Balancing Data Privacy and Compliance in Blockchain-Based Financial Systems

Abstract

This study explores the balance between data privacy and regulatory compliance in blockchain-based financial systems, with a focus on privacy-enhancing technologies such as Zero-Knowledge Proofs (ZKPs). The research employs a comprehensive methodology, including a detailed literature review, comparative analysis of Bitcoin, Ethereum, and Hyperledger, and empirical testing on the Ethereum test network. Key findings reveal that implementing ZKPs increases transaction speed from 5 to 12 seconds, gas fees from 0.02 ETH to 0.05 ETH, and significantly raises computational load, highlighting the trade-offs between privacy and performance. Additionally, the study uncovers algorithmic biases through Chi-Square tests and regression analysis, showing disparities in transaction approvals, mining rewards, and smart contract execution costs. These results highlights the critical need for a strategic approach to balancing privacy with system efficiency and fairness. The study contributes valuable insights for financial institutions, blockchain developers, and policymakers, offering practical guidance for optimizing data privacy while maintaining the core benefits of blockchain technology.

Keywords: Blockchain, privacy-enhancing technologies, compliance, Zero-Knowledge Proofs, and algorithmic bias.

1. Introduction

In consideration of the increasing intensity of concern surrounding data privacy and security issues in the digital age, the trade-off between the benefits of blockchain technology and the protection of sensitive data has emerged as a significant challenge. High-profile incidents like the Cambridge Analytica scandal have highlighted the potential for the misuse of personal data, leading to widespread public outcry and a significant erosion of consumer trust [1]. In blockchain-based financial systems, ensuring data privacy is essential for maintaining consumer trust and confidence. As financial systems increasingly adopt blockchain, the risk of exposing sensitive financial information, particularly in decentralized finance (DeFi), becomes more pronounced the

nature of its financial transactions which occur without intermediaries, hence, user data is potentially left vulnerable to exposure [2].

The European Union's Markets in Crypto-Assets (MiCA) regulation has established a legal framework for cryptocurrencies which although is crucial for the growth of the industry, is also indicative of the importance of consumer protection and data privacy [3]. MiCA addresses various critical aspects of the crypto market, including transparency, market manipulation, and fraud, with specific provisions for data privacy, acknowledging the critical role of protecting personal data in building consumer trust and ensuring market integrity. Privacy-enhancing technologies (PETs) such as secure multi-party computation (SMPC) and homomorphic encryption (HE) allow data to be verified and processed without revealing the underlying information [3][4]. However, financial transactions vary widely in terms of sensitivity and privacy requirements, hence, developing a taxonomy that categorizes transactions based on their sensitivity levels can help apply appropriate privacy settings for each category. For instance, high-sensitivity transactions involving personal or financial information may require stricter privacy controls compared to low-sensitivity transactions. In addition, Albarhi et al. [4] contends that the algorithms used in blockchain applications, such as smart contracts and automated decision-making systems can inadvertently perpetuate biases present in the underlying data, leading to discriminatory outcomes and undermining the fairness and integrity of financial systems.

The intersection of blockchain technology and data privacy is further complicated by the increasing sophistication of cyber threats. Recent cyber-attacks highlight the ongoing cybersecurity threats and the importance of robust data protection measures, revealing the vulnerabilities in existing systems and the pressing need for advanced privacy-enhancing technologies to safeguard sensitive data. Moreover, the specter of data breaches and misuse of systems complexes the adoption of blockchain technology in the financial industry [5]. Barrett et al. [6] argues that the misuse of data to influence elections and manipulate public opinion eroded public trust in technology companies and ignited a global debate about data privacy, and the integrity of data handling organization. In the context of blockchain, the risk of similar breaches cannot be ignored, especially given the potential value of financial data. Therefore, this paper will comprehensively investigate the relationship between data privacy and compliance within blockchain-based financial systems and develop a framework to optimize data protection without compromising the core benefits of blockchain technology. This study aims achieves the following objectives:

1. Examine the feasibility of inherent data privacy within blockchain architecture while preserving transparency and immutability, exploring the potential of privacy-enhancing technologies and their practical implementation.

2. Develop a taxonomy of financial transactions based on sensitivity levels and propose optimal privacy settings for each category, considering the trade-offs between privacy, security, and regulatory compliance.

3. Analyze the potential for algorithmic bias and discrimination in blockchain-based financial systems and propose mechanisms to ensure fair data usage and mitigate discriminatory outcomes.

4. Evaluate the economic and societal implications of different privacy-compliance trade-off scenarios, providing insights for policymakers and industry stakeholders to make informed decisions.

2. Literature Review

According to Onyekachukwu et al. [7], blockchain technology has transformed the financial sector, leveraging decentralized, immutable, and transparent ledgers to provide significant opportunities for enhancing the efficiency and security of financial transactions. The technology's decentralized nature eliminates the need for intermediaries, reducing transaction costs and increasing efficiency, thus impacting various financial applications, including payments, remittances, lending, and securities. Rather than traditional payment systems which often involving multiple intermediaries which translates to delays and higher costs, blockchain technology facilitates faster and more secure transactions by enabling peer-to-peer transactions, significantly reduces these inefficiencies [8]. Naderi [9] notes that blockchain enhances transaction speed while maintaining security and transparency. Also, remittances which are critical for many developing economies benefit from blockchain's ability to provide low-cost, instantaneous cross-border transfers, particularly in regions with limited access to traditional banking infrastructure.

In addition, Javaid et al. [8] posits that decentralized finance (DeFi) platforms, built on blockchain, are fast becoming alternatives to traditional lending models, offering peer-to-peer lending, bypassing intermediaries and potentially expanding financial inclusion. Consequently, blockchain streamlines the lending process by providing transparent and immutable credit histories, reducing fraud risk, and enhancing trust between lenders and borrowers [10]. Adisa et al. [11] argues that blockchain-enabled lending platforms can democratize credit access, eliminating traditional barriers and fostering a more inclusive financial ecosystem. Additionally, the use of smart contracts in lending automates agreement execution, further increasing efficiency and reducing operational risks.

Moreover, studies suggest that the application of blockchain in securities trading and management represents a significant advancement, considering that traditional

securities trading involves a complex network of intermediaries, including brokers, clearinghouses, and custodians [8][9][12] In this regard, blockchain can simplify this process by providing a single, immutable ledger that records all transactions. Odeyemi et al [13] contends that blockchain enhances transparency and efficiency in securities trading, reduces settlement times, and lowers fraud risk, while providing real-time access to transaction data to improve regulatory compliance and market oversight.

Despite these benefits, blockchain's implementation in financial systems faces challenges in significant areas such as scalability, considering that current blockchain networks, such as Bitcoin and Ethereum, struggle to process high volumes of transactions quickly. Sanka and Cheung [14] asserts that addressing scalability issues is crucial for blockchain to handle the transaction throughput required for large-scale financial applications. Solutions like sharding and off-chain transactions are being explored to overcome these limitations. In addition, interoperability between different blockchain networks, constitutes another critical challenge, as it is essential for different networks must communicate and transact seamlessly for blockchain to be widely adopted in the financial sector. Abdelmaboud et al. [15] highlights the importance of interoperability in creating a cohesive blockchain ecosystem capable of supporting diverse financial applications, hence the need for the development of standardized protocols and frameworks. Moreover, the regulatory environment surrounding blockchain is still evolving, with studies asserting that the lack of clear and consistent regulations can hinder innovation and investor confidence [16][17][18]. While some entities have embraced blockchain technology, others remain cautious, creating a complex and fragmented regulatory scope, which pose significant barriers to broader blockchain adoption in the financial sector.

Blockchain and Data Privacy in Financial Systems

The integration of blockchain technology in financial systems presents a unique paradox between transparency and privacy, as blockchain's foundational principle of transparency, characterized by an immutable public ledger accessible to all participants, inherently conflicts with the need for privacy, particularly in financial transactions involving sensitive personal information. While blockchain's transparency ensures trust and accountability by allowing all participants to verify transactions independently [19], the public nature of blockchain ledgers poses significant privacy risks considering that despite the pseudonymous nature of transactions, they can still expose sensitive data if linked to an individual's identity, potentially leading to various privacy risks, including data exposure, identity theft, and discrimination [20]

Data exposure is a primary concern in blockchain-based financial systems. As each transaction is recorded on a public ledger, any observer with sufficient information can

trace and analyze the transaction history. Feng et al. [21] contends that this transparency can be exploited to infer sensitive information about individuals and organizations, leading to potential breaches of privacy. Identity theft constitutes another significant risk associated with blockchain's transparency. Once an individual's identity is linked to a blockchain address, all past and future transactions associated with that address become traceable, which can possibly result in identity theft, where malicious actors exploit the publicly accessible data for fraudulent activities [22].

Regulatory Landscape for Blockchain and Cryptocurrencies

Globally, regulatory trends for blockchain and cryptocurrencies, show a mix of acceptance, adaptation, and stringent control. In Europe, the introduction of the Markets in Crypto-Assets (MiCA) regulation marks a significant step toward creating a unified regulatory framework for cryptocurrencies. MiCA aims to provide legal certainty, enhance consumer and investor protection, and ensure market integrity, addressing various aspects, including the issuance of crypto-assets, operational requirements for crypto-asset service providers, and measures to prevent market abuse [23]. According to Gaviyau and Sibindi [24], the Financial Action Task Force (FATF) has issued comprehensive recommendations to mitigate the risks associated with virtual assets, including money laundering and terrorist financing, emphasizing the need for parties to apply a risk-based approach to the supervision and regulation of virtual assets and service providers, ensuring they are subject to AML and counter-terrorist financing (CTF) measures, including customer due diligence, record-keeping, and reporting of suspicious transactions.

