Literature Review on the Application of Blockchain Technology Initiative

Chisom Elizabeth Alozie
School of Computer and Information Sciences, University of the Cumberlands, Williamsburg, USA

* Corresponding author. Email: calozie18274@ucumberlands.edu(C.E.A.)
Manuscript received January 31, 2025; accepted March 30, 2025; published June 23, 2025.
DOI: 10.18178/IJBTA. 2025.3.1.48-61

Abstract: This literature review examines the use of blockchain technology, specifically Zcash, in the Banking, Financial Services, and Insurance (BFSI) sector. It examines the role of Zero-Knowledge Proofs (ZKPs) in enhancing privacy and identity verification processes. The study uses data from internet sources, whitepapers, and academic publications to analyze ZKPs' potential in addressing privacy concerns. It reveals vulnerabilities in existing deanonymization techniques and the need for further refinement of Zcash's privacy mechanisms. The review also discusses the balance between transparency and confidentiality in public blockchain systems, where transaction details are visible to all participants. This transparency poses risks to sensitive data, making privacy-preserving technologies like ZKPs critical. The study concludes that zero-knowledge cryptography offers a solution to privacy and confidentiality challenges in blockchain transactions, emphasizing the need for further research to enhance these techniques, especially in the BFSI sector, where privacy and security are paramount. By examining Zcash's innovative use of ZKPs, the study contributes valuable insights into the broader implications of blockchain technology for privacy, identity verification, and secure digital transactions.

Keywords: Blockchain technology, Zcash, Zero-knowledge cryptography

1. Introduction

Blockchain was invented by Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency Bitcoin [1]. It has emerged as a transformative force across various sectors, particularly in humanitarian aid, public services, and healthcare. Its decentralized and transparent nature enhances efficiency, accountability, and trust, making it a valuable tool for social initiatives. Blockchain technology is transforming the financial sector by enhancing security, transparency, and transaction efficiency. Its decentralized nature and immutable ledger provide a robust framework for various applications, including cryptocurrencies, smart contracts, and identity verification. Blockchain integration not only streamlines operations but also fosters trust among stakeholders. Below are critical aspects of blockchain's application in finance.

1.2. Zcash Description

Zcash is a digital currency made available with a security focus. Zcash has emerged as a noteworthy advancement in the realm of virtual currency. It was designed to maintain blockchain technology's decentralized and untrustworthy nature while providing enhanced protection and security for information sharing. It uses a mechanism called Zk-SNARKs -Zero-Knowledge Succinct Non-Interactive Argument of Knowledge, which permits private transactions. In general, Zcash offers two kinds of transactions: shielded and transparent.

1.3. Zcash in the Financial Sector

This section discusses the effect of blockchain through Zcash on the financial sector.

Blockchain technology, particularly as exemplified by Zcash, is making significant strides in the financial sector by enhancing security, privacy, and efficiency. Zcash, a privacy-focused cryptocurrency, utilizes advanced cryptographic techniques to ensure transaction confidentiality while maintaining the integrity of the blockchain. This dual capability positions Zcash as a pivotal player in the evolving landscape of financial technologies. The impact of blockchain technology in the financial sector, mainly through Zcash, includes.

Enhanced Security and Privacy: Zcash employs zero-knowledge proofs, verifying transactions without revealing the sender, receiver, or transaction amount, thus ensuring user privacy. Also, the decentralized nature of blockchain reduces the risk of centralized data breaches, enhancing overall security in financial transactions [2].

Efficiency and Cost Reduction: Blockchain technology streamlines transaction processes, reducing the need for intermediaries, which lowers transaction costs and speeds up processing times. Zcash's implementation of smart contracts can automate and secure transactions, minimizing human error and increasing operational efficiency [2].

Regulatory Challenges: Despite its benefits, using Zcash raises concerns regarding the potential misuse of illicit activities, necessitating regulatory frameworks to ensure compliance and security. The evolving nature of blockchain technology presents challenges in standardization and regulation, which must be addressed to foster trust and adoption in the financial sector [3].

