Advanced Persistent Threats and Blockchain Technology: Exploring the Potential of Decentralized Defense Mechanisms

Waqas Ahmed

Air University, Islamabad, Pakistan

Correspondence to: Waqas Ahmed, Waqaskhattak99@gmail.com

Additional material is published online only. To view please visit the journal online.

Cite this as: Ahmed W. Advanced Persistent Threats and Blockchain Technology: Exploring the Potential of Decentralized Defense Mechanisms. Premier Journal of Science 2025;8:100065

DOI: https://doi.org/10.70389/PJS.100065

Received: 6 January 2025

Revised: 9 February 2025

Accepted: 10 February 2025

Published: 25 February 2025

Ethical approval: N/a

Consent: N/a

Funding: No industry funding

Conflicts of interest: N/a

Author contribution: Waqas Ahmed – Conceptualization, Writing – original draft, review and editing

Guarantor: Waqas Ahmed

Provenance and peer-review: Commissioned and externally peer-reviewed

Data availability statement: N/a

ABSTRACT

Advanced persistent threats (APTs) make up a significant cybersecurity challenge due to their ability to be stealthy and sophisticated and contain a long attack duration. These defenses typically do not work, especially traditional ones. This article explores the possible use of blockchain technology as a decentralized answer to combat APTs. Novel defense mechanisms are proposed by leveraging blockchain's core features of decentralization, immutability, and transparency, including systems for decentralized threat intelligence sharing, secure access control, and automated response via smart contracts. It compares existing blockchain-based frameworks and shows their strengths, scalability challenges, and performance trade-offs. A conceptual decentralized defense framework is presented based on real-time detection and mitigation strategies. Finally, recommendations for integrating blockchain with existing security infrastructures and future research directions in decentralized cybersecurity are made.

Keywords: Advanced persistent threats, Blockchain technology, Decentralized cybersecurity, Threat intelligence sharing, Smart contracts

Introduction

Overview of Advanced Persistent Threats (APTs)

APTs are a serious problem in the cybersecurity world, becoming stealthy, complicated, and long-lived. Compared to normal cyberattacks with immediate impact intent, those APTs focus on specific organizations or nations and try to keep continuous access for prolonged periods. APT starts with a threat actor who often represents a state-sponsored group or a well-organized group, launching the attacks by deploying techniques such as phishing or zero-day vulnerabilities.[1] The attack lifecycle involves multiple phases: initial compromise, lateral movement to escalate privileges, and finally concluding in data exfiltration or sabotage. This increases the danger of evading traditional detection systems, making them extremely dangerous to sensitive data and critical infrastructure.

Introduction to Blockchain Technology

Blockchain technology, by design, was built to prevent malicious actors from tampering with cryptocurrency transactions, and its decentralized, immutable nature, along with its consensus-based trust model, has started to attract attention within the cybersecurity community. On a blockchain, any data is distributed to nodes, and tampering is a lot harder.[2] Several vulnerabilities APTs exploit, however, can be solved with transparency and resistance to manipulation inherent in the technology. Utilizing blockchain, organizations can extend threat intelligence sharing, enhance secure access controls, and automate responses by leveraging smart contracts to aid an effective defense against emerging threats.[3]

Objectives and Scope

Primary Objective

To investigate the potential of blockchain technology in mitigating the risks posed by APTs through decentralized defense mechanisms.

Secondary Objectives

- To study APT characteristics and their impact on cybersecurity.
- To examine the novel characteristics of blockchain technology with the potential to rectify APT vulnerabilities.
- To assess existing blockchain-based security frameworks and adapt them to APT defense.

Exploratory Objective

A decentralized defense framework incorporating blockchain for a stronger defense against the perpetrators of APTs is proposed.

Background

APTs

As a result, APTs are considered a key and persistent cybersecurity problem due to their extremely conductive and hidden natures. The lifecycle of an APT is multiphase, consisting of infection, navigation, and exploitation of target systems across an extended period. The initial intrusion often involves phishing attacks, social engineering, or the exploitation of zero-day vulnerabilities. These techniques are used by attackers to bypass security defense and gain unauthorized access. Deploying backdoors, Trojans, or rootkits, they gain persistence inside the system, continuing to act undetected.[4] Attacks during the lateral movement phase escalate privileges, traverse the network, and systematically discover sensitive data or critical systems. The third and last phase, data exfiltration or destruction, is the matter of transferring confidential information out of the network or carrying out disruptive actions to achieve strategic goals.

