reporting protocols are imperative to avert or cyber-attack's adverse consequence and irreversible damage. Incident reporting requirements can improve organisational and technological resilience by analysing the root of the problem in the interest of blockchain-enabled peer-to-peer energy systems. The lack of mandatory incident reporting of a cyber security violation on critical infrastructures increases the risk of internal and external attacks.[79] However, the regulatory concern is determining whether the incident reporting obligation is directed only at blockchain developers, platform operators or all the blockchain network nodes.

In essence, this section highlights the technical and organisational safeguards that effectively circumvent blockchain security violations, thus ensuring the efficacy and resilience of critical infrastructures. Regulators need to consider integrated and comprehensive approaches by embarking on more significant efforts to ensure effective regulation of blockchain technology.

4.3 Ex-post Response to Cyberattacks

To punish perpetrators who commit cyber-attacks, effective legal and regulatory mechanisms are pertinent. There are two schools of thought. The former asserts that existing regulations or legal principles limit malicious practices that may be adequate, appropriate, and viable for blockchain activities and applications.[80] The latter states that existing laws,

[75] Maurushat and Nguyen (n 64).

[76] ibid.

[77] Alketbi, Talib and Nasir (n 65).

[78] Taimur Bakhshi and Bogdan Ghita, 'Perspectives on Auditing and Regulatory Compliance in Blockchain Transactions' in Muhammad Habib ur Rehman and others (eds), *Trust Models for Next-Generation Blockchain Ecosystems* (Springer 2021) 37–65 <https://doi.org/10.1007/978-3-030-75107-4_2>.

[79] Erik Silfversten and others, *Cybersecurity-A State-of-the-Art-Review* (Rand Europe, 2020) <http://hdl.handle.net/20.500.12832/3016>.

[80] Simona Ramos, Lela Melon and Joshua Ellul, 'Exploring Blockchains Cyber Security Techno-Regulatory Gap. An Application to Crypto-Asset Regulation in the EU' (10th Graduate Conference in Law and Technology, Sciences Po (2022), Paris, 2022) <https://doi.org/10.2139/ssrn.4148678>.

regulations and guidelines need to grapple with the advent of blockchain technology.[81] While 156 of 195 countries have enacted cybercrime legislation on computer technologies, blockchain raises novel and technology-specific safety and security challenges. The architecture of blockchain, which has specific characteristics, coupled with the novelty of the technology, makes it unusually challenging to regulate. Therefore, a nuanced cybersecurity framework is crucial for blockchain participants' protection.[82]

Regulators need to examine the cyber practices of their jurisdiction and determine how closely or well aligned these legal and regulatory frameworks are with security issues that manifest in blockchain landscapes. In many jurisdictions, such as Singapore,[83] Australia,[84] Japan,[85] and India,[86] it is unlawful to commit or facilitate unauthorised access, modification or impairment of computer systems, networks, or data residing on the computer, knowingly or intending to cause harm or damage.

Further, in the United Kingdom, the Computer Misuse Act 1990 was enacted to address the challenges posed by hacking under the ambit of unauthorised system access and data manipulation. However, it did not envisage various digital architectures as vulnerable attack surfaces. The Computer Misuse Act's fundamental prohibition was the 'unauthorised modification of the contents of any computer.'[87] In the previous Computer Misuse Act enactment, the prohibition was replaced by a broader provision by the Police and Justice Act 2006, criminalising 'unauthorised acts with intent to impair the operation of any computer,' designed to hinder the proliferation of DDoS and deal with information technology attacks. DDoS is an offence under Section 3 of the amended Computer Misuse Act.

Currently, specific national legislation or international framework exists globally to address blockchain cybersecurity attacks. It is crucial to determine if such legislation is necessary for blockchain cyber-attacks or whether a better approach lies within existing legislation.

In many countries, existing cyber security legislation focuses on (a) impairment of computer functions, (b) lack of authority, and (c) intent to cause harm or damage. It is pertinent to consider whether the terms computer, computer networks, data storage device, computer material, and data held in a computer in cyber laws are broad enough to encompass blockchain technology.

