Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 5, 2025

OPTIMIZING CYBERSECURITY PERFORMANCE: A PERFORMANCE-BASED ANALYSIS OF BLOCKCHAIN AND TRADITIONAL SECURITY ARCHITECTURES

Muhammad Moazam[*1], Dr Jawaid Iqbal[2], Samarah Ashraf[3], Dr Mairaj Nabi[4]

[*1]*MS Scholar, Riphah International University, Islamabad, Pakistan*
[2]*Assistant Professor, Riphah International University, Islamabad, Pakistan*
[3]*Independent Scholar, Pakistan*
[4]*Associate Professor, Shaheed Benazir Bhutto University, Shaheed Benazirabad, Pakistan*

[*1]moazomsaimgujjar@gmail.com, [2]jawaid.iqbal@riphah.edu.pk, [3]samra.leads@yahoo.com, [4]mairaj_bhatti@yahoo.com

DOI: https://doi.org/10.5281/zenodo.15541642

Keywords
Cyber Security Performance, Traditional Security, Blockchain Security, Enterprise blockchain adoption, Regression Analysis.

Article History
Received on 21 April 2025
Accepted on 21 May 2025
Published on 29 May 2025

Corresponding Author: * Muhammad Moazam

Abstract

A quantitative benchmarking analysis of traditional versus blockchain-based cybersecurity solutions using a comparative holistic performance assessment approach was presented in this study. This research creates parallel testbeds where baseline security infrastructure consisting of a FortiGate firewall, Microsoft PKI, Splunk SIEM, and OpenVPN forms a traditional ecosystem, while Hyperledger Fabric, Ethereum, IPFS, and MetaMask set up the blockchain ecosystem. The evaluation encompassed latency (end-to-end transaction time), cost (3-year total cost of ownership), and attack resistance (threat simulated success rates). Six standardized test scenarios were conducted which included user login (10,000 simultaneous engagements), DDoS attack simulation (100Gbps), and logging (100,000 entries), with a 30 cycle test repetition for significant statistical confidence (ANOVA, α=0.05). Key trade-offs surfaced as findings blockchains showed commanding resistance to tampering with logs (0% alteration compared to 14.2% in traditional systems) while also possessing lower performance. Black systems exhibited higher latency (47.3seconds vs. 4.2 seconds for authentication) and 3-5x greater implementation costs. A hybrid decision framework developed from the research combines five performance dimensions: security, cost, speed, scalability, and compliance mapped to organizational profiles including SMB's, enterprises and government, providing clear guidance for security architects. This research clarifies many of the operational claims and assumptions purported by the blockchain heralds, showcasing the practical realities applicable for modernization strategies in cybersecurity.

INTRODUCTION

To keep pace with the quickly evolving cyber threats, it is important to advance security mechanisms, which has led to the development of new strategies outside the boundaries of traditional cybersecurity for organizational exploration. Defense systems have traditionally relied on firewalls, Public Key Infrastructure (PKI), Intrusion Detection Systems (IDS), and centralized authentication protocolsThese systems, however, face immense challenges from operational shortcomings, encapsulated as single

points of failures, vulnerability to local attackers, and overreliance on trusted third parties (Zargar et al., 2021; Yang et al., 2022). The ever growing concern over centralized cyber security mechanisms has faced major scrutiny due to the SolarWinds data breach in 2020 and Colonial Pipeline ransomware attack in 2021, where organizations sustained monetary losses, reputational damage, and were imposed with regulatory fines (Kshetri, 2022). Relying on traditional cybersecurity will further exacerbate these issues, of which blockchain technology seeks to mitigate by providing decentralized trust, cryptographically secured immutability, alongside timestamping transactions in a way that renders them impossible to alter (Zheng et al., 2020; Guo, 2022; Shirimalo and Patel, 2022). Although promising, the integration of blockchain into cyber security infrastructures still remains scarce due to unresolved issues of "latency, operational costs, and scalability" (Warkentin & Ormond, 2022; Bilal et al., 2022).

The security benefits of Blockchain arise from its Distributed Ledger Technology (DLT), which removes trust on a central authority by using a consensus mechanism such as Proof of Work (PoW) or Proof of Stake (PoS) (Nakamoto, 2008). As Mohanta et al (2019) highlighted, this makes blockchain useful where "data integrity, secure identity management, and auditability" are needed, like in supply chain management, healthcare, and decentralized finance (DeFi) . However, blockchain technology also offers certain drawbacks such as slower speeds in transactions due to the time needed to reach a consensus. For example, Bitcoin processes approximately 7 (TPS) while Visa averages 24,000 TPS, resulting in sluggish speeds (Tschorsch & Scheuermann, 2016). While resistant to tampering of the traditional sense, blockchains are still vulnerable to "51% attacks, Sybil attacks, and smart contract exploits" (Atzei et al., 2017; Samreen and Alalfi, 2021). The expense and resources necessary to implement blockchain
such as energy-intensive mining in PoW systems—further complicate its adoption (Vranken, 2017). The existing comparisons of traditional with blockchain-based cybersecurity measures have predominantly been 'qualitative' concentrating on theoretical gains rather than measurable benchmarks of performance.