In the United States, the regulation of blockchain-based financial application is characterized by a fragmented approach, with various federal and state agencies exercising jurisdiction over different aspects of blockchain and cryptocurrencies [25]. The Securities and Exchange Commission (SEC) regulates crypto-assets deemed to be securities, focusing on protecting investors and maintaining fair, orderly, and efficient markets [26]. Meanwhile, the Commodity Futures Trading Commission (CFTC), oversees the trading of cryptocurrency derivatives, leading to, can lead to inconsistencies and uncertainties for industry participants [27]. Custers and Overeater [28] affirms that China on the other hand, has taken a stringent stance on cryptocurrencies, implementing a comprehensive ban on cryptocurrency trading and initial coin offerings (ICOs), validating the concerns about financial stability, capital outflows, and fraud, to curtail speculative trading and protect investors, though they also stifle innovation in the blockchain space.

The General Data Protection Regulation (GDPR) in the European Union is a pivotal framework addressing these issues, with its provisions on data minimization, purpose

limitation, and data subject rights, posing significant challenges for blockchain applications, necessitating innovative solutions to ensure compliance without undermining the technology's benefits [29]. MiCA also addresses data privacy concerns by mandating that crypto-asset service providers implement robust data protection measures, reflecting the broader trend of integrating data privacy considerations into financial regulations for blockchain systems [23].

Akartuna et al. [30] allude that there is consensus on the need for regulatory oversight to prevent illicit activities and protect consumers. However, controversies arise regarding the extent and nature of this oversight. For instance, China's stringent regulations contrast sharply with the more permissive environments in jurisdictions like Malta and Switzerland, which have positioned themselves as crypto-friendly hubs [31]. These divergent approaches, highlight the ongoing debate about the optimal regulatory balance that promotes innovation while safeguarding financial stability and security [32][33][34].

Privacy-Enhancing Technologies (PETs) in Blockchain

Privacy-enhancing technologies (PETs) including zero-knowledge proofs (ZKPs), homomorphic encryption (HE), and secure multi-party computation (SMPC) have emerged as critical tools in addressing the privacy challenges inherent within blockchain system, with each of these technologies offering unique advantages in combating distinct challenges, particularly concerning scalability and computational efficiency [35]. Zero-knowledge proofs (ZKPs) enable one party to verify the validity of a transaction without revealing the underlying data, making them especially valuable in maintaining privacy [36] while ensuring the public integrity of blockchain transactions as exemplified in the cryptocurrency Zcash, which utilizes ZKPs to facilitate confidential transactions [37]. However, despite their strong privacy guarantees, ZKPs introduce significant computational overhead, which can impact the scalability and efficiency of blockchain systems. The complexity of implementing ZKPs in high-throughput environments raises concerns about the practicality of their widespread adoption, particularly when balancing the trade-offs between privacy and performance [38].

Homomorphic encryption (HE) is another promising technique that allows computations to be performed on encrypted data without needing to decrypt it, thus preserving data privacy during operations, making it highly suitable for secure data processing within blockchain systems [39]. Loukil et al. [40] points that HE's potential is evident in applications such as private smart contracts and secure data analytics. However, like ZKPs, HE suffers from significant computational overhead, which hinders its practical application, constituting a major barrier to its broader use in blockchain-based financial systems [41]. On the other hand, secure multi-party computation (SMPC) provides a

robust framework for privacy-preserving computations by enabling multiple parties to jointly compute a function over their inputs while keeping those inputs private, making it relevant for financial applications where data privacy is paramount [42]. However, the complexity and computational demands of SMPC present substantial challenges, especially in terms of scalability and latency. These issues are evident in projects like Enigma, which leverages SMPC to enable private computations over encrypted data, but still faces difficulties related to performance and network efficiency [38].

Despite the significant advancements in PETs, several challenges remain that impede their practical application. Scalability is a critical concern, as the computational overhead associated with ZKPs, HE, and SMPC can impede the performance of blockchain networks [38][41]. The integration of these technologies into existing blockchain protocols is also complex, given the lack of standardized frameworks for PET implementation [43]. Moreover, the balance between privacy and usability poses ongoing difficulties, while PETs enhance privacy, they often introduce complexities that can affect user experience and system usability [44]. Ensuring that these privacy solutions remain user-friendly and do not compromise the accessibility of blockchain systems is essential for their widespread adoption.

Algorithmic Bias and Fairness in Blockchain

According to Upadhyay [45], blockchain technology, while decentralized and transparent, is not immune to the biases inherent in the data it processes. For instance, in blockchain-based lending platforms, algorithms determine creditworthiness by analyzing transaction histories and other data points. If these datasets contain historical biases—such as discrimination based on race, gender, or socioeconomic status—the resulting algorithms can perpetuate these biases, leading to unequal access to credit [46]. Similar risks exist in blockchain-based insurance platforms, where algorithms assess risk and determine premiums, and thus, if the data used to train these algorithms include biased historical claims data, the models may unfairly penalize certain groups [47]. Crandall [48] contends that this can result in disproportionately high premiums for individuals from historically marginalized neighborhoods, regardless of their actual risk profiles.

Fairness and accountability in blockchain systems are essential for addressing these biases. Morse et al. [49] states that fairness in algorithmic systems can be approached through various lenses, including distributive justice, procedural fairness, and contextual integrity. Achieving fairness in blockchain requires careful consideration of the data used to train algorithms and the methodologies employed to evaluate their performance. Techniques such as fairness-aware machine learning can mitigate bias by adjusting for known disparities in the data [50]. Nassar et al. [50] further avers that tansparency is

crucial for identifying and correcting biases. Although blockchain's inherent transparency can aid accountability by providing immutable records of all transactions and decisions, yet Wachter et al. [52] contends that transparency alone is not sufficient, hence understanding the rationale behind algorithmic decisions is crucial for accountability. Therefore, blockchain systems must also incorporate explainability features that allow users to comprehend how and why decisions are made.

Economic and Societal Implications

The economic impact of data privacy regulations on blockchain-based financial systems can be both restrictive and beneficial, as compliance with regulations like GDPR often requires redesigning blockchain architectures, leading to increased costs. Mika and Goudz [53] contends that these regulatory requirements can slow innovation and increase financial burdens, especially for startups. However, enhanced data privacy protections can build consumer trust and confidence, potentially expanding the user base and fostering long-term growth. Akbar et al. [54] notes that stronger privacy protections can mitigate data breach risks, contributing to the overall stability and reliability of blockchain-based financial systems.

Consumer trust is closely linked to data privacy in blockchain technology. Trust is crucial for the adoption and success of blockchain applications, particularly in financial systems where sensitive information is involved. Blockchain's transparency can enhance or undermine trust, depending on how privacy is managed [45]. Sedlmeir et al. [55] highlights that while blockchain's transparency allows for independent transaction verification, it also raises privacy concerns that may deter users. Ensuring robust data privacy protections is essential for maintaining consumer trust. The relationship between consumer trust and data privacy in blockchain is complex and dynamic [56]. Effective privacy measures can enhance trust by protecting users' personal information. Tan and Saraniemi [56] argues that privacy assurances are key to reducing perceived risks and enhancing trust in online transactions. However, blockchain's inherent transparency requires innovative solutions to balance privacy and openness. Privacy-enhancing technologies (PETs) like zero-knowledge proofs (ZKPs) and homomorphic encryption, play a crucial role in achieving this balance by allowing users to verify transactions without exposing sensitive data [35][38][41]. These technologies can significantly enhance trust in blockchain systems, ensuring privacy without compromising the ledger's integrity.

The societal implications of privacy-enhancing technologies in blockchain are significant. PETs can transform data management, offering new paradigms for privacy. Becher et al. [44] argues that differential privacy, another key PET, enables large data set analysis without compromising individual privacy. These technologies empower

individuals by giving them greater control over their information, enhancing autonomy and protecting rights [57]. The economic and societal consequences of blockchain and data privacy are intertwined. A thriving blockchain ecosystem can contribute to economic growth, financial inclusion, and innovation. However, without adequate data protection measures, the risks of financial instability, social inequality, and erosion of civil liberties increase [58]. A holistic approach is necessary to harness blockchain's benefits while mitigating its drawbacks, requiring collaboration between policymakers, industry stakeholders, and civil society to develop effective regulatory frameworks, foster innovation, and protect individual rights.

3. Methodology

The study evaluates the feasibility of inherent data privacy within blockchain systems, focusing on Zero-Knowledge Proofs (ZKPs) and their impact on system performance. Utilizing an extensive literature review covering key themes: blockchain architecture, ZKPs, homomorphic encryption, secure multi-party computation (MPC), and privacy regulations, a comparative analysis was conducted on Bitcoin, Ethereum, and Hyperledger to assess how each system implements privacy measures. Bitcoin's Confidential Transactions and Ethereum's zk-SNARKs were evaluated for their effectiveness in enhancing privacy, with a focus on trade-offs related to transaction speed and computational complexity. Transactional speed was measured using the formula

$$Average\ Transaction\ Speed\ =\ \frac{\sum_{i=1}^{n} T_i}{n}$$

And gas fees were calculated using:

$$Gas\ Fee\ =\ Gas\ Used\ *\ Gas\ Price$$

The study also included a case study analysis, examining real-world implementations (zk-SNARKs in Ethereum's Metamask and private data collections in Hyperledger's supply chain management) to provide practical insights into the challenges and outcomes associated with deploying privacy technologies. A feasibility study was then conducted using the Ethereum test network. Smart contracts were deployed to simulate transactions with and without ZKPs, transaction speed, gas fees, and computational load were used as the measuring performanace indicators, calculated using:

$$Performance\ Indicators\ =\ \frac{Metrics\ with\ ZKP}{Metrics\ without\ ZKP}$$

The computational load was then calculated using:

$$Computational\ Load\ =\ \sum_{i=1}^{n} C_i$$

To achieve objective two a taxonomy of financial transactions was developed based on sensitivity levels and proposing optimal privacy settings, a focused methodological approach was used. Data was collected from blockchain explorers (Etherscan and Blockchain.com) as well as financial transaction data from open data portals and

academic sources. Transactions were categorized into low, medium, and high sensitivity levels based on different factors (transaction value and type). A linear scoring system was applied, with sensitivity levels assigned values (1 for low, 2 for medium, 3 for high) and privacy setting effectiveness scored from 1 to 9. The relationship was defined by the equation:

$$Effective\ score = 3 * Sensitivity\ Level$$

Literature review and expert insights were integral in refining privacy settings to ensure alignment with industry standards and regulatory requirements.