Enhanced Security and Fraud Prevention: Cryptographic Hashing: Zcash employs advanced cryptographic techniques that secure transactions, making it difficult for unauthorized parties to alter data [4]. The blockchain's design ensures that all transactions are recorded permanently, which helps in preventing fraud and enhancing trust among users [4].

Increased Transaction Efficiency: Smart Contracts are automated contracts that streamline processes such as margin financing and settlement, reducing the time and costs associated with traditional methods [5]. Also, for Cross-Border Transactions, blockchain can facilitate faster and cheaper international transfers, addressing inefficiencies in current banking systems.

Transparency and Market Fairness: For instance, in Open Ledgers, the transparent nature of blockchain allows all participants to access the same information, fostering a fairer market environment. In addition, suggested that immediate transaction confirmations can enhance operational efficiency and customer satisfaction in real-time updates.

Ultimately, the potential applications of blockchain in the financial sector are promising, but challenges such as regulatory uncertainty and scalability must be addressed to realize these benefits fully. Integrating Zcash into existing financial frameworks could face hurdles, but its unique features position it as an asset in the evolution of finance. Zcash draws attention to the continuous conflict between technical development and governmental regulation, even though it provides creative privacy and efficiency solutions. The long-term viability of blockchain in finance depends on striking a balance between these factors.

2. Background and Issue Description

This section explains the background and issues identified in the reviewed articles. Portuondo *et al.* [6] addressed the primary issue of ensuring privacy and confidentiality in blockchain technology. While blockchain offers transparency and traceability, it also exposes sensitive information, which can lead to privacy concerns for users. This is particularly problematic in public blockchains where transaction details are visible to all participants. Their previous initiatives have sought to enhance privacy in blockchain transactions. For instance, cryptocurrencies like Zcash and Monero utilize zero-knowledge cryptography to mask transaction details, allowing users to conduct transactions without revealing their identities or the amounts involved. These efforts highlight the ongoing struggle to balance transparency with privacy in blockchain applications. Guo *et al.* [7]

addressed significant privacy concerns in blockchain payment channels, particularly regarding the transaction amount and the relationship between the parties involved. Existing payment channel technologies, while improving scalability, do not adequately protect sensitive information, leading to potential privacy breaches. The Previous Attempt noted that several blockchain initiatives, including Zcash, Blockmaze, and Monero, have attempted to enhance privacy. These projects have made strides in addressing privacy issues in general blockchain transactions. However, they need to specifically tackle the privacy challenges associated with payment channel setups, leaving a critical gap in privacy protection for off-chain transactions. Vijay *et al.* [8] suggested that the integration of blockchain technology has raised significant privacy concerns due to its public and transparent nature. While blockchain enhances trust and accountability, it also exposes sensitive data, particularly in finance, healthcare, and identity management. Previous attempts to address these issues have included various privacy-preserving techniques, but they often need to balance transparency and confidentiality. Zero-Knowledge Proofs (ZKPs) have emerged as a promising solution, allowing for the validation of transactions without revealing underlying data. Zhang *et al.* [9] pointed out that Zcash, an altcoin of Bitcoin, aims to provide enhanced anonymity through its unique features, including shielded addresses (z-addresses) and transparent addresses (t-addresses). However, despite its design, Zcash's anonymity is still vulnerable to deanonymization techniques, which can expose user identities and transaction details. Their previous research has focused on analyzing Zcash's anonymity using methods borrowed from Bitcoin, primarily targeting transactions between t-addresses. Techniques such as address clustering and user behavior identification have been employed, but they often overlook the complexities of shielded transactions. Researchers have also noted that most users in Shielded Pool are founders and miners, which contradicts the intended privacy features of Zcash. Albuquerque and Rodrigues [10] noted that the issue is the profitability of solo mining Zcash, a cryptocurrency known for its enhanced privacy features compared to Bitcoin. The paper aims to analyze how profitable solo mining can be, particularly in the context of the minimum wage in the United States, which serves as a baseline for evaluating mining profitability. However, previous attempts to examine this issue have often focused on Bitcoin, with less emphasis on Zcash and its unique attributes, such as zero-knowledge proofs that enhance user privacy. The paper also compares Zcash against Bitcoin and other top cryptocurrencies, highlighting the need for a comprehensive analysis of mining profitability across different platforms. Roy *et al.* [11] stated that the increasing reliance on digital financial transactions has raised significant concerns regarding security and trust within the financial ecosystem. Cybersecurity threats and vulnerabilities in digital payments necessitate robust solutions to protect sensitive information and maintain transaction integrity. The Prior attempts to address these issues included various blockchain initiatives such as Zcash to enhance security and transparency. With its decentralized and immutable ledger, blockchain technology has been explored as a potential solution to mitigate risks associated with digital payments. Studies have evaluated the effectiveness of blockchain in comparison to traditional cybersecurity measures, revealing both advantages and challenges in its implementation. Joseph [12] addressed the critical balance between data privacy and regulatory compliance in blockchain-based financial systems. As blockchain technology becomes more prevalent in finance, robust data protection measures are paramount due to the sensitive nature of financial data. Previous attempts to examine this issue have highlighted the inherent tension between blockchain's transparency and the need for privacy, particularly in financial transactions involving sensitive personal information. Similar blockchain initiatives have explored Privacy-Enhancing Technologies (PETs) like Zero-Knowledge Proofs (ZKPs), which Zcash is an example of, and Multiparty Computations (MPCs). These technologies aim to provide privacy while maintaining compliance with regulatory frameworks. However, they often introduce trade-offs regarding transaction speed, gas fees, and computational load, complicating their implementation in real-world applications. Akram and Sen [13] examined the fact that the BFSI (Banking, Financial, Services, and Insurance) sector faces significant challenges in digital identity verification, primarily due to vulnerabilities in traditional systems like passwords and biometrics. These systems are often prone to security breaches and privacy concerns, necessitating a more robust solution for identity management. However, previous attempts to address these issues have included various blockchain initiatives to enhance identity verification while maintaining user privacy. For