Another example, some studies have emphasized blockchain's capability of reducing "Distributed Denial-of-Service (DDoS) attacks" through the decentralization of Domain Name System (DNS) Dorri et al (2017) and Arif et al., (2020) but none seem to evaluate how cost efficient it is or its latency compared to cloud-based DDoS protection services like the AWS Shield. Along the same lines, while self-sovereign identity SSI systems promise enhanced privacy Azaria et al, (2018) and Huang et al., (2019) resolve concerning barriers to usage and adoption. Addressing these gaps is essential to establish whether security features of blockchains nullify the operational burdens of blockchain technology in the considered context. In addition, examining "industry perceptions" using expert interviews can highlight regulatory ambiguity, interoperability challenges, and skill gap deficiencies as primary barriers to adoption (Warkentin & Ormond, 2022).

The purpose of this paper is to respond to the three central research questions (RQ). In the first place, RQ1 looks at the traditional security of information systems and the blockchain approaches investigating what latency, cost, and resistances to attacks they offer, issuing empirical standards for decisions.

Secondly, RQ2 examines the potential for blockchain solutions to exceed benchmarks set by, or act as a complement to, traditional methods, providing insights into optimal use case scenarios. In answering these questions, the study pursues three research objectives (ROs) which are: (1) executing performance benchmarking to capture metric quantification across paradigms and measuring defined performance metrics and (2) formulating an enterprise decision-making framework on model selection and hybrid security model implementation. The main contribution of this research stems from its robust data-driven approach which applies theory rationales focused on blockchain advantages on the gap devoid of real-world applicability. The analysis will add policy decision materials, imperative to the IT and security architectural community abolishing uninformed sequencing, positioned where the integration of blockchain in cybersecurity methodologies yields substantial value.

1. Literature Review

The rise of digital systems gives a basis for the changing landscape of the field of cybersecurity. Organizational system security strategies have been dominated for decades by traditional approaches rooted in central architectures (Stallings, 2021). These systems use perimeter bases of defenses such as firewalls, intrusion detection systems (IDS), and public key infrastructure (PKI) to protect their digital assets. While effective against conventional threats, these models demonstrate critical vulnerabilities when faced with sophisticated attacks targeting their centralized system (Zargar et al., 2021).

Centralized systems weaknesses were strikingly brought to the foreground during the high-profile security breach of traditionally secured systems. One of the classical cases is the Equifax breach of 2017, where sensitive data of 147 million individuals was exposed. Equifax laid bare the potential risks of centralized data repositories (Goodin, 2017; Lehto, 2022). Another incident is the SolarWinds attack in 2020, which showed how central supply chain instantiates centralized update systems and vitiates thousands of organizations (Krebs, 2023; Griewing et al., 2022). These hackers have encouraged security experts to seek decentralized alternatives, especially blockchain technology, which has built in resistances to many attack vectors exploiting centralized systems (Nakamoto, 2008).

Credentials establishing Blockchain as a solution to security issues stem from its core identity factors like centralized system. The technology is regarded as offering decentralization, supports cryptographic hashing, and enables consensus validation (Zheng et al., 2020).

These attributes solve a number of shortcomings that are characteristics of conventional systems. For example, blockchain's distributed ledger technology removes single points of failure, thus making systems encounter lesser DDoS attacks (Dorri et al., 2017). The technology's immutability guarantees data integrity while also ensuring reliable audit trails which are critical in finance and healthcare (Azaria et al., 2016).

Numerous researches are suggestive of blockchain being useful in selective security domains. For example, Mohanta et al. (2019) demonstrated the application of blockchain technology to secure IoT networks by decentralizing device authentication. As with Kshetri (2020) also described the possibility of implementing blockchain technology for forming systems capable of preventing modifications for intellectual property protection. However, these works highlight important obstacles such as impractical feasibility, technological limits, and the consumption of energy resources that may obstruct adoption.

Although the security benefits associated with blockchain technology are noteworthy, its adoption is impeded by a number of challenges. Additionally, there are gaps regarding performance in blockchain and conventional systems. In comparison to conventional payment systems, public blockchains like Ethereum are much slower; for example, Ethereum is only capable of processing 15-30 transactions per second, while Visa can serve 24,000 transactions per second (Tschorsch & Scheuermann, 2016). The energy consumption of proof of work consensus mechanisms, particularly for Bitcoin which utilizes more energy than some small countries, is also a point of concern (Vranken, 2017).

Furthermore, concerns related to security strategies incorporated into blockchain systems also arose. Atzei et al. (2017) detailed smart contracts vulnerabilities, like reentrancy attacks from the notorious DAO hack. Moreover, blockchain networks are still susceptible to 51% attacks, where malicious users take control of the majority of the network's hashing power (Bano et al., 2019; Xu et al., 2023; Hussein et al., 2023; Singh et al., 2023). Warkentin and Ormond (2022) highlights these problems, along with organizational issues such as regulatory ambiguity and a lack of skilled personnel, as main reasons of enterprise reluctance to embracing new technologies.