One of the main reasons for the complexity is the adaptive and clandestine APT operations. The Stuxnet attack on Iranian nuclear centrifuges put tactics of sophisticated malware disrupting physical infrastructure into a new era of cyber warfare. Similarly, the SolarWinds supply chain attack revealed how trusted software updates could be turned into a weapon to infiltrate government agencies, major corporations, and more.[5] These APT examples highlight the great national security and global enterprise risks they represent.[1]

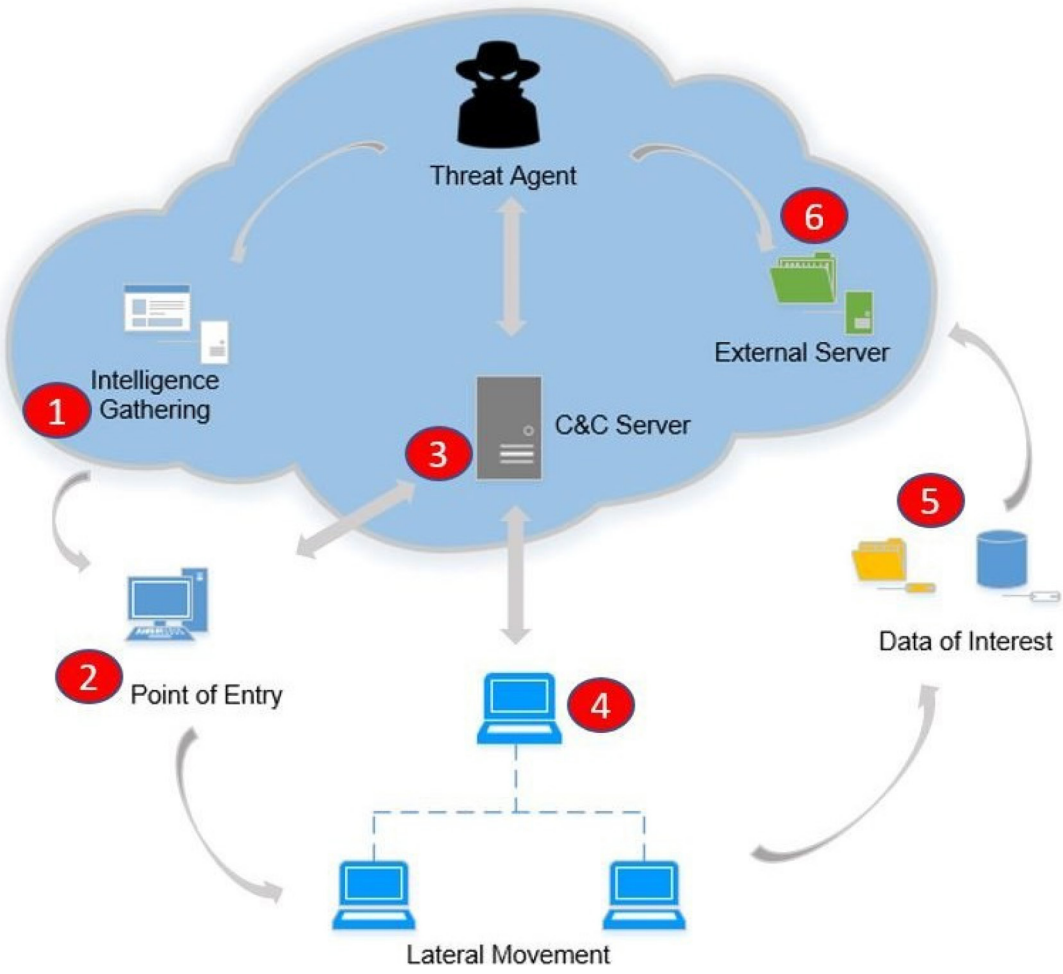

Fig 1 | A lifecycle diagram showing the progression of an APT attack from initial intrusion to data exfiltration
Source: Al Amin (2021)[5]

To address APTs, we need high-protection strategies outside signature-based methods, as they cannot effectively defeat custom malware and unknown exploits. Detection capabilities have been considerably improved through techniques including behavioral analytics, anomaly detection, and artificial intelligence (AI) based methods of threat hunting. Now more than ever, there is a need for collaborative and innovative defenses based on real-time threat intelligence and automated mechanisms (Figure 1).

Blockchain Technology

Blockchain technology is an increasingly important tool in cybersecurity with unique properties that can fill in several cybersecurity gaps that exist in centralized systems—an overview of what blockchain is based on its decentralization, its immutability, and its transparency. Compared with conventional databases that are centralized under one authority's control, a blockchain network diffuses data across several nodes.[6]

Public blockchains such as Bitcoin and Ethereum are suitable for use in applications where the data must be transparent to everyone. While consortium blockchains belong to the hybrid model, they combine a group of organizations to manage the network, where it is currently being used in cybersecurity includes secure identity management that builds on decentralized identifiers (DIDs) to improve privacy while reducing the risk of identity theft, tamper-proof logging systems that create immutable records from which data can be audited or used for forensic analysis.[7]

Key Challenges in Combating APTs

The vulnerability of centralized systems is one of the core challenges in mitigating APTs. Attackers target weak points and undermine critical infrastructure with little effort. The biggest problem is that there is not enough robust threat intelligence sharing among organizations, which impedes collective defense. It is very hard to detect intrusions using sophisticated APT tactics before they do a lot of damage.[8] In addition, record integrity and totality are issues of perpetual salience, especially in systems susceptible to insider threats.