instance, studies have explored the application of Zero-Knowledge Proof (ZKP) protocols in public blockchains to reduce the disclosure of sensitive identification data. Gross *et al.* [14] observed that the issue is the declining use of cash as a payment method and the increasing competition from Big Tech companies, cryptocurrencies, and stablecoins. Central banks in advanced economies are considering issuing Central Bank Digital Currencies (CBDCs) to address these challenges. Moreover, a significant problem is the degree of transaction privacy in CBDCs. Existing solutions often either need to improve security or provide complete cash-like privacy. This raises concerns about compliance with Anti-Money Laundering (AML) and countering the Financing of Terrorism (CFT) regulations, as fully private payment systems may conflict with these legal frameworks. Their study noted that the previous attempts to address these issues include privacy-oriented modifications of cryptocurrencies like Zerocoin and Zerocash, which aimed to enhance transaction privacy. However, these systems have not been widely adopted and often need to consider regulatory constraints. Samanta *et al.* [15] noted that many individuals need help accessing proper medical treatment due to high costs and inefficient insurance processes. Traditional healthcare insurance often involves lengthy application processes and numerous challenges, such as claim settlement and processing times, leading to financial strain and even bankruptcy for some patients. Previous attempts indicate that various blockchain initiatives have been explored to address these issues. For instance, Ethereum introduced smart contracts, which automate and enforce agreements without intermediaries, potentially streamlining the insurance claim process. Additionally, integrating blockchain technology in healthcare aims to enhance data privacy and security, as seen in using Zk-SNARKs in Zcash, which allows for secure transactions without revealing sensitive patient information (see Table 1).