Recent studies look into the new hybrid models which integrate blockchain and other conventional security frameworks. Axon (2015) put forward PKI systems with blockchain-based security which kept the standard authentication mechanisms and utilized blockchain for certificate visibility. Likewise, Zargar et al. (2021) looked into hybrid DDoS protection models with blockchain-based coordination and cloud-based traffic-free filtering.

New developments show an increasing attention toward the use of permissioned blockchains for

enterprise security applications. These systems incorporate blockchain technology and 'permit' controlled access to address performance and privacy concerns via alternative consensus mechanisms (Androulaki et al., 2018; Gorenflo et al., 2020; Marchesi et al., 2022). Even so, as Kshetri (2022) points out, the domain is still void with a comprehensive empirical analysis that quantifies the trade-offs of different approaches with varying organizational contexts and multiplex use cases.

These literature gaps have been addressed by this study. First, as countless studies focus on the theoretical security benefits of blockchain, very few offer empirical evaluations of performance metrics against other systems. Second, there is an absence of comprehensive frameworks for technology selection as most research is application centric. Lastly,

The impact of organizational elements on the implementation and efficacy of these security paradigms is not well understood.

The knowledge gap is addressed in this study by presenting quantitative comparisons of the security, performance, and cost attributes with the associated model while also exploring adoption barriers through expert perspectives. This work seeks to create actionable recommendations for security architects and organizational leaders when considering the evaluation of the technologies.

2. Research Methodology

The study utilizes a quantitative research design which investigate the performance benchmarking to explore the difference between classical cybersecurity systems and blockchain-based systems. The methodology is organized into three systemically designed steps, each intended to answer particular research questions in a methodologically sound manner.

The quantitative performance benchmarking, we established two parallel test environments to enable direct comparison. The traditional security environment was configured with industry-standard components including a FortiGate 100F firewall for network protection, Microsoft PKI infrastructure running on Windows Server 2022 for authentication, Splunk Enterprise (Version 8.2) for security information and event management, and an OpenVPN access server (Version 2.11) for secure remote access. The blockchain environment was implemented using Hyperledger Fabric (v2.5) for enterprise use cases, Ethereum (Geth v1.12) for public blockchain simulation, IPFS (v0.19) for decentralized storage solutions, and MetaMask (v10.28) for identity management. We operationalized three critical performance dimensions across these environments: latency (measured as end-to-end transaction processing time using Wireshark and custom Python scripts), cost (calculating total cost of ownership over 3 years incorporating hardware, energy, and labor expenses through AWS Pricing Calculator and NREL's System Advisor Model), and attack resistance (evaluating success rates of simulated attacks using tools like Metasploit, Ganache, and Truffle).

Six standardized test scenarios were executed in both environments under controlled conditions: user authentication (simulating 10,000 concurrent requests), data integrity verification (using a 1GB dataset), DDoS mitigation (against 100Gbps attack simulations), tamper-evident logging (processing 100,000 log entries), cross-domain access control, and security patch distribution. Each test scenario was repeated 30 times to ensure statistical reliability, with results analyzed using ANOVA, regression, and other analysis in SPSS (α=0.05) to determine significant differences between the traditional and blockchain approaches. This robust experimental design allows for direct and quantifiable comparison of the two security paradigms across multiple operational dimensions. We measured three key dimensions with the following operationalization:

Table 1: Operational dimensions of security paradigms

Metric	Measurement Approach	Tool Used
Latency	End-to-end transaction processing time	Wireshark custom python scriptsa
Cost	TCO over 3 years (hardware, energy, labor)	AWS pricing calculator, NREL's SAM
Attack Resistance	Success rates of simulated attack	Metasploit, Ganache, Truffle

3. Analysis of Quantitative Performance Benchmarking

Table 2: ANOVA Table for Latency Comparison

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	8924.72	5	1784.93	38.73	.000
Within Groups	7982.15	27	1.896		
Total	16905.88	174			

Groups: Traditional PKI, Hyperledger Fabric, Ethereum (PoW) × 2 test scenarios (Authentication, DDoS mitigation).

The ANOVA table regarding latency performance evaluation of the Traditional PKI, Hyperledger Fabric and Ethereum (PoW) systems, given two test scenarios (authentication and DDoS mitigation), is below. One-way Analysis of Variance (ANOVA) has been used in this test to determine whether there are any statistically significant differences in the mean latency time among the systems. The F-statistic of 38.73 ($p = .000$) indicates moderate to high significance, meaning there is substantial variation between groups compared to within-group variation. With between-group sum of squares corresponding to 52.8% of total variance (8,924.72/16,905.88), the analysis implies that system type and scenario considerably influence latency performance. Evidence shows that implementations of blockchain technology, especially those with Ethereum's PoW systems, increase latency significantly more than traditional ones, which supports the findings. The p-value, being extremely low (less than .001), strongly disproves the null hypothesis on equal performance across systems, thus warranting further post hoc testing to find specific pairwise differences. The analysis presented strengthens the study's overall assertion that while the blockchain provides undeniable benefits such as increased security warranting through tamper resistance, it does incur major latency drawbacks which must be considered when deciding architecture in cybersecurity. The caution reported on using PoW blockchains in latency-sensitive applications may also suggest the reconsideration of employing more efficient counterparts like Hyperledger Fabric for some enterprise use cases.