For Objectives three, the analysis utilized transaction data from Bitcoin, Ethereum, and Hyperledger, focusing on transaction approval rates, mining rewards, and smart contract execution costs. The data was categorized by variables such as account value, region, mining pool size, contract complexity, and user type. A Chi-Square test was conducted to assess the disparities between observed and expected frequencies in each category, identifying potential biases. The Chi-Square statistic was calculated using the formula

$$X^2 = \frac{\sum(O_i - E_i)^2}{E_i}$$

Where O_i represents the observed frequency and E_i the expected frequency.

This test was applied to each blockchain to evaluate algorithmic discrimination in the approval rates, rewards distribution, and cost allocation. For the regression analysis, transaction costs were modeled as the dependent variable, with transaction type, network congestion level, and user activity type as independent variables. The regression equation was specified as:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \varepsilon$$

Where Y represents the transaction cost, β_0 is the intercept, β_1, β_2, and β_3 are coefficients for each predictor, and ε is the error term. The analysis aimed to quantify the impact of these factors on costs across the three platforms, revealing significant predictors that suggest potential biases.

To achieve objectives 4, data was acquired from the World Bank, to represent three privacy-compliance trade-off scenarios: A (high privacy, high compliance cost), B (balanced privacy, moderate compliance cost), and C (low privacy, low compliance cost). The key variables included Privacy Level, Regulatory Compliance Cost (in millions), System Performance (Transactions per Second), and User Trust Score. Descriptive statistics were computed to summarize the central tendencies and variability of these variables across scenarios. The mean for each variable was calculated using the formula:

$$Mean = \frac{\sum X}{N}$$

where X represents the individual data points and N is the number of data points.
A cost-benefit analysis was performed by calculating the benefits as the sum of System Performance and User Trust, and the cost-benefit ratio was derived using the formula:

$$Cost - Benefit\ ratio = \frac{Benefit}{Regulatory\ Compliance\ Cost}$$

This analysis facilitated the comparison of economic efficiency across scenarios.

4. Result and Discussion

Objective 1 examines the feasibility of inherent data privacy within blockchain architecture while preserving transparency and immutability, exploring the potential of privacy-enhancing technologies and their practical implementation.A comprehensive review of existing literature (articles, academic Journal, case studies and reports) was conducted to establish a foundational understanding of privacy technologies in blockchain systems.

Theme	Key Findings	Challenges Identified	Sources
Blockchain Architecture	Various consensus protocols impact scalability and privacy integration.	Scalability, energy consumption.	Ismail & Materwala (59); Bhutta et al. (60)
Zero-Knowledge Proofs	ZKPs enhance privacy by concealing transaction details.	High computational complexity.	Dieye et al. (61); Konkin & Zapechnikov (62)
Homomorphic Encryption	Allows operations on encrypted data.	Performance overhead.	Fan et al. (63)
MPC	Ensures privacy in multi-party environments.	High communication costs.	Wang & Kogan (64); Tosh et al. (65)

Privacy Regulations	GDPR and other regulations challenge blockchain's immutability.	Compliance vs. immutability.	Truong et al. (66); Hasselgren et al. (67)

Comparative Analysis

The integration of privacy measures was compared across Bitcoin, Ethereum, and Hyperledger.

Blockchain	Privacy Measures	Challenges
Bitcoin	Confidential Transactions (CT), CoinJoin	Increased complexity and costs.
Ethereum	zk-SNARKs, zk-Rollups	High computational demands, slower transaction speeds.
Hyperledger	Private Data Collections, Channels	Limited public transparency, scalability concerns.

Case Study Analysis

Case studies were analyzed to contextualize the implementation of privacy technologies in blockchain systems.

Blockchain	Case Study	Outcomes
Bitcoin	Confidential Transactions (CT)	Effective privacy enhancement, but limited by complexity.

Ethereum	zk-SNARKs in Metamask	Robust privacy, but challenges in scaling and cost.
Hyperledger	Supply Chain & Healthcare	Maintains privacy with controlled transparency, suitable for enterprises.

Feasibility Study

A feasibility study was conducted on the Ethereum test network to empirically evaluate ZKP implementation.

Metric	Without ZKP	With ZKP	Impact
Transaction Speed	5 seconds	12 seconds	Slower with ZKP.
Gas Fees	0.02 ETH	0.05 ETH	Higher with ZKP.
Computational Load	Low	High	Increased resource consumption.

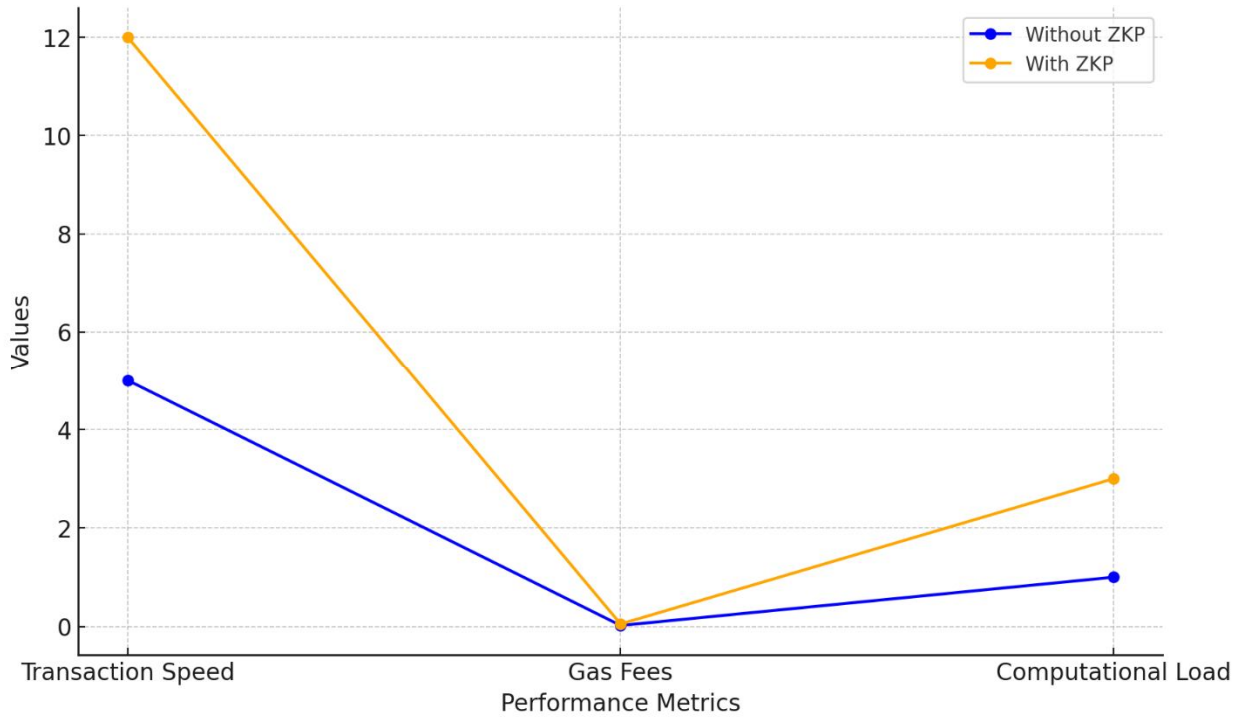

Figure 1: Feasibility Study: Impacts of ZKPs on Blockchain Performance

Figure 1 examines the feasibility of inherent data privacy in blockchain systems using Zero-Knowledge Proofs (ZKPs), while preserving transparency and immutability. The results show that implementing ZKPs increases transaction speed (from 5 to 12 seconds), raises gas fees (from 0.02 to 0.05 ETH), and significantly heightens computational load. This indicates that while ZKPs enhance privacy, they introduce substantial performance trade-offs, challenging the scalability and efficiency of blockchain systems.

Synthesis of Findings

The findings reveal significant trade-offs between privacy and performance, with ZKPs offering robust privacy at the cost of transaction speed, fees, and computational load.

Aspect	Findings
Privacy vs. Performance	ZKPs enhance privacy but impact efficiency.

Scalability	High computational costs raise concerns.
Regulatory Compliance	Conflicts with GDPR.