Table 1. Research Gaps Identified

Ref.	Article Title	Research Gaps
[6]	Application of Zero-Knowledge Cryptography in Blockchain Technology: Guaranteeing Privacy and Data Integrity	Blockchain, like Zcash, provides traceability and transparency but also makes private data public, which may cause consumers to worry about privacy. This is incredibly challenging in public blockchains where all members may see transaction details.
[7]	Zk-SNARKs-Based Anonymous Payment Channel in Blockchain	significant privacy concerns in blockchain payment channels, particularly regarding the transaction amount and the relationship between the parties involved.
[8]	Blockchain privacy through Zero-knowledge proofs: A survey of techniques and use cases.	Blockchain, such as Zcash, increases accountability and trust, but it also makes sensitive data public, especially in identity management, healthcare, and finance.
[9]	A Refined Analysis of Zcash Anonymity	Zcash's anonymity is susceptible to deanonymization techniques, which can reveal usernames and transaction data, even with its current design.
[10]	Analyzing the Solo Mining Profitability of Zcash Cryptocurrency in the United States of America	The issue is the profitability of solo mining Zcash, a cryptocurrency known for its enhanced privacy features compared to Bitcoin.
[11]	Cybersecurity and Blockchain for Secure Financial Transactions: Evaluating, Implementing, and Mitigating Risks of Digital Payments	Concerns about security and trust in the financial ecosystem have grown significantly due to the growing reliance on digital financial transactions.
[12]	Balancing Data Privacy and Compliance in Blockchain-Base Financial Systems	Issue of critical balance between data privacy and regulatory compliance in blockchain-based financial systems.
[13]	A case study Evaluation of Blockchain for digital identity verification and management in BFSI using Zero-Knowledge Proof	Due to flaws in conventional methods like passwords and biometrics, the Banking, Financial, Services, and Insurance (BFSI) industry needs help verifying digital identities.
[14]	Designing a central bank digital currency with support for cash-like privacy	The problem is the decrease in cash payments and the rise in competition from Big Tech firms, stablecoins, and cryptocurrencies.
[15]	Application of Ethereum Smart Contract in healthcare and health insurance using Zk-SNARKsin Zcash	Many struggle to pay for necessary medical care because of exorbitant expenses and ineffective insurance procedures.

3. Research Questions

This section explores various research questions from the reviewed literature, which include the concepts of blockchain technology and Zcash. The research questions posed by [6] focus on how zero-knowledge cryptography can mitigate privacy and confidentiality challenges in blockchain technology. Specific questions include the theoretical foundations of zero-knowledge cryptography, the effective implementation of zero-knowledge protocols in blockchain systems, and the limitations and challenges associated with these cryptographic methods. The research questions posed by [7].

Paper focuses on enhancing privacy in payment channels while maintaining scalability. Key questions include the achievement of privacy and relational anonymity in payment channels and methodologies that can be employed to ensure that off-chain transactions do not reveal sensitive information about the parties involved. These questions reflect the need for a deeper understanding of privacy mechanisms in blockchain technology. Another study by [8] focuses on improving privacy in ZKPs while maintaining the integrity of blockchain systems, the implications of using different types of ZKPs, such as zk-SNARKs and zk-STARKs, on scalability and efficiency and challenges ZKPs face in terms of computational overhead and regulatory compliance. Zhang *et al*. [9] raised research questions on the enhancement of the existing clusters method to improve the clustering rate of Zcash transactions, the distribution of mining rewards, how it affects the anonymity of users in shieldedpool, and the role mining pools play in the connectivity of the Zcash transaction network. Roy and Tinny [11] posed several critical research questions, including blockchain technology to enhance the security of financial transactions, the inherent and external cybersecurity threats faced by digital payment systems, risk mitigation strategies that can be implemented to address these threats, and comparison of blockchain to traditional cybersecurity protocols in terms of efficiency and robustness. Joseph [12] focused on understanding the trade-offs between data privacy and compliance in blockchain systems. Key questions include privacy-enhancing technologies impacting transaction performance and regulatory compliance, the algorithmic biases in blockchain financial systems, how they affect different user groups, and developing a tiered privacy approach to optimize data protection based on transaction sensitivity. The research questions by Akram and Sen [13] focused on understanding the problems associated with identity privacy in public blockchain networks and how ZKP can address these issues. Specific questions include the problem of the public blockchain network in terms of identity privacy, how the zero-knowledge proof protocol addresses it, and the techno-commercial use cases of zero-knowledge proof in digital identity verification using blockchain. The primary research question addressed in the paper is whether a regulatorily compliant CBDC system can be designed to support full (cash-like) privacy using Zero-Knowledge Proofs (ZKPs). This question is crucial, given the tension between privacy and regulatory compliance. Other literature in this area has explored the balance between privacy and regulatory requirements, the effectiveness of ZKPs in ensuring transaction privacy, and the implications of decentralized finance on privacy in digital payments. The research questions by Samanta *et al.* [15] focused on the implications of using Ethereum smart contracts in healthcare insurance, particularly how they can improve the efficiency and transparency of insurance claims. Key questions include smart contracts automation in the execution of insurance policies, the role of Zk-SNARKs in enhancing privacy and security in healthcare transactions, and blockchain technology transformation in the healthcare insurance landscape (see Table 2).