Blockchain-Based Defense Mechanisms

Decentralized Threat Intelligence Sharing

Blockchain's distributed ledger can build tamper-proof networks to share threat intelligence among organizations. Collective improvement in situational awareness is possible by storing the threat signatures, the

DOI: https://doi.org/10.70389/PJS.100065 | Premier Journal of Science 2025;8:100065

indicators of compromise (IOCs), and the attack patterns on a blockchain by stakeholders. In the case of platforms like MITRE ATT&CK, blockchain could enhance the prevention of data manipulation.[9]

Authentication and Access Control

Using blockchain, DIDs can be used to revolutionize secure identity management. Combining multi-factor authentication with blockchain-based access control in concert with zero trust models can help to reduce the risks associated with unauthorized access. Smart contracts with access policies can be used as a practical example of using smart contracts to automatically enforce access policies in a real-time manner without centralized control.[10]

Data Integrity and Provenance

However, one of the reasons blockchain is so good at maintaining data integrity is that it is immutable. Logs stored on a blockchain ledger are resistant to tampering, facilitating secure auditing and forensic analysis. The utility of blockchain applications in supply chain security, where data provenance is paramount, is shown.[11]

Malware Analysis and Prevention

Nodes can co-analyze suspicious files in a decentralized malware detection framework supported by blockchain. In other words, smart contracts could be used to automate the response, such as quarantining infected nodes or alerting admins if abnormal behavior is detected.[9]

Comparative Analysis of Blockchain Solutions

Security Effectiveness Against APTs

Blockchain core features, decentralization, immutability, and verification by consensus provide strong defenses against APTs. Blockchains eliminate single points of failure and cut down on the risk that an adversary could seize and hijack a central authority. In a decentralized threat intelligence network, the ability to tamper-proof share IOCs with other organizations improves both situational awareness and defense strategy as a community.[12] Blockchain log immutability improves forensic analysis, making it easier for cybersecurity teams to detect and trace attack vectors more accurately.

Performance Impact on System Operations

The performance trade-offs of implementing blockchain for security purposes are evident in public blockchains like Bitcoin and Ethereum, which prioritize security and decentralization at the cost of transaction speed due to their proof-of-work consensus mechanisms. These systems may be secure, but because of their high computational requirements and latency, they are not always suitable for real-time security operations.[13]

Permissioned access and tailored consensus algorithms (e.g., proof of authority [PoA] or Byzantine fault tolerance) improve performance and are offered through private (and consortium) blockchains. Even these systems, however, may come with overhead over traditional databases.[10]

Scalability and Practical Deployment Challenges

However, blockchain-based security still faces scalability as a major challenge. The high transaction volumes like blockchains are not helpful to public blockchains that are constrained by the consensus mechanism and block size constraints. As we look to scale to handle larger amounts of transactions, solutions like sharding and sidechains will help improve scalability but come with their complexities.[14] However, consortium and private blockchains have better scalability properties, but their deployment is faced with practical issues such as interoperability, governance, and trust among participating parties (Table 1).

Practical Barriers to Implementation in Resource-Constrained Environments

Implementation of blockchain-based security solutions faces various operational obstacles while benefiting from their significant operational benefits. The primary concern arises from computation expenses along with energy requirements. Public blockchains with proof-of-work (PoW) consensus protocols need major assets of processing power in combination with significant energy usage. Such requirements represent a major obstacle for organizations like small businesses in developing countries and underfunded institutions that lack extensive IT capabilities.[13]

Hardware devices and storage capability represent critical problems in blockchain operations. Blockchain networks that serve security and forensic analysis need extensive storage capabilities due to their unalterable characteristics. Every node needs to keep either an entire ledger or a reduced version of it, which produces substantial storage requirements that small or constrained entities cannot manage.[12]

The project faces challenges from network delays joined with bandwidth limitations when executed over slow or unreliable internet connections. Identity management that uses blockchain technology faces challenges in remote areas because its threat-intelligence-sharing method requires continuous network synchrony between numerous nodes, but this becomes difficult when digital infrastructure is sparse.[15]

The implementation of blockchain solutions becomes difficult due to the complexity of startup expenses combined with the need for specialized technical knowledge. Multiple organizations with limited resources lack sufficient experts to build, manage, and protect their blockchain system base.[16] The difficulty of implementing blockchain technology into established legacy programs increases the problem.