Table 3: Post Hoc Tests (Tukey HSD):

Comparison	Mean Difference (ms)	95% CI	p-value
Traditional PKI vs. Hyperledger	-8.60	[-10.2, -7.0]	<0.001***
Traditional PKI vs. Ethereum	-43.10	[-44.7, -41.5]	<0.001***
Hyperledger vs. Ethereum	-34.50	[-36.1, -32.9]	<0.001***

As part of the post hoc analysis for the ANOVA, the Tukey HSD tests were applied to determine where specific pairwise differences lay with respect to latency performance among the three selected cyber security systems. These tests offer an understanding of how each system compares against the others and where each system stands.

For the Traditional PKI and Hyperledger Fabric comparison, the mean difference in latency was -8.60 ms (95% CI [-10.2, -7.0], $p < 0.001$) which implies that, on average, Traditional PKI was significantly more efficient than Hyperledger Fabric. This marked disparity ($p < 0.001$) also demonstrates the performance penalty Hyperledger suffers due to its consensus mechanism, although it is still more efficient than PoW based systems.

The greatest difference was noted with Traditional PKI and Ethereum, where Traditional PKI showed a remarkable 43.10 ms advantage (95% CI [-44.7, -41.5], $p < 0.001$). This massive difference in latency ($p < 0.001$) signals the deep performance drawbacks inflicted by Ethereum's Proof-of-Work (PoW) consensus on cybersecurity functions, where time-sensitive speed is frequently essential.

Regarding the comparison of Hyperledger Fabric and Ethereum, the former had a 34.50 ms advantage over the latter (95% CI [-36.1, -32.9], $p < 0.001$). Although still significant, this difference – smaller,

yet still substantial – shows that enterprise-optimized blockchains like Hyperledger can alleviate some, but not all, of the performance losses associated with decentralized frameworks.

All comparisons were corroborated with statistically significant results ($p < 0.001$) where confidence intervals did not overlap, strongly supporting the argument that:

1. Centrally controlled systems outperform their peers in latency-sensitive scenarios.
2. Among blockchain alternatives, enterprise platforms (Hyperledger) outperform public chains (Ethereum).
3. The ranking of performance is as follows: Traditional PKI > Hyperledger > Ethereum.

These findings corroborate the study's recommendation to claim blockchain should be reserved for use in applications where security benefits justify performance costs. It also advocates for enterprise blockchains when a decentralized system architecture is unavoidable. The results warn, especially, against using PoW-based systems like Ethereum in situations needing rapid low-latency responses.

Table 4: Descriptive Statistics of Latency Performance (in milliseconds)

System	Test Scenario	Mean	SD	Median	Min	Max	IQR	95% CI	Skewness	Kurtosis
Traditional PKI	Authentication	4.2	0.3	4.1	3.8	4.6	0.4	[4.1, 4.3]	0.12	-0.45
	DDoS Mitigation	5.3	0.4	5.2	4.7	5.9	0.5	[5.1, 5.5]	0.08	-0.32
Hyperledger Fabric	Authentication	12.8	1.1	12.6	10.9	14.7	1.8	[12.3, 13.3]	0.21	0.67
	DDoS Mitigation	11.5	1.0	11.3	9.8	13.6	1.6	[11.0, 12.0]	0.18	0.54
Ethereum (PoW)	Authentication	47.3	3.6	46.8	40.1	53.9	5.1	[45.8, 48.8]	0.45*	1.12*
	DDoS Mitigation	44.2	3.3	43.7	38.5	50.2	4.8	[42.9, 45.5]	0.39*	0.98*

The table containing the descriptive statistics encapsulates the side-by-side comparison of latency performance across the three cybersecurity systems, which include: Traditional PKI, Hyperledger Fabric, and Ethereum (PoW), in the context of authentication and DDoS mitigation. Traditional PKI outperformed the other systems with extremely low latency of 4.2 ms and 5.3 ms for authentication and DDoS mitigation, respectively, along with very low variability (SD = 0.3-0.4, IQR = 0.4-0.5), which supports its use in critical, time sensitive operations. Hyperledger Fabric performed reasonably well with moderate latency, 12.8 ms for authentication and 11.5 ms for DDoS mitigation, as well as acceptable variability (SD = 1.0-1.1, IQR = 1.6-1.8), which indicates that it may be an appropriate solution for enterprises that need auditability. In stark contrast, Ethereum's PoW implementation had extremely high latency with mean values of 47.3 ms for authentication and 44.2 ms for DDoS mitigation, along with high variability (SD = 3.3-3.6, IQR = 4.8-5.1), which makes it unsuitable for tasks that require prompt execution.

The patterns discovered in the data are noteworthy with respect to the discerning of system performance. Response times appear to be consistent, as traditional PKI systems are predictable with respect to their functionality, given the tight confidence intervals (e.g., [4.1, 4.3] for authentication) along with the nearly symmetrical distribution, skewness ≈ 0.1). Though slower than traditional systems, Hyperledger Fabric showed improved performance during DDoS Mitigation compared to authentication, which indicates its consensus mechanism may be tailored for burst traffic. Ethereum struggles with achieving performance targets the most, as the high skewness (0.39 - 0.45) along with the high kurtosis (0.98-1.12) showcase the frequent extreme values of latency that would negatively affect any deployment ecosystem.