The logical approach is to assess the definitional parameters of blockchain. In recent years, scholars have made active efforts to define blockchain comprehensively. According to

[81] ibid.

[82] Nazar Waheed and others, 'Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures' (2020) 53 ACM Computing Surveys 122 <https://doi.org/10.1145/3417987>.

[83] Computer Misuse Act 1993, ss 3–8.

[84] Cybercrime Act 2001, s477(1), (2), and (3).

[85] The Basic Act on Cybersecurity Act No. 104 of 2014), Article 2.

[86] Information and Technology Act of 2000, ss 43(a)–(h).

[87] Computer Misuse Act 1990 prior to amendment by the Police and Justice Act 2006, s3.

scholar Figueiredo et al., 'blockchain is a computer technology that relies on the capabilities of computer algorithms and processes involved in data authentication, consistency, and transparency assessments.'[88] Scholars Adamska et al and Duan et al regard blockchain as a data storage system.[89] Others connote blockchain as a shared database between multiple nodes on the computer network.[90] Further, growing legal and regulatory initiatives focus on defining blockchain to facilitate functionality and governance and remove barriers to entry in diverse blockchain domains. For instance, in the United States, Illinois defines blockchain as 'an electronic record created by the use of a decentralised method by multiple parties to verify and store a digital record of transactions which is secured by the use of a cryptographic hash of previous transaction information' under the Blockchain Technology Act 2019.[91] A robust definition of computer technology, systems, programs, and networks can include a wide range of technologies, such as blockchain, which uses computer hardware or software as a tool to facilitate operations.

Numerous blockchain cyber security attacks fall within the domain of existing cyber laws, criminalising unauthorised use, access, alteration, modification, or impairment of computer networks or systems.[92] For instance, the prevalent attacks on hot and cold wallets, where malicious attackers attempt to retrieve the private keys of blockchain users from the server, constitute an offence under these cyber laws. Besides that, creating multiple malicious identities to act as legitimate nodes, restricting engagements between honest nodes, and compromising blockchain network performance would contradict of regulatory provisions.[93] Isolating and disconnecting multiple nodes from the blockchain network by committing routing and eclipse attacks constitute computer offences as such attacks

[88] Karoline Figueiredo and others, 'Assessing the Usability of Blockchain for Sustainability: Extending Key Themes to the Construction Industry' (2022) 343 Journal of Cleaner Production 131047 <https://doi.org/10.1016/j.jclepro.2022.131047>.

[89] Barbara Aleksandra Adamska, David Blahak and Fonbeyin Henry Abanda, 'Blockchain in Construction Practice' in Syed M Ahmad and others (eds), *Collaboration and Integration in Construction, Engineering, Management and Technology* (Springer 2021) 339–343 <https://doi.org/10.1007/978-3-030-48465-1_57>; Chaojie Duan, 'Design and Implementation of an Information Security Platform for the IoT Based on Blockchain' in Bernard J Jansen, Haibo Liang and Jun Ye, *International Conference on Cognitive based Information Processing and Applications (CIPA 2021)*, vol 2 (Springer 2022) 382–389 <https://doi.org/10.1007/978-981-16-5854-9_48>.

[90] Prashant Singh and others, 'Blockchain and AI Technology Convergence: Applications in Transportation Systems' (2022) Vehicular Communications 100521 <https://doi.org/10.1016/j.vehcom.2022.100521>; Bodicherla Digvijay Sri Sai and others, 'A Decentralised KYC based Approach for Microfinance using Blockchain Technology' (2023) 1 Cyber Security and Applications 100009 <https://doi.org/10.1016/j.csa.2022.100009>.

[91] In what follows, the term electronic means 'technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities,' similar to the definition of 'computer' under the Computer Misuse and Cybersecurity Act of Singapore.