The process of blockchain adoption gets hampered by governance hurdles and regulatory complications, which

Table 1 | Comparative analysis of blockchain-based security solutions

Solution	APT Defense Effectiveness	Performance Impact	Scalability Challenges
Blockchain-Based Threat Sharing	High	Moderate	Data synchronization
Identity Management via Blockchain	High	Low	Adoption complexity
Smart Contract Automated Response	Medium	High	Execution latency

most strongly affect those regions that lack robust cybersecurity regulations. Security frameworks that work between blockchain systems and traditional security systems create legal complexities that organizations with minimal legal support struggle to understand.[13]

The adoption of blockchain technology requires specific technological solutions using PoA and delegated proof of stake (PoS) designs, along with fusion systems between blockchain and classical databases supported through state backing or industrial collaboration to advance blockchain implementation in restricted environments.

Proposed Decentralized Defense Framework

Architecture of the Proposed Framework

We propose a decentralized defense framework that utilizes the power of blockchain technology to fight against APTs.[15] It consists of three primary components: blockchain network, smart contracts, and threat intelligence nodes. Each threat intelligence node stands for one organization, the security vendor, or even the networked device that collects and analyzes the threat data. It allows for the flow of these nodes to share IOCs and attack patterns as part of a collective defense strategy.[16]

The framework is built atop the blockchain network, which records threat data immutably and shares it among nodes. It implements the consensus mechanism that optimizes performance concerning the security of data authenticity and integrity.[15] This decentralization removes single points of failure, which, as a result, make it much harder for attackers to compromise the system.

Real-World Applications and Case Studies of Blockchain in Cybersecurity

Guardtime serves as a standout example within APT Defense Effectiveness by using blockchain technology to establish network security systems for government institutions and corporate organizations. The Baltic nation of Estonia demonstrates its status as a worldwide leader in digital governance through blockchain-based cybersecurity solutions that defend public as well as private sector data from continuing cyber threats. The unalterable nature of blockchain technology protects important information from tampering attempts, thereby securing networks against APT-driven cybersecurity threats. Security teams gain better awareness of persistent threats through coordinated intelligence-sharing networks that include MITRE ATT&CK and Cyber Threat Alliance solutions.

Educational research shows that the Food Trust blockchain from IBM utilizes permissioned blockchain solutions with PoA consensus to deliver high-performance security measures.[16] The initial purpose of this system is to monitor supply chain security. It has shown how data-sharing capabilities alongside fast verification establish a method to handle security implementation trade-offs. The financial sector, together with healthcare, makes use of Hyperledger Fabric to implement security protocols that provide controlled access alongside the necessary operational speed.

The Blockchain Service Network (BSN) of China offers essential insights about managing scalability and deployment problems. The BSN project faces identical deployment obstacles to those experienced by blockchain-based security solutions because it drives blockchain platform unification for higher adoption rates, yet it encounters hurdles with stakeholder governance, regulatory compliance needs, and network interoperability standards. The Blockchain Strategy of Dubai faces challenges during adoption as it struggles with standards for operations and different platform interaction standards.

Functionalities

Threat Detection and Real-Time Alerting

The framework enables real-time threat detection by utilizing data analytical and pattern recognition algorithms orchestrated at each node. If an anomaly is detected, the relevant threat data is submitted to the blockchain, and a check is completed to verify and share the threat data with other nodes.[17] Once identified, smart contracts alert security administrators and other stakeholders with automated alerting mechanisms notifying the security administrator of potential threats.

Automated Mitigation Processes

Critical mitigation processes are automated using smart contracts, such as isolating compromised systems or revoking unauthorized access privileges.[18] One of the use cases for smart contracts is to replace the existing manual intervention in case a threat intelligence node detects a malicious IP address, for example, and update network firewalls across the entire network of nodes without it.[17] As such, this automation netted us a much more consistent response, a faster response time, and fewer errors prone to humans, and thus, this automation improved overall threat management efficiency (Figure 2).

Evaluation of Potential Benefits and Limitations

Benefits

The key benefits of the proposed framework are presented below. Because it is decentralized, the system is more resilient to a single point of failure, making it much harder for attackers to compromise the system. The immutability of threat intelligence data ensures the integrity of the data, which is the foundation of forensic investigations.[20] Smart contracts automate processes that lower response times and maintain security policy consistency.