This serves as an important finding related to the selection of a cybersecurity system. The performance hierarchy is sufficient enough to prove that traditional PKI systems outperform Hyperledger Fabric systems, which in turn perform better than Ethereum (PoW). This goes to show that although blockchain solutions present possible benefits in

security, the disadvantages of latency have to be thought through. It seems that enterprise implementations like Hyper Ledger may serve certain applications well, unlike PoW based systems such as Ethereum, which are placed in unsuitable positions for latency-sensitive cybersecurity frameworks. These findings serve as guidance for determining the security performance and decentralization balance in organizational cybersecurity architectures.

Table 5: Power-law Regression Analysis of Blockchain Transaction Latency

Parameter	Estimate	Std. Error	t-value	p-value	95% CI
Exponent (α)	1.83	0.07	25.0	<0.001***	[1.68, 1.96]
Coefficient (β)	0.14	0.01	16.0	<0.001***	[0.13, 0.17]
R^2	0.92	-	-	-	-
Adjusted R^2	0.90	-	-	-	-
F-statistic	675.0	(df = 1, 48)	-	<0.001***	-

For the power-law regression of the blockchain transaction latency, there exists a mathematically precise link between the volume of transactions and responsiveness of the system described by Latency = $0.14 \times \text{Transactions}^{1.83}$. This model guarantees an outstanding fit ($R^2 = 0.92$, F-statistic = 675, $p < 0.001$), validating that blockchain systems fundamentally scale in a different manner than traditional cybersecurity architectures. The exponent indicating super linearity ($\alpha = 1.83$) supports the thesis of increasing latency at a rate disproportionately stronger than that of transaction growth; in this case, each doubling of transactions causes about a 3.54 times increase in response time ($2^{1.83} \approx 3.54$). This explanation of non-linear response scaling provides an understanding of the drastic performance deterioration that blockchain systems experience under load, which increases latency from ~25ms at 1000 transactions to over 8 seconds at 100,000. The coefficient of high significance ($\beta = 0.14$, $p < 0.001$) strengthens the argument that fundamental architectural latency 'costs' are present for blockchains even under low transaction volumes. Parameter estimates with restrictive confidence intervals ([1.68,1.96] for α; [0.13,0.17] for β) make these results highly reliable. We quantitatively illustrate that the security benefits of decentralization within blockchain come precluded with considerable disadvantages in scalable performance, firmly reaffirming the necessity for new architectural advances, such as layer-2 solutions, called upon for easing the burden for performance-critical latency applications in cybersecurity.

As mentioned earlier, the power law is useful in helping system designers estimating performance requirements and resource planning in the context of security implementations using blockchain technology.

Table 6: Linear Regression Analysis of System Performance

Parameter	Traditional Systems	Blockchain Systems	Comparison
Response Variable	Latency (ms)	Latency (ms)	Cost (3-year TCO, $K)
Predictor	Transaction Volume	Transaction Volume	Security Level (1-10)
Model Type	Linear	Power-law	Linear
R^2	0.99	0.93	0.88
Adjusted R^2	0.99	0.92	0.87
Intercept (β_0)	4.1*** (SE=0.1)	0.15*** (SE=0.01)	85.2*** (SE=2.3)
Slope (β_1)	0.001*** (SE=0.0001)	1.82*** (SE=0.07)^α	12.4*** (SE=0.8)
F-statistic	F(1,58)=9800, p<0.001	F(1,48)=676, p<0.001	F(1,28)=240, p<0.001
Residual Std. Error	0.2 ms	3.1 ms	$8.7K
Normality (Shapiro-Wilk)	W=0.98, p=0.34	W=0.97, p=0.12	W=0.96, p=0.08

Heteroskedasticity	BP χ^2=1.2, p=0.27	BP χ^2=2.1, p=0.15	BP χ^2=1.8, p=0.18

***p<0.001; ^αExponent for power-law*

The linear regression analysis gives an exhaustive evaluation relating the performance attributes of traditional and blockchain-based cybersecurity systems in terms of latency, scalability, and cost efficiency. For classical systems, the linear model (Latency = 4.1 + 0.001×Transactions) is almost perfectly predictable (R^2 = 0.99). Their performance is remarkably stable with near-zero residual error (0.2ms) and flat slope (β_1 = 0.001ms per transaction). This suggests that classical architectures have predictable and low latency operating conditions compared to transaction volume. In sharp contrast, blockchain systems exhibit a power-law scaling characteristic in which latency is considerably more sensitive to increased workload (Latency = $0.15\times\text{Transactions}^{1.82}$) demonstrating significantly lower predictability (R^2 = 0.93) which results in greater residual error (3.1ms) reflecting the uncontrollable chaos of decentralized consensus algorithms.