[92] Sabreen Ahmadjee and others, 'A Study on Blockchain Architecture Design Decisions and their Security Attacks and Threats' (2022) 31 ACM Transactions on Software Engineering and Methodology (TOSEM) 36e <https://doi.org/10.1145/3502740> Anthony Serapiglia, *Cybersecurity and Cryptocurrencies: Introducing Ecosystem Vulnerabilities through Current Events* (Proceedings of the EDSIG Conference, Cleveland, Ohio, 2019) <https://proc.iscap.info/2019/cases/5110.pdf>; Fangfang Dai and others, 'From Bitcoin to Cybersecurity: A Comparative Study of Blockchain Application and Security Issues' (2017 4th International Conference on Systems and Informatics (ICSAI), China, 2017) 975–979 <https://doi.org/10.1109/ICSAI.2017.8248427>.

manipulate and interfere with the blockchain network. Under this pretext, there is no requirement for separate legislation specifically addressing blockchain, as existing cyber security provisions are adequate and effective in countering most blockchain attacks. Without specific frameworks, general rules, policies, and legislation on cybercrime should continue to govern blockchain users, developers, and operators. Even though existing cybersecurity laws are not tailored explicitly for blockchain technology, they may be effective in cases where a blockchain developer intentionally develops a platform or introduces specific features that aid or abet the commission of illegal activities. — considering the embryonic stage of blockchain, regulating too soon risks stymieing blockchain development. As such, the tide remains against specific legislation in stimulating technological growth.

However, the challenge is the need for more structured and architecture-related legislation to address various blockchain-related attacks.[94] Blockchain attacks compromise the functionality and operation of the network by forging or withholding transactions, isolating honest nodes, adding fake nodes, exposing sensitive information, storing malware, delaying confirmation time, and exploiting vulnerabilities. Considering the existing legislations, technological and operational specificities of blockchain systems need to address different classifications of blockchain cyberattacks in a targeted and streamlined manner. As such, they are stretching existing frameworks to deal with blockchain attacks that may be inappropriate to circumvent specific blockchain layer attacks, network attacks, and malware attacks. The preferred regulatory strategy is promulgating fit-for-purpose legislation to recognise, identify, and protect blockchain users, legitimate nodes, and miners more effectively against security attacks. Specifically, legislative provisions tailored for blockchain attacks testify to the limited protection under general cyber security legislation. A national government maintains the ability to influence blockchain development by enacting laws that directly impede blockchain attacks, thus allowing the adoption of blockchain-enabled energy trading.

5. Conclusion

Blockchain-enabled energy trading applications have gained traction worldwide, with numerous pilot projects in progress. In this article, the author sheds light on blockchain technology's threats, vulnerabilities, and impacts, emphasising the potential cybersecurity risks that could have disastrous consequences for critical infrastructure. One prominent concern is the anonymity feature of blockchain, which threatens the network and renders perpetrator-focused governance instruments useless. The existing legislative framework falls short in deterring perpetrators, as blockchain applications are not confined to specific geographic locations, raising questions about responsibility and liability attribution. To

[93] Sotirios Brotsis and others, 'On the Suitability of Blockchain Platforms for IoT Applications: Architectures, Security, Privacy, and Performance' (2021) 191 Computer Networks 108005 <https://doi.org/10.1016/j.comnet.2021.108005>.

[94] Ramos, Melon and Ellul (n 80).

address these issues, the author analyses ex-ante and ex-post mitigation measures to circumvent unauthorised access, operations, and modifications that could manipulate and impair blockchain applications and recommends that nation-states take a proactive approach to defining adjudication and enforcement measures, offering a cohesive framework to combat blockchain-related attacks. While blockchain-enabled applications play a crucial role in achieving decarbonisation, decentralisation, and digitalisation goals, it is essential to establish regulatory instruments that safeguard blockchain users, nodes, and miners. Looking ahead, the author proposes developing a regulatory readiness assessment framework that includes regulatory indicators. This framework would enable countries to assess their regulatory readiness levels and develop suitable and enabling frameworks to address blockchain-related challenges.

Acknowledgement

The author expresses her gratitude to Drs Felicity Deane, Sherin Kunhibava, and Pardis Moslemzadeh Tehrani for their comprehensive comments on the draft of this article.

Funding

The author received no funding from any party for the research and publication of this article.◆

(This page is intentionally left blank.)