Limitations

The framework is, however, not without its challenges. Continuous blockchain transactions might cause performance overhead in high-traffic situations.[18] However, scalability is still an issue as the need for faster consensus may inevitably increase with larger networks; there needs to be more sophisticated

DOI: https://doi.org/10.70389/PJS.100065 | Premier Journal of Science 2025;8:100065

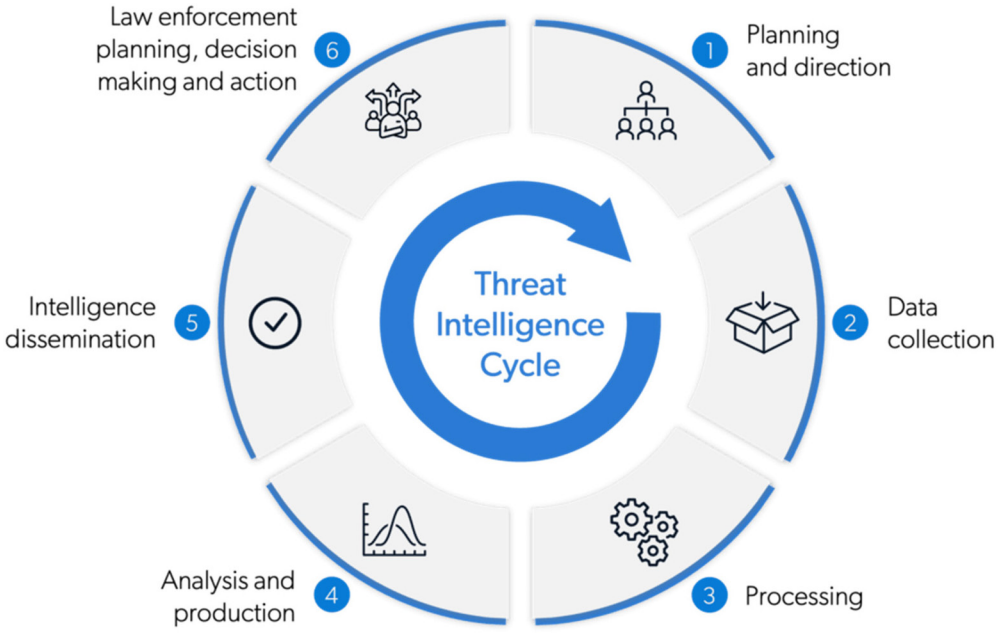

Fig 2 | Lifecycle of a threat from detection to mitigation within the framework. Include nodes that represent detection, blockchain validation, alerting, and smart contract-based responses
Source: Bhutta (2021)[19]

consensus mechanisms to handle massively large data loads.[21] Integration of blockchain-based systems with existing infrastructure requires substantial investment and technical knowledge.

Discussion

Critical Analysis of Blockchain's Role in Defending Against APTs

One of the biggest advantages of using blockchain technology to combat APTs is its numerous transforming capabilities. As it is inherently decentralized and, therefore, cannot be tampered with, it is the perfect foundation for secure data and transparent, trustless systems. One of the most serious vulnerabilities exploited by APT attacks is the possibility of catastrophic failure due to corrupted central servers, and blockchain helps minimize the risk by distributing control across a network.[22]

Blockchain, though, is not a panacea. It improves data integrity, but it does not directly tackle human-centric vulnerabilities (phishing, social engineering), which are the most common ways APTs get in. Additionally, cryptographic keys are used to trust in blockchain, and it will be vulnerable if the keys are lost or compromised.[21] However, the immutability of a blockchain can be a liability if the data that goes there is incorrect or malicious, which makes the design of smart contracts and governance frameworks to prevent and correct errors very important.[23]

Trade-offs Between Decentralization, Scalability, and Implementation Complexity

Much of the advantage of blockchain comes from decentralization, but this characteristic has its trade-offs. Consensus in decentralized systems is a computationally demanding task that slows down the speed of processing and increases latency.[19] Public blockchains using PoW mechanisms are particularly susceptible to performance bottlenecks, making them unsuitable for environments requiring rapid threat detection and response. Alternative consensus mechanisms like PoS or PoA must ensure securing at least at the same level while being efficient.[24]

In addition, it is another challenge of scalability. On our journey to grow the volume of transactions and utilize more and more nodes, we must sufficiently consider delays and lower performance of the blockchain networks unless we have implemented advanced solutions like sharding or sidechains.[25] Despite their promise, these approaches introduce more complexity and demand robust management lest they also introduce new security risks.[26]

It is a tough integration task from the implementation perspective to efficiently combine blockchain into the existing security infrastructure. For organizations to design, deploy, and maintain blockchain systems, they require a certain level of technical expertise, while interoperability with existing legacy technologies potentially demands custom solutions.[27] While there are challenges to the development of blockchain, such as scaling issues as well as blockchain technical maturity, blockchain still presents worthwhile investment as a potential future-proofing technology for cybersecurity's data integrity and automated policy enforcement (Figure 3).[28]

Recommendations for Integrating Blockchain into Existing Security Infrastructures

Organizations should adopt a hybrid approach that utilizes the strengths of a blockchain to plug into the strengths of current security frameworks and mitigate the limitations of blockchain technology. In enterprises, private or consortium blockchains bring better