The linear model (TCO = 85.2 + 12.4× Security Level) encapsulated by the cost analysis yields no less significant insights. Cost remains a major factor, with security performance in blockchain systems exhibiting stronger prominence (shown in the slope of $12.4K per security level compared to $8.3K for traditional systems) but at significantly higher base costs ($85.2K for traditional versus $412.5K for blockchain). All models reveal explosive levels of statistical significance, p less than 0.001, alongside all major regression assumptions, surviving normality (Shapiro-Wilk p > .05) and heteroscedasticity (Breusch-Pagan p > .10) tests. With these results, one can visualize the deep trade-off difference stemming from the architectural approaches: the traditional system meets needs for classic security with reasonably complex and economically efficient processes. In contrast, blockchains offer robust security but incur severe unpredictability—especially under high load operational stress. The models allow decision-making based on defined performance needs and budget limits, which promotes optimal cost allocation.

Table 7: Independent Samples T-Test Results

Comparison	Mean (Traditional)	Mean (Blockchain)	Mean Difference	t-value	df	p-value	Cohen's d	95% CI
Latency (ms)	4.2	47.3	-43.1	-38.2	58	<0.001***	4.72	[-45.7, -40.5]
DDoS Mitigation Success Rate (%)	98.7	72.3	+26.4	21.6	58	<0.001***	3.14	[24.1, 28.7]
Cost (3-year TCO, $K)	674	1,112	-438	-9.8	28	<0.001***	1.87	[-512, -364]
Energy Use (kWh/1k transactions)	0.03	18.7	-18.67	-45.3	28	<0.001***	8.91	[-19.2, -18.1]
Tamper Resistance (Success Rate)	14.2%*	0%	+14.2%	6.4	28	<0.001***	1.32	[9.8%, 18.6%]

The independent samples t-test results indicate that there is a significant difference between traditional and blockchain-based cybersecurity systems in all system performance metrics assessed (p < 0.001). The analysis indicates that blockchain architectures have a significantly greater mean latency (mean difference = -43.1ms, t = -38.2, d = 4.72), which validates their performance for time-sensitive operations. Although there is greater resistance to tampering in blockchain systems (0% versus 14.2% success for traditional systems, t = 6.4, d = 1.32), they perform worse for DDoS mitigation (26.4% lower success rate, t = 21.6, d = 3.14), revealing an important security vulnerability.

The cost analysis provides evidence of significant economic drawbacks for blockchain, indicating a 3-year total cost of ownership (mean difference = -$438K, t = -9.8, d = 1.87) and energy consumption (623× higher at 18.7 kWh/1k transactions versus 0.03 kWh, t = -45.3, d = 8.91) that are 65% higher.

All these large effect sizes (Cohen's d > 0.8) show that the differences are not only statistically significant but also practically significant. The narrow 95% confidence intervals (for example, [-45.7, -40.5] for latency) further validate these findings.

These results taken together show that although blockchain possesses idealistic theoretical claims, such as providing perfect tamper resistance, the actual security considerations come with real world tradeoffs in performance, cost effectiveness, and energy efficiency. The effect sizes which are particularly large for latency (d = 4.72) and energy use (d = 8.91) suggest that these are more patterns of systemic issues, instead of implementation faults, with current paradigms of blockchain architecture. These results ought to caution organizations against blindly adopting blockchain enabled solutions as they need to carefully assess whether its touted security gains are worth the operational costs for their contexts, especially when considering applications with high throughput requirements or sensitivity to latency.

1. Latency Performance Analysis The latency measurements revealed significant disparities between traditional and blockchainbased systems across all test scenarios ($F(5,174) = 38.72$, $p < 0.001$). Authentication processes demonstrated the most pronounced difference, with traditional PKI completing 10,000 authentications in 4.2 seconds (SD = 0.3), while Hyperledger Fabric required 12.8 seconds (SD = 1.1) for equivalent operations. The Ethereum implementation showed even greater latency at 47.3 seconds (SD = 3.6) due to PoW consensus delays. Transaction processing times followed a power-law distribution in blockchain systems ($R^2 = 0.93$), while traditional systems maintained consistent linear performance ($R^2 = 0.99$). This suggests blockchain latency becomes increasingly unpredictable at scale, particularly evident during the DDoS mitigation test where traditional systems processed 98.7% of requests within 50ms servicelevel agreements (SLAs), compared to blockchain's 72.3% compliance rate. Cost Structure Comparison The total cost of ownership (TCO) analysis over 36 months revealed complex trade-offs (Table 1). While blockchain solutions showed 28-42% lower ongoing operational costs, their initial deployment expenses were 3-5× higher than traditional setups. Energy consumption emerged as the most significant differentiator, with PoW implementations consuming 18.7 kWh per 1,000 transactions versus 0.03 kWh for traditional systems.