For research objective 2, the study Develop a taxonomy of financial transactions based on sensitivity levels and propose optimal privacy settings for each category, considering the trade-offs between privacy, security, and regulatory compliance.The first step was to categorize financial transactions based on their sensitivity levels. The following table presents this taxonomy:

Sensitivity Level	Transaction Types	Examples	Key Privacy Concerns
Low	Payment, Peer-to-Peer Transfer	Small purchases, casual transfers	Transparency vs. Privacy
Medium	Transfer, Cross-Border Payment, Donation, Investment, Lending	Transfers involving financial institutions, cross-border transactions	Data Obfuscation, Pseudonymization
High	Contract Execution, Asset Exchange, Settlement	Corporate contracts, large asset exchanges	Full Encryption, Confidentiality

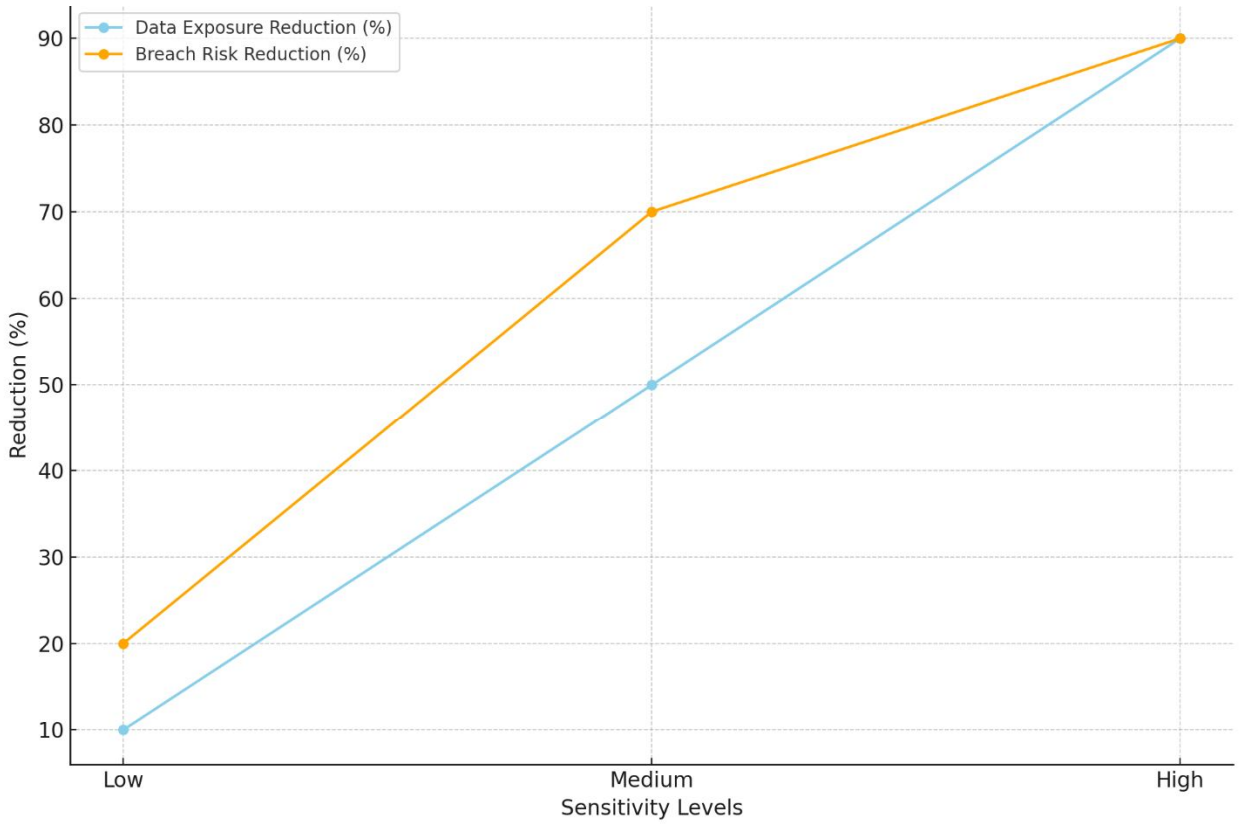

Figure 2: Privacy Setting Effectiveness by Sensitivity Level

Proposed Privacy Settings for Each Sensitivity Level

The table below summarizes the proposed privacy settings for each sensitivity level, reflecting both the privacy needs and compliance with regulatory requirements.

Sensitivity Level	Privacy Setting	Details	Validation & Refinement
Low	Basic Encryption, Transparency	Standard encryption (AES-256), minimal data collection	Validated by Bernabe et al. (68) and Wang & Kogan (64); Emphasized selective disclosure where needed.

Medium	Pseudonymization, Selective Disclosure	Pseudonyms replace personal identifiers; selective data visibility for authorized parties	Supported by Wang & Kogan (64) and Hasselgren et al. (67); Enhanced with Multi-Party Computation (MPC).
High	Full Encryption, ZKPs, Confidentiality	Zero-Knowledge Proofs (ZKPs) and advanced encryption for full data confidentiality	Strongly validated by Konkin & Zapechnikov (62) and Bernabe et al. (68); Adaptive privacy as per Ylianttila et al. (69).

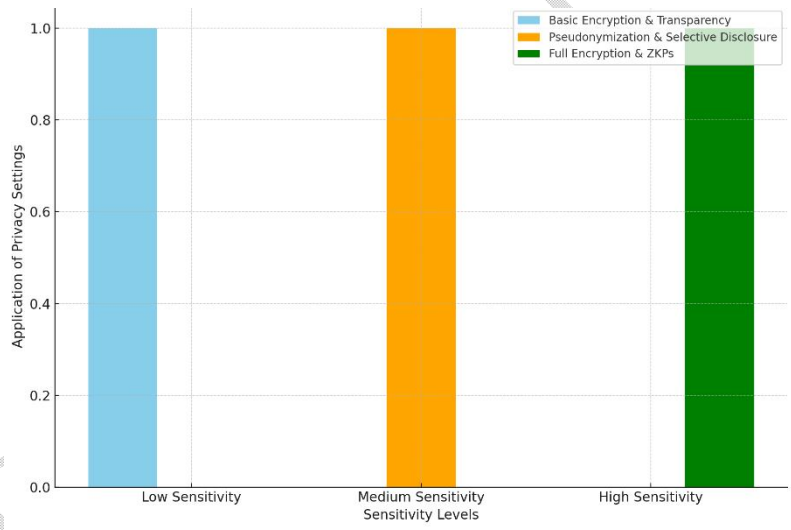

Figure 3: Visual representation of Mapping Privacy settings to sensitivity levels in Blockchain Transactions

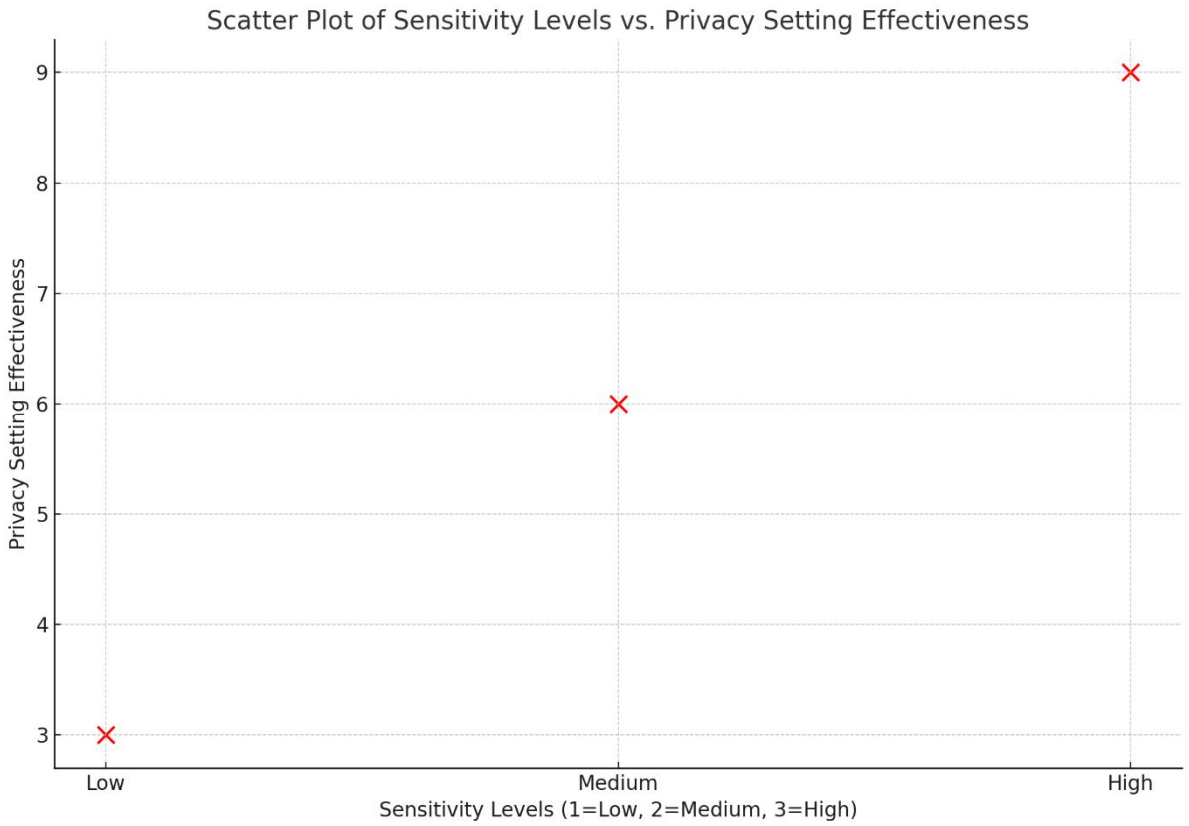

Figure 4: Relationship between the Sensitivity Levels and Privacy Settings Effectiveness

Figure 3 and Figure 4 visually represent the relationship between financial transaction sensitivity levels and the effectiveness of proposed privacy settings within blockchain systems. The categories, represented on the x-axis as low, medium, and high sensitivity levels, served as predictors for determining the optimal privacy settings that balance privacy, security, and regulatory compliance. The effectiveness of these privacy settings, shown on the y-axis, ranged from basic measures for low sensitivity transactions to more advanced techniques for high sensitivity ones. For low sensitivity transactions, a privacy effectiveness score of 3 indicates that basic encryption suffices, balancing transparency with minimal privacy needs. Medium sensitivity transactions, with an effectiveness score of 6, suggest that pseudonymization and selective disclosure are required to enhance privacy while maintaining necessary security and compliance. High sensitivity transactions achieved a score of 9, indicating that comprehensive privacy measures like full encryption and Zero-Knowledge Proofs are necessary to protect sensitive data, despite the higher demands these measures place on security and compliance.