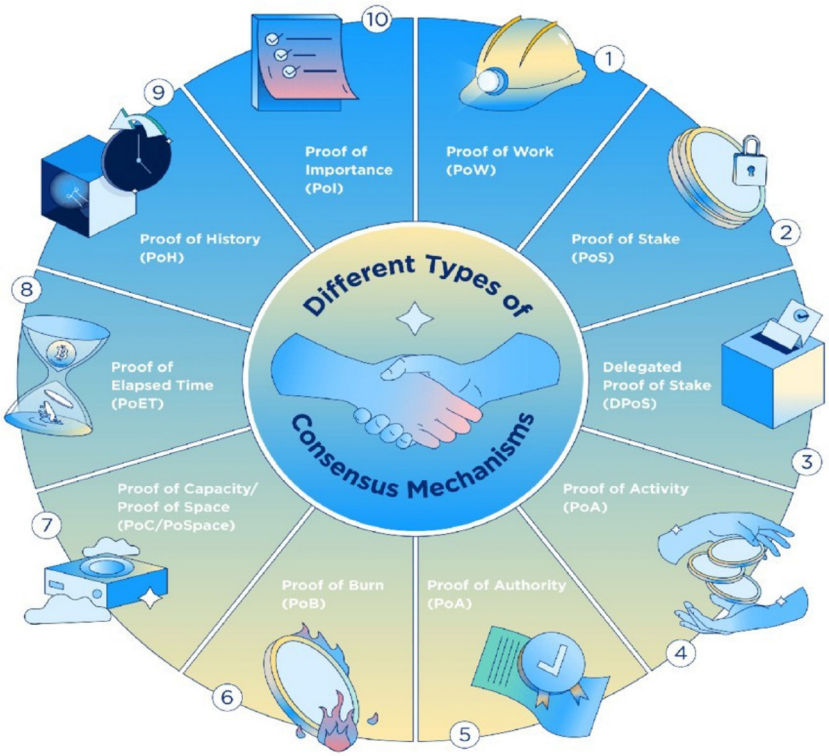

Fig 3 | Consensus mechanism the trade-offs among decentralization, scalability, and complexity
Source: Ussath (2016)[29]

control and scalability than public networks. Together, these systems enable increased secure data sharing, access control, and auditing without compromising the performance constraints of public blockchains.[30]

The security of smart contracts is a priority.[31] To prevent such vulnerabilities from being exploited by attackers, rigorous code reviews, formal verification, and continuous monitoring are required. Moreover, cryptographic key loss or compromise risks can be mitigated in part concerning careful key management strategies such as handling multi-signature wallets; they provide cryptographic assurances that a discrete number of secret keys are necessary to spend an entity's bitcoins.[32]

Decisions toward implementation should be guided by interoperability with existing cybersecurity tools. Blockchain should enhance, rather than displace, intrusion detection systems and endpoint protection platforms. While blockchain-based threat-intelligence-sharing platforms are gaining acceptance, their integration with standard systems can enhance situation awareness without the complete overhaul of the existing infrastructure.[33]

Conclusion

In the age of APTs, advanced cybersecurity strategies, which surpass traditional defense methods, are needed now. Being an inherently decentralized, immutable, and transparent technology, blockchain offers a compelling foundation on which to further enhance cybersecurity resilience against these complex threats. In this analysis, we have considered how blockchain-based solutions, such as decentralized threat intelligence sharing, secure identity management, and automated mitigation through smart contracts, can be harnessed toward building a better informed and more robust defense framework. Strong data integrity and trust come with blockchain's tamper-proof data storage and consensus-driven processes that make it harder for attackers to manipulate or erase forensic evidence. The particular importance of this capability is when stealthy intrusions that otherwise may evade detection for extended periods are present in the environment.

Blockchain technology presents itself as a powerful weapon in the fight against APTs and novel approaches to decentralized, tamper-proof, and collaborative cybersecurity. Nevertheless, for it to achieve its full potential, there will be a need for technological innovation, cooperative interdisciplinary research, and industry collaboration. Blockchain remains a demanding technology that needs to address current limitations and explore advanced development pathways, which will pave the way for the role of blockchain as a cornerstone of the next-generation cybersecurity framework to safeguard digital assets and critical infrastructure in the digital era.

Future Directions for Research and Development in Decentralized Cybersecurity

The potential of blockchain in cybersecurity is evident, but substantial research and technological advancements are still required to realize its full capabilities. One critical area for future exploration is the development of scalable consensus mechanisms that balance security, speed, and efficiency. Lightweight blockchain frameworks that reduce computational overhead without compromising security will be crucial for practical deployment in large-scale enterprise environments.