Table 2. Research Questions from the Reviewed Literature

Ref.	Article Title	Research Questions
[6]	Application of Zero-Knowledge Cryptography in Blockchain Technology:	What are the theoretical foundations of zero-knowledge cryptography?

	Guaranteeing Privacy and Data Integrity	How can zero-knowledge protocols be effectively implemented in blockchain systems? What are the limitations and challenges associated with these cryptographic methods?
[7]	Zk-SNARKs-Based Anonymous Payment Channel in Blockchain	How can transaction amount privacy and relational anonymity be achieved in payment channels? What methodologies can ensure that off-chain transactions do not reveal sensitive information about the parties involved?
[8]	Blockchain privacy through Zero-knowledge proofs: A survey of techniques and use cases.	How can ZKPs enhance privacy while maintaining the integrity of blockchain systems? What are the implications of using different types of ZKPs, such as zk-SNARKs and zk-STARKs, on scalability and efficiency? What challenges do ZKPs face in terms of computational overhead and regulatory compliance? [4]. Methodology
[9]	A Refined Analysis of Zcash Anonymity	How can existing address clustering methods be improved to enhance the clustering rate of Zcash transactions? What is the distribution of mining rewards, and how does it affect the anonymity of users in shieldedpool? What role do mining pools play in the connectivity of the Zcash transaction network?
[10]	Analyzing the Solo Mining Profitability of Zcash Cryptocurrency in the United States of America	How can the mining hash rate be computed under solo mining conditions to achieve a liquid revenue equivalent to the minimum wage in the U.S.?
[11]	Cybersecurity and Blockchain for Secure Financial Transactions: Evaluating, Implementing, and Mitigating Risks of Digital Payments	How can blockchain technology enhance the security of financial transactions? What are the inherent and external cybersecurity threats faced by digital payment systems? What risk mitigation strategies can be implemented to address these threats? How does blockchain compare to traditional cybersecurity protocols regarding efficiency and robustness?
[12]	Balancing Data Privacy and Compliance in Blockchain-Base Financial Systems	How do privacy-enhancing technologies impact transaction performance and regulatory compliance? What algorithmic biases are present in blockchain financial systems, and how do they affect different user groups?

		How can a tiered privacy approach be developed to optimize data protection based on transaction sensitivity?
[13]	A case study Evaluation of Blockchain for digital identity verification and management in BFSI using Zero-Knowledge Proof	What problems does the public blockchain network have regarding identity privacy, and how does the zero-knowledge proof protocol address it [4]? What is the techno-commercial use cases of zero-knowledge proof in digital identity verification using blockchain?
[14]	Designing a central bank digital currency with support for cash-like privacy	whether a regulatorily compliant CBDC system can be designed to support full (cash-like) privacy using Zero-Knowledge Proofs (ZKPs)
[15]	Application of Ethereum Smart Contract in healthcare and health insurance using Zk-SNARKsin Zcash	How can smart contracts automate the execution of insurance policies? What roles do Zk-SNARKs play in enhancing privacy and security in healthcare transactions? How can blockchain technology transform the healthcare insurance landscape?