Table 8: Three-Year TCO Comparison (USD thousands)

Cost Component	Traditional	Hyperledger	Ethereum
Initial Deployment	85.20	320.70	412.50
Personnel	450	380	420
Energy	18.30	25.10	187.40
Maintenance	120.50	85.20	92.70
Total	674	811	1112.60

The break-even point occurred at month 28 for Hyperledger implementations, suggesting blockchain becomes cost-effective only for long-term deployments. Sensitivity analysis showed energy prices and personnel expertise were the most volatile cost drivers ($\beta = 0.67$ and 0.53 respectively). 3. Attack Resistance Evaluation The simulated attack tests produced non-parametric results requiring Mann-Whitney U analysis ($p < 0.01$ for all comparisons). Traditional systems demonstrated superior resistance to volumetric attacks (DDoS success rate: 3.2% vs 11.7% in blockchain), while blockchain showed stronger defense against data tampering (0% vs 8.4% modification success)

Notably, smart contract vulnerabilities accounted for 68% of successful blockchain breaches, primarily: - Reentrancy attacks (22% success rate) - Integer overflow/underflow (17%) - Access control violations (29%) The blockchain's cryptographic immutability proved particularly effective against forensic attacks, with 0% success in log tampering attempts versus 14.2% in traditional systems. However, its decentralized nature increased susceptibility to Sybil attacks (23.5% success rate vs 2.1% in centralized

systems). 4. Hybrid Performance Characteristics The evaluation of hybrid models revealed non-linear performance relationships. Combining traditional firewalls with blockchain logging produced synergistic effects, reducing DDoS success rates to 1.8% while maintaining sub-100ms latency for 95.3% of transactions. However, these configurations increased complexity costs by 35-40%, with diminishing returns observed when exceeding three integrated security layers ($\chi^2(4) = 12.57$, $p = 0.014$).

4. Practical Implications

Practitioners and firms thinking about adopting blockchain technologies will benefit from understanding the impact of this study on practical cybersecurity applications. Most importantly, the research indicates that blockchain technology should be implemented selectively in ways that maximize value for example in secure audit logging or decentralized identity management while steering clear of latency-sensitive applications such as real-time authentication systems. The study strongly recommends integrating traditional systems with efficient cyber defense protocols using blockchain's incorruptible features like establishing PKI systems protected by blockchain. Organizations need to perform sophisticated cost-benefit assessments that consider not only the primary deployment costs but also expenditures related to long-term operations such as energy consumption, especially in the case of Proof-of-Work blockchains and large-scale deployments. Legislative leaders should address the survey expert's concerns regarding regulations and focus on creation of uniform policies dedicated for blockchains in cybersecurity.

5. Future Directions

Interpreting the results within the context of the current study presents a few limitations that need to be addressed. The study concentrated on the Proof-of-Work and enterprise blockchain systems such as Ethereum and Hyperledger, so findings may not apply as well to newer systems like Ethereum 2.0's Proof-of-Stake. Although the controlled attack simulations provided useful testing conditions, they may differ from actual real-world threats. The calculations surrounding energy expenditure for computation were based on pre-2023 electricity pricing models and did not consider the integration of renewable energy sources. Furthermore, the expert survey sample, although very useful, suffers from selection bias due to predominantly enterprise blockchain skeptic perspectives.

Building upon these findings for future research should focus on several critical aspects. First and foremost, assessing post-Merge implementations in blockchain technology focusing on energy efficiency and latency improvements should be analyzed. Additionally, future research would benefit from the development of quantum-resistant blockchain architectures that incorporate post-quantum cryptography to defend against future quantum attacks. There is mounting demand for the development of lightweight consensus protocols that are sufficiently decentralized but more responsive to latency demands. Meanwhile, HIPAA-compliant solutions for healthcare and real-time settlement mechanisms for finance suggest advanced refinements in sector-specific frameworks. There is no doubt that blockchain technology offers substantial value in augmenting the cybersecurity infrastructure of certain applications, but systematic adoption would require breakthroughs in the overwhelming cost, scalability, and regulatory complexity challenges defined in this study.

6. Conclusion

The analysis revealed blockchain's performance characteristics follow a shaped distribution, excelling in specific security dimensions while underperforming in operational metrics. This explains the polarization in adoption patterns observed in practice - blockchain sees concentrated adoption in applications where its security advantages outweigh
operational costs (e.g., financial settlements, healthcare records), while traditional systems dominate latency-sensitive use cases. The energy consumption findings align with prior research (Vranken, 2017) but extend the analysis by quantifying the cost-security tradeoffs. Our data suggests enterprises face a trilemma between: 1. Security (favors blockchain) 2. Performance (favors traditional) 3. Cost (context-dependent) The emergence of hybrid models as a viable middle

ground supports recent theoretical work (Zargar et al., 2021) while providing empirical evidence of their practical limitations. The 35-40% complexity cost premium indicates hybrid approaches are most justified in high-value, high-risk scenarios.

The exhaustive study shows that there are significant trade-offs between traditional cybersecurity systems and blockchain-based ones. Performance testing proves that blockchain causes significant delays, and Ethereum's PoW consensus is 10× slower than PKI (47.3 ms vs. 4.2 ms), with a power-law scaling pattern (R^2 = 0.93) that becomes more adverse under load. Blockchain systems also offer superior resistance to tampering (0% success rate compared to traditional systems' 14.2%) but poor DDoS attack mitigation (72.3% compared to 98.7% success rate). Cost analysis indicates that blockchain has 65% higher 3-year TCO ($1,112K vs. $674K), and consumes 623× more energy (18.7 kWh vs. 0.03 kWh per 1k transactions), making it economically, and environmentally, unviable.

This demonstrates that blockchain cannot simply replace existing systems without consideration of application. The advantages of using blockchain have to be weighed against considerable increases in latency, cost, and energy use. Selective approaches are recommended whereby blockchain is reserved for tasks where immutable records are paramount (like secure logging), while traditional systems are used for time-sensitive tasks. Future work should look into developing standards to address current policies and energy-efficient consensus mechanisms (like PoS).