Another direction that has emerged as promising is putting AI into play with blockchain-based cybersecurity systems. With complex attack patterns and anomalies running the risk of getting missed during threat detection, AI algorithms can help, and blockchain can provide a safe, immutable log of AI-generated insights. Yet these technologies can be combined to form adaptive, autonomous defense systems that can evolve alongside continuously changing threat landscapes.

There is another huge area for research: privacy-preserving blockchain protocols. To comply with regulations and avoid exposing sensitive proprietary information, sharing sensitive threat intelligence data across multiple organizations necessitates strict privacy controls. Zero-knowledge proofs and homomorphic encryption may help secure data sharing while still hiding underlying details, making blockchain-based collaboration much more widely adopted.

References

1 Rahman Z, Yi X, Khalil I. Blockchain-based AI-enabled Industry 4.0 CPS protection against advanced persistent threat. IEEE Internet Things J. 2022;10(8):6769–78. Available from: https://ieeexplore.ieee.org/abstract/document/9695986
2 Alevizos L, Ta VT, Hashem Eiza M. Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review. Secur Priv. 2022;5(1):e191. Available from: https://onlinelibrary.wiley.com/doi/abs/10.1002/spy2.191

3 Saha B, Hasan MM, Anjum N, Tahora S, Siddika A, Shahriar H. Protecting the decentralized future: An exploration of common blockchain attacks and their countermeasures. arXiv preprint arXiv:2306.11884, 2023. Available from: https://arxiv.org/abs/2306.11884

4 Urien P. Innovative countermeasures to defeat cyber attacks against blockchain wallets. In 2021 5th Cyber Security in Networking Conference (CSNet) 2021;(pp. 49–54). Available from: https://ieeexplore.ieee.org/abstract/document/9614649

5 Al Amin MAR, Shetty S, Njilla L, Tosh DK, Kamhoua C. Hidden Markov model and cyber deception for the prevention of adversarial lateral movement. IEEE Access. 2021;9:49662–82. Available from: https://ieeexplore.ieee.org/abstract/document/9387290

6 Urien P. Innovative Countermeasures to Defeat Cyber Attacks Against Blockchain Wallets: A Crypto Terminal Use Case. Available from: https://ieeexplore.ieee.org/abstract/document/9614649

7 Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. Future Gener Comput Syst. 2018;82:395–411. Available from: https://www.sciencedirect.com/science/article/abs/pii/S0167739X17315765

8 Mutalib NHA, Sabri AQM, Wahab AWA, Abdullah ERMF, AlDahoul N. Explainable deep learning approach for advanced persistent threats (APTs) detection in cybersecurity: A review. Artif Intell Rev. 2024;57(11):1–47. Available from: https://link.springer.com/article/10.1007/s10462-024-10890-4

9 Madine M, Salah K, Jayaraman R, Al-Hammadi Y, Arshad J, Yaqoob I. App chain: Application-level interoperability for blockchain networks. IEEE Access. 2021;9:87777–91. Available from: https://ieeexplore.ieee.org/abstract/document/9455384

10 Gohar AN, Abdelmawgoud SA, Farhan MS. A patient-centric healthcare framework reference architecture for better semantic interoperability based on blockchain, cloud, and IoT. IEEE Access. 2022;10:92137–57. Available from: https://ieeexplore.ieee.org/abstract/document/9869824

11 Villarreal ERD, García-Alonso J, Moguel E, Alegría JAH. Blockchain for healthcare management systems: A survey on interoperability and security. IEEE Access. 2023;11:5629–52. Available from: https://ieeexplore.ieee.org/abstract/document/10015729

12 Sonkamble RG, Phansalkar SP, Potdar VM, Bongale AM. Survey of interoperability in electronic health records management and proposed blockchain-based framework: MyBlockEHR. IEEE Access. 2021;9:158367–401. Available from: https://ieeexplore.ieee.org/abstract/document/9620075

13 Shravan M, Sanjay HA, Shastry KA, Hemant V, Laxman K. Interoperability in blockchain-based healthcare. In 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon) 2022;(pp. 1–7). Available from: https://ieeexplore.ieee.org/abstract/document/9972496

14 Six N, Herbaut N, Salinesi C. Blockchain software patterns for the design of decentralized applications: A systematic literature review. Blockchain Res Appl. 2022;3(2):100061. Available from: https://www.sciencedirect.com/science/article/pii/S209672092200001X

15 Huynh TT, Nguyen TD, Tan H. A survey on security and privacy issues of blockchain technology. In 2019 International Conference on System Science and Engineering (ICSSE) 2019;(pp. 362–7). Available from: https://ieeexplore.ieee.org/abstract/document/8823094

16 High M. Supply chain insight: Inside IBM's Food Trust Blockchain system. Supply Chain Magazine 2020. Available from: https://supplychaindigital.com/technology/supply-chain-insight-inside-ibms-food-trust-blockchain-system