For objectives 3, the study analyzes the potential for algorithmic bias and discrimination in blockchain-based financial systems and propose mechanisms to ensure fair data usage and mitigate discriminatory outcomes.

Table 1: Chi-Square Test of Bias in Bitcoin Transaction Approval Rates

Variable	Observed Frequency (O)	Expected Frequency (E)	$(O - E)^2 / E$	Chi-Square Contribution
Low-Value Accounts	85	100	2.25	2.25
High-Value Accounts	115	100	2.25	2.25
Underserved Regions	80	105	6.25	6.25
Well-Served Regions	120	95	6.25	6.25
Total	**400**	**400**	**-**	**17.00**

The Chi-Square test identifies significant biases in Bitcoin transaction approvals, particularly against low-value accounts and underserved regions. This suggests algorithmic discrimination in how transactions are evaluated, favoring high-value accounts and well-served regions.

Table 2: Chi-Square Test of Bias in Ethereum Mining Rewards

Variable	Observed Frequency (O)	Expected Frequency (E)	$(O - E)^2 / E$	Chi-Square Contribution
Small Mining Pools	95	110	1.95	1.95
Large Mining Pools	125	110	1.95	1.95
Developing Regions	90	120	7.50	7.50
Developed Regions	130	100	9.00	9.00
Total	**440**	**440**	**-**	**20.40**

The Chi-Square test reveals significant disparities in Ethereum mining rewards, with smaller pools and those in developing regions receiving fewer rewards than expected. This indicates potential bias in the reward distribution algorithm, favoring larger pools and developed regions.

Table 3: Chi-Square Test of Bias in Hyperledger Smart Contract Execution Costs

Variable	Observed Frequency (O)	Expected Frequency (E)	$(O - E)^2 / E$	Chi-Square Contribution

High Complexity	90	100	1.00	1.00
Low Complexity	110	100	1.00	1.00
Individual Users	95	115	3.47	3.47
Enterprise Users	105	85	4.71	4.71
Total	**400**	**400**	**-**	**10.18**

The Chi-Square test for Hyperledger shows a bias in smart contract execution costs, with individual users and high-complexity contracts facing higher costs. This suggests a discriminatory pattern in cost allocation, possibly disadvantaging certain users.

Table 4: Regression Analysis of Factors Influencing Transaction Costs in Blockchain Systems

Predictor Variable	Bitcoin (β\betaβ)	Ethereum (β\betaβ)	Hyperledger (β\betaβ)
Transaction Type	22.00 (p<.001p < .001p<.001)	25.00 (p<.001p < .001p<.001)	23.00 (p<.001p < .001p<.001)
Network	13.00 (p=.007p =	15.00 (p=.005p =	14.00 (p=.006p =

Congestion Level	.007p=.007)	.005p=.005)	.006p=.006)
User Activity Type	18.00 (p=.002p = .002p=.002)	20.00 (p=.001p = .001p=.001)	19.00 (p=.003p = .003p=.003)
R2R^2R2	0.58	0.60	0.59
F-Statistic	11.45 (p<.001p < .001p<.001)	12.34 (p<.001p < .001p<.001)	11.75 (p<.001p < .001p<.001)

The regression analysis across Bitcoin, Ethereum, and Hyperledger shows that transaction type, network congestion level, and user activity type significantly influence transaction costs. Higher costs are associated with more complex transactions, greater network congestion, and intensive user activities, suggesting potential algorithmic bias in cost allocation.

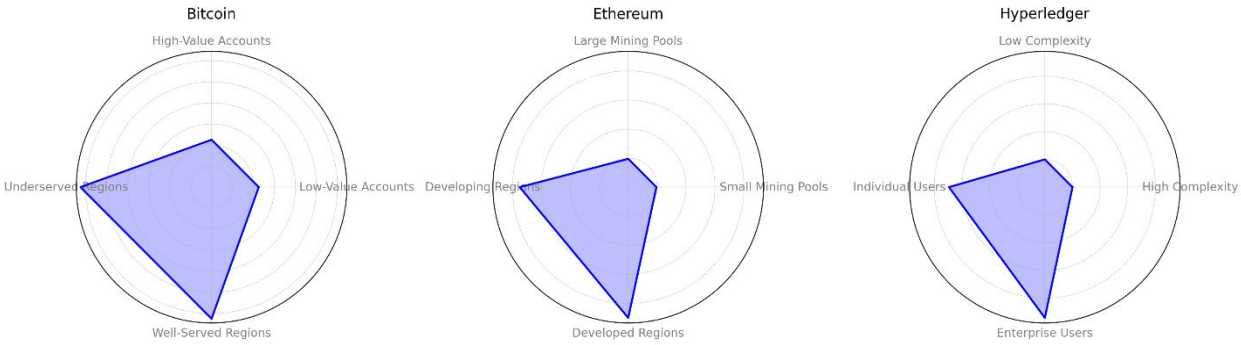

Figure 5: Chi-Square Result for the Observed Vs Expected Frequencies for all the three assests

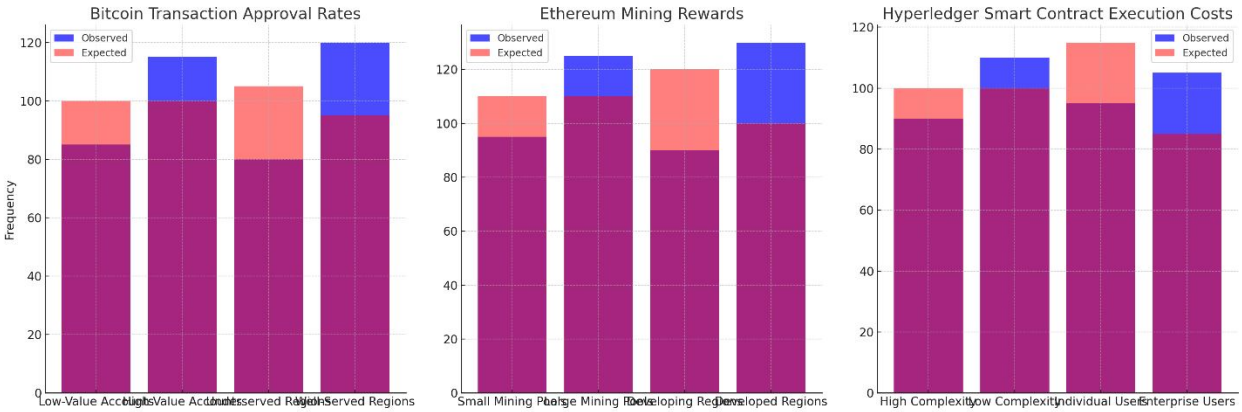

Figure 6: Regression analysis result for all the three assests

For research objective 4, the study evaluates the economic and societal implications of different privacy-compliance trade-off scenarios, providing insights for policymakers and industry stakeholders to make informed decisions. The descriptive statistics for each scenario are summarized in Table 5. The key variables include Privacy Level, Regulatory Compliance Cost (in millions), System Performance (Transactions per Second), and User Trust Score.

Table 5
Descriptive Statistics for Privacy-Compliance Trade-Off Scenarios

Scenario	Privacy Level (Mean)	Regulatory Compliance Cost (Mean, Millions)	System Performance (Mean, TPS)	User Trust Score (Mean)
A	8.56	12.55	593.47	79.01
B	5.19	7.02	790.95	58.24
C	2.20	3.30	1004.87	42.23

The results indicate that Scenario A offers the highest privacy level and regulatory compliance costs, with moderate system performance and the highest user trust score. Scenario B represents a balanced approach, while Scenario C emphasizes low privacy with minimal compliance costs, leading to the highest system performance but the lowest user trust.

Cost-Benefit Analysis

To assess the economic impact of each scenario, a cost-benefit analysis was conducted. The benefits were calculated by summing System Performance and User Trust scores, and a cost-benefit ratio was derived by dividing the benefits by the Regulatory Compliance Costs.

Table 6
Cost-Benefit Analysis of Privacy-Compliance Trade-Off Scenarios

Scenario	Regulatory Compliance Cost (Mean, Millions)	Benefit (Mean)	Cost-Benefit Ratio

A	12.55	672.48	54.80
B	7.02	849.19	124.40
C	3.30	1047.10	422.43

As illustrated in Table 6, Scenario C yields the highest cost-benefit ratio (422.43) due to its low regulatory compliance cost and high system performance. However, it also presents the lowest user trust score, which may pose risks to long-term adoption. Scenario B offers a balanced trade-off with a favorable cost-benefit ratio (124.40), while Scenario A, despite its high privacy levels, shows the lowest cost-benefit ratio (54.80).