REFERENCES

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Yellick, J. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. Proceedings of the Thirteenth EuroSys Conference, 1–15. https://doi.org/10.1145/3190508.3190538

Gorenflo, C., Lee, S., Golab, L., & Keshav, S. (2020). FastFabric: Scaling hyperledger fabric to 20 000 transactions per second. International Journal of Network Management, 30(5), e2099.

Marchesi, L., Marchesi, M., Tonelli, R., & Lunesu, M. I. (2022). A blockchain architecture for industrial applications. Blockchain: Research and Applications, 3(4), 100088.

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts. ACM Computing Surveys, 50(6), 1–36. https://doi.org/10.1145/3136016

Samreen, N. F., & Alalfi, M. H. (2021). A survey of security vulnerabilities in ethereum smart contracts. arXiv preprint arXiv:2105.06974.

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. Health Informatics Journal, 24(2), 1–13. https://doi.org/10.1177/1460458218775420

Huang, J., Qi, Y. W., Asghar, M. R., Meads, A., & Tu, Y. C. (2019, August). MedBloc: A blockchain-based secure EHR system for sharing and accessing medical data. In 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 594-601). IEEE.

Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., & Danezis, G. (2019). Consensus in the age of blockchains. arXiv preprint arXiv:1711.03936. https://arxiv.org/abs/1711.03936

Xu, J., Wang, C., & Jia, X. (2023). A survey of blockchain consensus protocols. ACM Computing Surveys, 55(13s), 1-35.

Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Blockchain for IoT security and privacy. IEEE Internet of Things Journal, 4(5), 1–12. https://doi.org/10.1109/JIOT.2017.2686300

Arif, S., Khan, M. A., Rehman, S. U., Kabir, M. A., & Imran, M. (2020). Investigating smart home security: Is blockchain the answer?. IEEE Access, 8, 117802-117816.

Goodin, D. (2017). Equifax attack was much worse than thought. Ars Technica. https://arstechnica.com/

Lehto, M. (2022). Cyber-attacks against critical infrastructure. In Cyber security: Critical infrastructure protection (pp. 3-42). Cham: Springer International Publishing.

Kshetri, N. (2022). Blockchain and sustainable cybersecurity. Journal of Information Security and Applications, 65, 102629. https://doi.org/10.1016/j.jisa.2022.102629

Mohanta, B. K., Jena, D., Ramasubbareddy, S., Daneshmand, M., & Gandomi, A. H. (2019). Addressing security and privacy issues in IoT using blockchain. IEEE Internet of Things Journal, 6(5), 8152–8160. https://doi.org/10.1109/JIOT.2019.2920385

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Bitcoin Whitepaper. https://bitcoin.org/bitcoin.pdf

Stallings, W. (2021). Cryptography and network security (8th ed.). Pearson.

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084–2123. https://doi.org/10.1109/COMST.2016.2535718

Vranken, H. (2017). Sustainability of bitcoin and blockchains. Current Opinion in Environmental Sustainability, 28, 1–9. https://doi.org/10.1016/j.cosust.2017.04.011

Warkentin, M., & Ormond, D. (2022). Why enterprises resist blockchain for cybersecurity. Computers & Security, 114, 102742. https://doi.org/10.1016/j.cose.2022.102742

Zargar, S. T., Joshi, J., & Tipper, D. (2021). A survey of defense mechanisms against DDoS attacks in the cloud. ACM Computing Surveys, 54(2), 1–42. https://doi.org/10.1145/3434393

Yang, C., Buluç, A., & Owens, J. D. (2022). GraphBLAST: A high-performance linear algebra-based graph framework on the GPU. ACM Transactions on Mathematical Software (TOMS), 48(1), 1-51.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2020). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 16(4), 352–375. https://doi.org/10.1504/IJWGS.2020.110139

Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. Blockchain: research and applications, 3(2), 100067.

Shrimali, B., & Patel, H. B. (2022). Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities. Journal of King Saud University-Computer and Information Sciences, 34(9), 6793-6807.

Bilal, K., Sajid, M., & Singh, J. (2022, October). Blockchain technology: Opportunities & challenges. In 2022 International Conference on Data Analytics for Business and Industry (ICDABI) (pp. 519-524). IEEE.

Hussein, Z., Salama, M. A., & El-Rahman, S. A. (2023). Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms. Cybersecurity, 6(1), 30.

Singh, A., Kumar, G., Saha, R., Conti, M., Alazab, M., & Thomas, R. (2022). A survey and taxonomy of consensus protocols for blockchains. Journal of Systems Architecture, 127, 102503.

Krebs, T. (2023). Electronic bills of lading, transnational and English law: blocking the blockchain?. Uniform Law Review, 28(3-4), 323-338.

Griewing, S., Lingenfelder, M., Wagner, U., & Gremke, N. (2022, October). Use case evaluation and digital workflow of breast Cancer care by artificial intelligence and Blockchain technology application. In Healthcare (Vol. 10, No. 10, p. 2100). MDPI.