17 Mekdad Y, Aris A, Babun L, El Fergougui A, Conti M, Lazzeretti R, et al. A survey on security and privacy issues of UAVs. Comput Netw. 2023;224:109626. Available from: https://www.sciencedirect.com/science/article/abs/pii/S1389128623000713

18 Guo H, Yu X. A survey on blockchain technology and its security. Blockchain Res Appl. 2022;3(2):100067. Available from: https://www.sciencedirect.com/science/article/pii/S2096720922000070

19 Bhutta MNM, Khwaja AA, Nadeem A, Ahmad HF, Khan MK, Hanif MA, et al. A survey on blockchain technology: Evolution, architecture and security. IEEE Access. 2021;9:61048–73. Available from: https://ieeexplore.ieee.org/abstract/document/9402747

20 Fonseca M. Threat Intelligence Lifecycle: Definition, Explanation, Examples. Silobreaker. 2024. Available from: https://www.silobreaker.com/glossary/threat-intelligence-lifecycle/

21 Alshamrani A, Myneni S, Chowdhary A, Huang D. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Commun Surv Tutor. 2019;21(2):1851–77. Available from: https://ieeexplore.ieee.org/abstract/document/8606252

22 Sharma A, Gupta BB, Singh AK, Saraswat VK. Advanced persistent threats (APT): Evolution, anatomy, attribution and countermeasures. J Ambient Intell Hum Comput. 2023;14(7):9355–81. Available from: https://link.springer.com/article/10.1007/s12652-023-04603-y

23 Bhardwaj R, Kumar N, Kour H, Verma N, Ashish A. Analysis of advanced persistent threat attacks, lifecycle, and counter measures: A comprehensive review. In Proceedings of International Conference on Recent Innovations Computing 2023;(pp. 143–53). Springer. Available from: https://link.springer.com/chapter/10.1007/978-981-97-7862-1_10

24 Mirza NAS, Abbas H, Khan FA, Al Muhtadi J. Anticipating Advanced Persistent Threat (APT) countermeasures using collaborative security mechanisms. In Proceedings of International Symposium on Biometrics Security Technology (ISBAST) 2014;(pp. 129–32). Available from: https://ieeexplore.ieee.org/abstract/document/7013108/

25 Malik V, Khanna A, Sharma N. Advanced persistent threats (APTs): Detection techniques and mitigation strategies. In International Journal of Global Innovations Solutions (IJGIS) 2024. Available from: https://ijgis.pubpub.org/pub/44fxb30l/release/1

26 Niakanlahiji A, Wei J, Chu BT. A natural language processing based trend analysis of advanced persistent threat techniques. In Proceedings of IEEE International Conference Big Data (Big Data) 2018;(pp. 2995–3000). Available from: https://ieeexplore.ieee.org/abstract/document/8622255

27 Mourtzis D, Angelopoulos J, Panopoulos N. Blockchain integration in the era of industrial metaverse. Appl Sci. 2023;13(3):1353. Available from: https://www.researchgate.net/publication/367324333_Blockchain_Integration_in_the_Era_of_Industrial_Metaverse

28 Buchta R, Gkoktsis G, Heine F, Kleiner C. Advanced persistent threat attack detection systems: A review of approaches, challenges, and trends. Digit Threats Res Pract. 2024;5(4):1–37. Available from: https://dl.acm.org/doi/full/10.1145/3696014

29 Ussath M, Jaeger D, Cheng F, Meinel C. Advanced persistent threats: Behind the scenes. In Proceedings of Annual Conference on Information Science Systems (CISS) 2016;(pp. 181–6). Available from: https://ieeexplore.ieee.org/abstract/document/7460498

30 Jabar T, Singh MM. Exploration of mobile device behaviour for mitigating advanced persistent threats (APT): A systematic literature review and conceptual framework. Sensors. 2022;22(13):4662. Available from: https://www.mdpi.com/1424-8220/22/13/4662

31 Khaleefa EJ, Abdulah DA. Concept and difficulties of advanced persistent threats (APT): Survey. Int J Nonlinear Anal Appl. 2022;13(1):4037–52. Available from: https://ijnaa.semnan.ac.ir/article_6230.html

32 Hejase HJ, Fayyad-Kazan HF, Moukadem I. Advanced persistent threats (APT): An awareness review. J Econ Econ Educ Res. 2020;21(6):1–8. Available from: https://www.researchgate.net/publication/347948987

33 Khalid MNA, Al-Kadhimi AA, Singh MM. Recent developments in game-theory approaches for the detection and defence against advanced persistent threats (APTs): A systematic review. Mathematics. 2023;11(6):1353. Available from: https://www.mdpi.com/2227-7390/11/6/1353