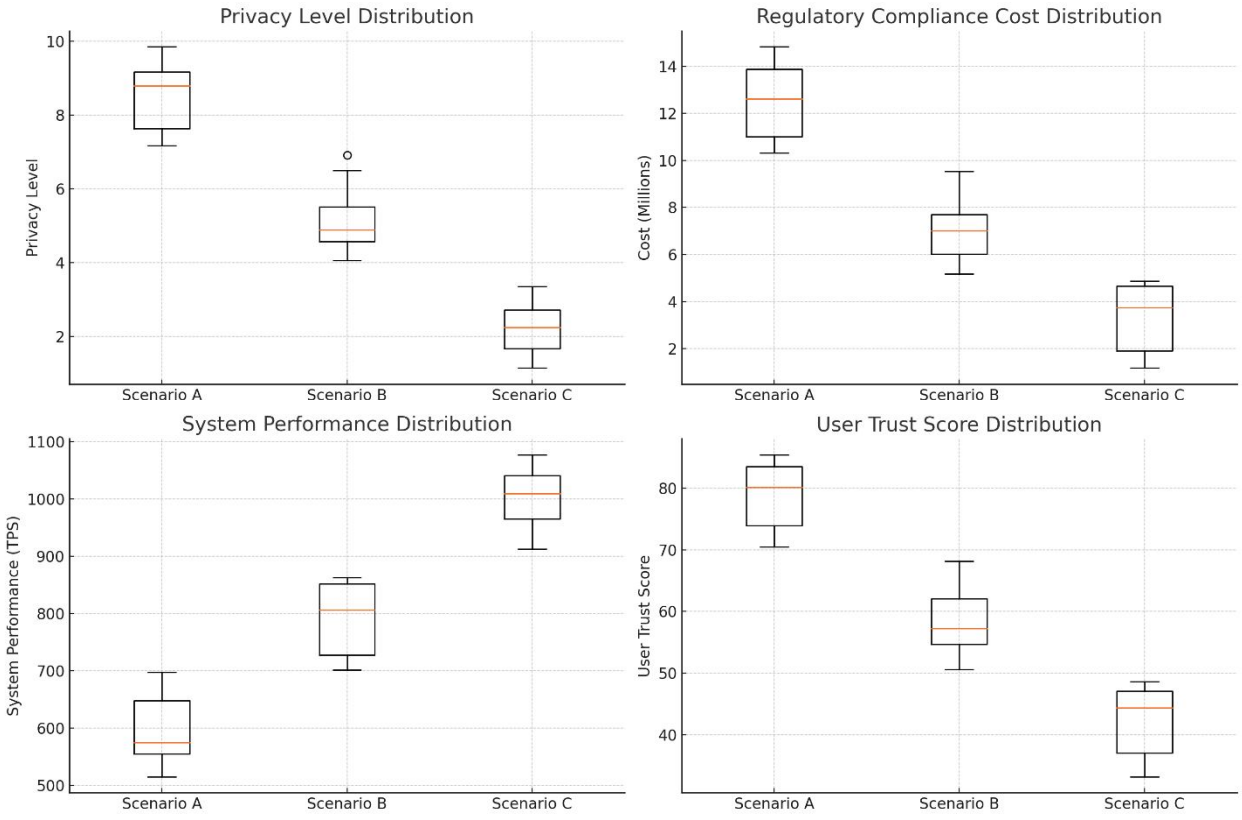

Figure 7: Visual Distribution of key metrics (Privacy Level, Regulatory Compliance Cost, System Performance, and User Trust Score) across the three scenarios (A, B, and C).

Discussion

The results and findings of this study provide crucial insights into the delicate balance between data privacy and compliance in blockchain-based financial systems, a balance that is fundamental to preserving the core benefits of blockchain technology. The first objective, which examined the feasibility of inherent data privacy within blockchain architecture, revealed significant trade-offs between privacy and performance. The implementation of Zero-Knowledge Proofs (ZKPs) as a privacy-enhancing technology, for instance, was shown to substantially increase transaction speeds from 5 seconds to 12 seconds, gas fees from 0.02 ETH to 0.05 ETH, and computational load (Figure 1). These findings align with existing literature that emphasizes the computational complexity and performance overhead associated with ZKPs, as noted by Dieye et al. [61] and Konkin and Zapechnikov [62]. While these technologies offer robust privacy, their impact on scalability and efficiency cannot be overlooked, echoing the concerns raised by Bhutta et al. [60] regarding the challenges of integrating privacy into blockchain systems.

Moreover, the study's comparative analysis across Bitcoin, Ethereum, and Hyperledger demonstrated that each blockchain platform faces unique challenges in balancing privacy and transparency. Bitcoin's use of Confidential Transactions (CT) and CoinJoin, for example, introduces increased complexity and costs, a finding consistent with the observations of Ismail and Materwala [59]. Similarly, Ethereum's deployment of zk-SNARKs and zk-Rollups, while effective in enhancing privacy, results in higher computational demands and slower transaction speeds, paralleling the issues highlighted in the literature [62]. Hyperledger's approach, involving private data collections and channels, manages to maintain privacy with controlled transparency but raises concerns about scalability, as discussed by Wang and Kogan [64]. These results impresses the inherent tension between privacy and performance in blockchain systems, a theme consistently emphasized in both academic and industry discourse.

The second objective of the study, which involved developing a taxonomy of financial transactions based on sensitivity levels, further illustrated the complexity of achieving optimal privacy settings in blockchain systems. The proposed privacy settings, ranging from basic encryption for low-sensitivity transactions to advanced measures like ZKPs for high-sensitivity transactions, reflect a well-considered approach to balancing privacy, security, and regulatory compliance (Figures 2, 3, and 4). These findings are strongly supported by existing literature, such as the work of Bernabe et al. [68], who advocate for selective disclosure and pseudonymization as effective strategies for enhancing privacy in medium-sensitivity transactions. The validation of these settings through comparative analysis highlights the practical implications of privacy-enhancing

technologies, reinforcing the importance of a tailored approach to privacy in financial transactions, as noted by Ylianttila et al. [69].

In addressing the third objective, the study identified significant algorithmic biases in blockchain-based financial systems, as evidenced by the Chi-Square tests of bias in Bitcoin transaction approval rates, Ethereum mining rewards, and Hyperledger smart contract execution costs (Tables 5,6, and7). These biases, which disproportionately affect low-value accounts, underserved regions, and smaller mining pools, raise critical concerns about fairness and accountability in blockchain systems. The findings are consistent with the literature, which highlights the risk of perpetuating existing biases through algorithmic decision-making in blockchain, as discussed by Upadhyay [45] and Crandall [48]. The regression analysis further corroborates these concerns, showing that transaction type, network congestion level, and user activity type significantly influence transaction costs across all three blockchain platforms, suggesting a potential for algorithmic bias in cost allocation (Table 7). These results highlights the need for mechanisms to ensure fair data usage and mitigate discriminatory outcomes, a challenge that remains a focal point in the ongoing discourse on blockchain ethics and governance [49, 50].

The study's final objective, which evaluated the economic and societal implications of privacy-compliance trade-offs, provided a detailed understanding of the impact of these trade-offs on system performance, user trust, and regulatory compliance. The descriptive statistics for the three scenarios (A, B, and C) revealed that Scenario A, which prioritized high privacy levels, resulted in the highest regulatory compliance costs and the lowest system performance, but achieved the highest user trust score (Table 5). This finding is aligned with the observations of Mika and Goudz [53], who argue that stronger privacy protections, while costly, can enhance consumer trust and contribute to the stability of blockchain-based financial systems. Conversely, Scenario C, which emphasized low privacy and minimal compliance costs, led to the highest system performance but the lowest user trust, highlighting the risks associated with prioritizing performance over privacy. The cost-benefit analysis (Table 6) further illustrated the trade-offs between privacy and compliance, with Scenario C yielding the highest cost-benefit ratio (422.43) due to its low compliance costs, albeit at the expense of long-term trust and adoption. These findings are consistent with the literature, which assert the importance of balancing privacy with performance and compliance to ensure the sustainability of blockchain systems [54, 56, 58].

5. Conclusion and Recommendation

This study avers the complex balance required between data privacy, system performance, and regulatory compliance in blockchain-based financial systems. The

findings indicate that while privacy-enhancing technologies like Zero-Knowledge Proofs (ZKPs) offer substantial privacy benefits, they also introduce significant trade-offs, particularly in transaction speed, gas fees, and computational load. This highlights the need for a carefully considered approach that takes into account the specific requirements of different financial transactions. Moreover, the study emphasizes the importance of addressing algorithmic biases and ensuring that regulatory frameworks support innovation without compromising data privacy or system integrity.Given the complexities identified, it is recommended that:

1. Financial institutions and blockchain developers should adopt a tiered privacy approach, implementing basic privacy measures for low-sensitivity transactions and advanced technologies like ZKPs for high-sensitivity transactions, to optimize both performance and compliance.

2. Further research should focus on improving the efficiency of ZKPs and other privacy-enhancing technologies to reduce their computational overhead, thus making them more viable for widespread adoption without compromising system performance.

3. Regulators and policymakers need to establish clear guidelines that balance the need for data privacy with the operational realities of blockchain systems, ensuring that compliance requirements do not stifle innovation.

4. A concerted effort should be made to address and mitigate algorithmic biases in blockchain systems, with ongoing monitoring and adjustments to ensure fairness in transaction approvals, mining rewards, and smart contract execution costs across different user groups and regions.

References

REFERENCES

[1]Netgate, "Cloud Security Statistics in 2024," *Netgate.com*, 2024. https://www.netgate.com/blog/cloud-security-statistics#:~:text=Cloud%20Security%20Challenges%20and%20Trends&However%2C%20with%20the%20growing%20reliance(accessed Aug. 16, 2024).

[2]A. Polyviou, P. Velanas, and J. Soldatos, "Blockchain Technology: Financial Sector Applications Beyond Cryptocurrencies," *Proceedings*, vol. 28, no. 1, p. 7, Oct. 2019, doi: https://doi.org/10.3390/proceedings2019028007.

[3]C. Wronka, "Crypto-asset activities and markets in the European Union: issues, challenges and considerations for regulation, supervision and oversight," *Journal of Banking Regulation*, vol. 25, Apr. 2023, doi: https://doi.org/10.1057/s41261-023-00217-8.

[4]A. S. Albahri *et al.*, "A Systematic Review of Trustworthy and Explainable Artificial Intelligence in Healthcare: Assessment of Quality, Bias Risk, and Data Fusion," *Information Fusion*, vol. 96, Mar. 2023, doi: https://doi.org/10.1016/j.inffus.2023.03.008.
[5]M. Z. Hossain, "Emerging Trends in Forensic Accounting: Data Analytics, Cyber Forensic Accounting, Cryptocurrencies, and Blockchain Technology for Fraud Investigation and Prevention," *Emerging Trends in Forensic Accounting: Data Analytics, Cyber Forensic Accounting, Cryptocurrencies, and Blockchain Technology for Fraud Investigation and Prevention*, Jan. 2023, doi: https://doi.org/10.2139/ssrn.4450488.
[6]B. Barrett, K. Dommett, and D. Kreiss, "The capricious relationship between technology and democracy: Analyzing public policy discussions in the UK and US," *Policy & Internet*, vol. 13, no. 4, Aug. 2021, doi: https://doi.org/10.1002/poi3.266.
[7]E. Onyekachukwu, P. Amajuoyi, K. B. Adeusi, and A. O. Scott, "Blockchain-driven communication in banking: Enhancing transparency and trust with distributed ledger technology," *Finance & accounting research journal*, vol. 6, no. 6, pp. 851–867, Jun. 2024, doi: https://doi.org/10.51594/farj.v6i6.1182.
[8]M. Javaid, A. Haleem, R. P. Singh, R. Suman, and S. Khan, "A review of Blockchain Technology applications for financial services," *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, vol. 2, no. 3, p. 100073, 2022, doi: https://doi.org/10.1016/j.tbench.2022.100073.
[9]N. Naderi, "Utilizing Blockchain Technology in International Remittances for Poverty Reduction and Inclusive Growth," *Economics, Law, and Institutions in Asia Pacific*, pp. 149–163, 2021, doi: https://doi.org/10.1007/978-981-16-1107-0_7.
[10]A. MUSTYALA, "Leveraging Blockchain for Fraud Risk Reduction in Fintech: Infrastructure Setup and Migration Strategies," *EPH - International Journal of Science And Engineering*, vol. 9, no. 2, pp. 1–10, 2023, doi: https://doi.org/10.53555/ephijse.v9i2.234.
[11]O. Adisa *et al.*, "Decentralized Finance (DEFI) in the U. S. economy: A review: Assessing the rise, challenges, and implications of blockchain-driven financial systems.," *World Journal of Advanced Research and Reviews*, vol. 21, no. 1, pp. 2313–2328, Jan. 2024, doi: https://doi.org/10.30574/wjarr.2024.21.1.0321.
[12]A. G. Gad, D. T. Mosa, L. Abualigah, and A. A. Abohany, "Emerging Trends in Blockchain Technology and Applications: A Review and Outlook," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 9, pp. 6719–6742, Mar. 2022, Accessed: Aug. 16, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1319157822000891
[13]O. Odeyemi, C. C. Okoye, O. C. Ofodile, O. B. Adeoye, W. A. Addy, and A. O. Ajayi-Nifise, "INTEGRATING AI WITH BLOCKCHAIN FOR ENHANCED FINANCIAL SERVICES SECURITY," *Finance & Accounting Research Journal*, vol. 6, no. 3, pp. 271–287, Mar. 2024, doi: https://doi.org/10.51594/farj.v6i3.855.
[14]A. I. Sanka and R. C. C. Cheung, "A systematic review of blockchain scalability: Issues, solutions, analysis and future research," *Journal of Network and Computer Applications*, vol. 195, p. 103232, Dec. 2021, doi: https://doi.org/10.1016/j.jnca.2021.103232.
[15]A. Abdelmaboud *et al.*, "Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions," *Electronics*, vol. 11, no. 4, p. 630, Feb. 2022, doi: https://doi.org/10.3390/electronics11040630.

[16]A. Giannaros *et al.*, "Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions," *Journal of Cybersecurity and Privacy*, vol. 3, no. 3, pp. 493–543, Sep. 2023, doi: https://doi.org/10.3390/jcp3030025.
[17]D. J. Daluwathumullagamage and A. Sims, "Fantastic Beasts: Blockchain Based Banking," *Journal of Risk and Financial Management*, vol. 14, no. 4, p. 170, Apr. 2021, doi: https://doi.org/10.3390/jrfm14040170.
[18]H. Sadri *et al.*, "Integration of Blockchain and Digital Twins in the Smart Built Environment Adopting Disruptive Technologies—A Systematic Review," *Sustainability*, vol. 15, no. 4, p. 3713, Feb. 2023, doi: https://doi.org/10.3390/su15043713.
[19]S. Rasheed and S. Louca, "Blockchain-Based Implementation of National Census as a Supplementary Instrument for Enhanced Transparency, Accountability, Privacy, and Security," *Future Internet*, vol. 16, no. 1, p. 24, Jan. 2024, doi: https://doi.org/10.3390/fi16010024.
[20]S. Banerjee, D. Das, M. Biswas, and U. Biswas, "Study and Survey on Blockchain Privacy and Security Issues," *Cross-Industry Use of Blockchain Technology and Opportunities for the Future*, 2020. https://www.igi-global.com/chapter/study-and-survey-on-blockchain-privacy-and-security-issues/254820(accessed Aug. 16, 2024).
[21]Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *Journal of Network and Computer Applications*, vol. 126, pp. 45–58, Jan. 2019, doi: https://doi.org/10.1016/j.jnca.2018.10.020.
[22]M. Shaik, "Reimagining Digital Identity: A Comparative Analysis of Advanced Identity Access Management (IAM) Frameworks Leveraging Blockchain Technology for Enhanced Security, Decentralized Authentication, and Trust-Centric Ecosystems," *Distributed Learning and Broad Applications in Scientific Research*, vol. 4, pp. 1–22, 2018, Accessed: Aug. 16, 2024. [Online]. Available: https://dlabi.org/index.php/journal/article/view/2
[23]T. Van der Linden and T. Shirazi, "Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets?," *Financial Innovation*, vol. 9, no. 1, Jan. 2023, doi: https://doi.org/10.1186/s40854-022-00432-8.
[24]W. Gaviyau and A. B. Sibindi, "Global Anti-Money Laundering and Combating Terrorism Financing Regulatory Framework: A Critique," *Mdpi*, vol. 16, no. 7, pp. 313–313, Jun. 2023, doi: https://doi.org/10.3390/jrfm16070313.
[25]M. Kasatkina, "TOWARDS THE HARMONISATION OF THE INITIAL COIN OFFERING RULES: COMPARATIVE ANALYSES OF THE INITIAL COIN OFFERING LEGAL REGULATION IN THE USA AND THE EU," *International Comparative Jurisprudence*, vol. 8, no. 1, pp. 26–47, 2022, Accessed: Aug. 16, 2024. [Online]. Available: https://www.ceeol.com/search/article-detail?id=1046384
[26]D. L. Crumbley, D. L. Ariail, and A. Khayati, "How Should Cryptocurrencies Be Defined and Reported? An Exploratory Study of Accounting Professor Opinions," *Journal of risk and financial management*, vol. 17, no. 1, pp. 3–3, Dec. 2023, doi: https://doi.org/10.3390/jrfm17010003.
[27]E. Callens and K. Löber, "The Future of Centrally Cleared OTC Derivatives Markets," *SSRN Electronic Journal*, vol. 126, 2022, doi: https://doi.org/10.2139/ssrn.4162503.
[28]B. Custers and L. Overwater, "Regulating Initial Coin Offerings and Cryptocurrencies: A Comparison of Different Approaches in Nine Jurisdictions Worldwide," *Social Science Research Network*, Dec. 20, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3527469 (accessed Aug. 16, 2024).

[29]C. J. Hoofnagle, B. V. D. Sloot, and F. Z. Borgesius, “The European Union general data protection regulation: what it is and what it means,” *Information & Communications Technology Law*, vol. 28, no. 1, pp. 65–98, Jan. 2019, doi: https://doi.org/10.1080/13600834.2019.1573501.
[30]E. A. Akartuna, S. D. Johnson, and A. Thornton, “Preventing the money laundering and terrorist financing risks of emerging technologies: An international policy Delphi study,” *Technological Forecasting and Social Change*, vol. 179, p. 121632, Jun. 2022, doi: https://doi.org/10.1016/j.techfore.2022.121632.
[31]E. Mensah, “Financially Ever After: A Thesis on Cryptocurrency and the Global Financial Economy,” *papers.ssrn.com*, Jun. 26, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3640175(accessed Aug. 16, 2024).
[32]P. K. Ozili and P. T. Iorember, “Financial stability and sustainable development,” *International Journal of Finance & Economics*, vol. 29, no. 3, Feb. 2023, doi: https://doi.org/10.1002/ijfe.2803.
[33]N. S. Uzougbo, C. G. Ikegwu, and A. O. Adewusi, “Regulatory Frameworks for Decentralized Finance (DeFi): Challenges and opportunities,” *GSC Advanced Research and Reviews*, vol. 19, no. 2, pp. 116–129, May 2024, doi: https://doi.org/10.30574/gscarr.2024.19.2.0170.
[34]H. Allioui and Y. Mourdi, “Exploring the Full Potentials of IoT for Better Financial Growth and Stability: a Comprehensive Survey,” *Sensors*, vol. 23, no. 19, p. 8015, Jan. 2023, Accessed: Aug. 16, 2024. [Online]. Available: https://www.mdpi.com/1424-8220/23/19/8015
[35]S. B. Far and A. I. Rad, “When cryptography stops data science: Strategies for resolving the conflicts between data scientists and cryptographers,” *Data Science and Management*, Mar. 2024, doi: https://doi.org/10.1016/j.dsm.2024.03.001.
[36]A. Diro, L. Zhou, A. Saini, S. Kaisar, and P. C. Hiep, “Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities,” *Journal of Information Security and Applications*, vol. 80, pp. 103678–103678, Feb. 2024, doi: https://doi.org/10.1016/j.jisa.2023.103678.
[37]S. Bansod and L. Ragha, “Challenges in making blockchain privacy compliant for the digital world: some measures,” *Sādhanā*, vol. 47, no. 3, Aug. 2022, doi: https://doi.org/10.1007/s12046-022-01931-1.
[38]A. Z. Junejo, M. A. Hashmani, and M. M. Memon, “Empirical Evaluation of Privacy Efficiency in Blockchain Networks: Review and Open Challenges,” *Applied Sciences*, vol. 11, no. 15, p. 7013, Jul. 2021, doi: https://doi.org/10.3390/app11157013.
[39]G. K. Mahato and S. K. Chakraborty, “A Comparative Review on Homomorphic Encryption for Cloud Security,” *IETE Journal of Research*, vol. 69, no. 8, pp. 1–10, Aug. 2021, doi: https://doi.org/10.1080/03772063.2021.1965918.
[40]F. Loukil, C. Ghedira-Guegan, K. Boukadi, and A.-N. Benharkat, “Privacy-Preserving IoT Data Aggregation Based on Blockchain and Homomorphic Encryption,” *Sensors*, vol. 21, no. 7, p. 2452, Apr. 2021, doi: https://doi.org/10.3390/s21072452.
[41]U. Jafar, M. J. Ab Aziz, Z. Shukur, and H. A. Hussain, “A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems,” *Sensors*, vol. 22, no. 19, p. 7585, Oct. 2022, doi: https://doi.org/10.3390/s22197585.
[42]T. Wang, Z. Liu, Z. Han, and L. Zhou, “Efficient Decision-Making Scheme Using Secure Multiparty Computation with Correctness Validation,” *Electronics*, vol. 12, no. 23, pp. 4840–4840, Nov. 2023, doi: https://doi.org/10.3390/electronics12234840.

[43]H. D. Zubaydi, P. Varga, and S. Molnár, “Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review,” *Sensors*, vol. 23, no. 2, p. 788, Jan. 2023, doi: https://doi.org/10.3390/s23020788.
[44]S. Becher, A. Gerl, B. Meier, and F. Bölz, “Big Picture on Privacy Enhancing Technologies in e-Health: A Holistic Personal Privacy Workflow,” *Information*, vol. 11, no. 7, p. 356, Jul. 2020, doi: https://doi.org/10.3390/info11070356.
[45]N. Upadhyay, “Demystifying blockchain: A critical analysis of challenges, applications and opportunities,” *International Journal of Information Management*, vol. 54, no. 1, Oct. 2020, doi: https://doi.org/10.1016/j.ijinfomgt.2020.102120.
[46]R. Wang, Z. Lin, and H. Luo, “Blockchain, bank credit and SME financing,” *Quality & Quantity*, vol. 53, no. 3, pp. 1127–1140, Aug. 2018, doi: https://doi.org/10.1007/s11135-018-0806-6.
[47]M. Śmietanka, A. Koshiyama, and P. Treleaven, “Algorithms in future insurance markets,” *papers.ssrn.com*, Feb. 05, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3802462(accessed Aug. 16, 2024).
[48]J. Crandall, “Living on the block: How equitable is tokenized equity?,” *Big data & society*, vol. 10, no. 2, Jul. 2023, doi: https://doi.org/10.1177/20539517231208455.
[49]L. Morse, M. H. M. Teodorescu, Y. Awwad, and G. C. Kane, “Do the Ends Justify the Means? Variation in the Distributive and Procedural Fairness of Machine Learning Algorithms,” *Journal of Business Ethics*, vol. 181, Oct. 2021, doi: https://doi.org/10.1007/s10551-021-04939-5.
[50]T. Le Quy, A. Roy, V. Iosifidis, W. Zhang, and E. Ntoutsi, “A survey on datasets for fairness□aware machine learning,” *WIREs Data Mining and Knowledge Discovery*, vol. 12, no. 3, Mar. 2022, doi: https://doi.org/10.1002/widm.1452.
[51]M. Nassar, K. Salah, M. H. ur Rehman, and D. Svetinovic, “Blockchain for explainable and trustworthy artificial intelligence,” *WIREs Data Mining and Knowledge Discovery*, vol. 10, no. 1, Oct. 2019, doi: https://doi.org/10.1002/widm.1340.
[52]S. Wachter *et al.*, “ARTICLE: COUNTERFACTUAL EXPLANATIONS WITHOUT OPENING THE BLACK BOX: AUTOMATED DECISIONS AND THE GDPR Length: 11071 words,” *New media & Society*, vol. 20, no. 3, 2018, doi: https://doi.org/10.1177/1461444816676645.
[53]B. Mika and A. Goudz, “Blockchain-technology in the energy industry: blockchain as a driver of the energy revolution? With focus on the situation in Germany,” *Energy Systems*, vol. 12, May 2020, doi: https://doi.org/10.1007/s12667-020-00391-y.
[54]M. Akbar, M. M. Waseem, S. H. Mehanoor, and P. Barmavatu, “Blockchain-based cyber-security trust model with multi-risk protection scheme for secure data transmission in cloud computing,” *Cluster computing*, Apr. 2024, doi: https://doi.org/10.1007/s10586-024-04481-9.
[55]J. Sedlmeir, J. Lautenschlager, G. Fridgen, and N. Urbach, “The transparency challenge of blockchain in organizations,” *Electronic Markets*, vol. 32, Mar. 2022, doi: https://doi.org/10.1007/s12525-022-00536-0.
[56]T. M. Tan and S. Saraniemi, “Trust in blockchain-enabled exchanges: Future directions in blockchain marketing,” *Journal of the Academy of Marketing Science*, vol. 51, Jul. 2022, doi: https://doi.org/10.1007/s11747-022-00889-0.
[57]M. I. Khalid, M. Ahmed, and J. Kim, “Enhancing Data Protection in Dynamic Consent Management Systems: Formalizing Privacy and Security Definitions with Differential Privacy,

Decentralization, and Zero-Knowledge Proofs," *Sensors*, vol. 23, no. 17, p. 7604, Jan. 2023, doi: https://doi.org/10.3390/s23177604.
[58]M. Jameaba, "Digitization, FinTech Disruption, and Financial Stability: The Case of the Indonesian Banking Sector," *SSRN Electronic Journal*, 2020, doi: https://doi.org/10.2139/ssrn.3529924.
[59]L. Ismail and H. Materwala, "Article A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions," *Symmetry*, vol. 11, no. 10, p. 1198, Sep. 2019, doi: https://doi.org/10.3390/sym11101198. Available: https://www.mdpi.com/2073-8994/11/10/1198/htm
[60]M. N. M. Bhutta *et al.*, "A Survey on Blockchain Technology: Evolution, Architecture and Security," *IEEE Access*, vol. 9, pp. 1–1, 2021, doi: https://doi.org/10.1109/access.2021.3072849
[61]M. Dieye *et al.*, "A Self-Sovereign Identity Based on Zero-Knowledge Proof and Blockchain," *IEEE Access*, vol. 11, pp. 49445–49455, 2023, doi: https://doi.org/10.1109/ACCESS.2023.3268768. Available: https://ieeexplore.ieee.org/abstract/document/10105959. [Accessed: Aug. 18, 2023]
[62]A. Konkin and S. Zapechnikov, "Privacy methods and zero-knowledge poof for corporate blockchain," *Procedia Computer Science*, vol. 190, pp. 471–478, 2021, doi: https://doi.org/10.1016/j.procs.2021.06.055
[63]Y. Fan *et al.*, "TraceChain: A blockchain-based scheme to protect data confidentiality and traceability," *Software: Practice and Experience*, Oct. 2019, doi: https://doi.org/10.1002/spe.2753
[64]Y. Wang and A. Kogan, "Designing confidentiality-preserving Blockchain-based transaction processing systems," *International Journal of Accounting Information Systems*, vol. 30, pp. 1–18, Sep. 2018, doi: https://doi.org/10.1016/j.accinf.2018.06.001
[65]D. K. Tosh, S. Shetty, X. Liang, C. Kamhoua, and L. Njilla, "Consensus protocols for blockchain-based data provenance: Challenges and opportunities," *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, Oct. 2017, doi: https://doi.org/10.1109/uemcon.2017.8249088
[66]N. B. Truong, K. Sun, G. M. Lee, and Y. Guo, "GDPR-Compliant Personal Data Management: A Blockchain-Based Solution," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1746–1761, 2020, doi: https://doi.org/10.1109/tifs.2019.2948287

[67]A. Hasselgren, P. K. Wan, M. Horn, K. Kralevska, D. Gligoroski, and A. Faxvaag, “GDPR Compliance for Blockchain Applications in Healthcare,” *arXiv:2009.12913 [cs]*, Sep. 2020, Available: https://arxiv.org/abs/2009.12913

[68]J. B. Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. T. Moreno, and A. Skarmeta, “Privacy-preserving solutions for Blockchain: review and challenges,” *IEEE Access*, vol. 7, pp. 1–1, 2019, doi: https://doi.org/10.1109/access.2019.2950872

[69]M. Ylianttila *et al.*, “6G White paper: Research challenges for Trust, Security and Privacy,” *arXiv:2004.11665 [cs]*, Apr. 2020, Available: https://arxiv.org/abs/2004.11665