4. Methodology

This part examines different methods in the literature reviewed on Zcash blockchain initiatives and others [6] employed a qualitative methodology, primarily through a bibliographic review. This approach allowed for an in-depth exploration of existing literature on zero-knowledge cryptography and its applications in blockchain technology. Data collection includes various zero-knowledge cryptography protocols and their implementations in blockchain systems, mainly focusing on cryptocurrencies like Zcash and Monero. Guo *et al.* [7] utilized a quantitative methodology, specifically employing zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) to develop an Anonymous Payment Channel (zk-APC). This approach allows for off-chain transactions while ensuring privacy. The data targeted in this study includes cryptocurrency users who engage in transactions requiring both scalability and privacy. The focus is on the interactions between payers and payees within a blockchain environment, emphasizing the need for privacy in these transactions. Reddy and Duvvi [8] used qualitative methods through literature reviews that focus on theoretical frameworks and practical implementations of ZKPs in blockchain technology. Data collected includes various blockchain applications across sectors like finance, supply chain management, and healthcare, emphasizing the need for privacy-preserving mechanisms. Zhang *et al.* [9] employed a quantitative methodology, analyzing blockchain data to refine existing deanonymization techniques. They focused on a sample of 1,000 blocks to build a transaction network, which allowed for a more manageable analysis of Zcash's complex data. The study concentrated on transactions involving both t-addresses and z-addresses, particularly those related to mining pools and founders, to understand the dynamics of anonymity within the Zcash ecosystem. Moreover, Albuquerque and Rodrigues [10] employed a quantitative approach, developing an analytical model to compute the mining hash rate necessary for achieving the desired revenue. This model incorporates various parameters related to the mining process, including electricity costs and hardware expenses. Data selected for analysis includes the ten most and least expensive states in the U.S. regarding electricity tariffs, allowing for a comprehensive understanding of how these costs impact mining profitability. Roy and Tinny [11] utilized a systematic literature review methodology, categorizing studies into thematic areas such as blockchain fundamentals, cybersecurity threats, and risk mitigation strategies. The data chosen for analysis included academic journals, industry reports, and case studies that directly addressed the intersection of cybersecurity and blockchain in financial transactions. Joseph [12] employed a mixed-methods approach, combining qualitative and quantitative methodologies. This included a literature review, comparative analysis, and empirical testing on the Ethereum test network. The data collected for analysis included transaction data from Bitcoin, Ethereum, and Hyperledger, focusing on various transaction types and user demographics. Akram and Sen

[13] used a case study methodology, which allows for an in-depth analysis of blockchain use cases in digital identity verification within the BFSI sector. This qualitative approach gathered data from various internet sources, whitepapers, and academic publications. The data chosen for this study includes various segments of the BFSI sector, focusing on how ZKP can be applied to enhance identity verification processes. Gross *et al.* [14] employed a design science research (DSR) approach to develop and evaluate a holistic software-based CBDC system. This methodology allowed for a comprehensive exploration of the design and implementation of the CBDC. The data selected for evaluation included experts from various fields, such as regulation, cryptography, central banking, identity, and payments. This diverse group provided a rich collection of perspectives on the proposed CBDC system. Samanta *et al.* [15] employed a qualitative approach, analyzing existing literature and case studies on blockchain applications in healthcare insurance. This methodology allows for a comprehensive understanding of the challenges and potential solutions within the industry. The data studied includes healthcare providers, insurance companies, and patients, focusing on their interactions and experiences with traditional insurance processes and the potential benefits of blockchain technology (see Table 3).

Table 3. Methodology in the Reviewed Literature

Ref.	Method	Data collected
[6]	Qualitative method through a bibliographic review.	Various zero-knowledge cryptography protocols and their implementations in blockchain systems, focusing on Zcash and Monero
[7]	Quantitative methodology	Cryptocurrency users who engage in transactions require scalability and privacy, focusing on payers and payees within a blockchain environment.
[8]	Qualitative method through a literature review.	Various blockchain applications across sectors like finance, supply chain management, and healthcare emphasize privacy-preserving mechanisms.
[9]	Quantitative method analyzing blockchain data to refine existing deanonymization techniques.	A sample of 1,000 blocks was used to build a transaction network, which allowed for a more manageable analysis of Zcash's complex data.
[10]	Quantitative, developing an analytical model to compute the mining hash rate necessary for achieving the desired revenue.	Data selected for analysis includes the ten most and least expensive states in the U.S. regarding electricity tariffs.
[11]	Systematic literature review methodology, categorizing studies into thematic areas such as blockchain fundamentals, cybersecurity threats, and risk mitigation strategies.	Academic journals, industry reports, and case studies that directly addressed the intersection of cybersecurity and blockchain in financial transactions.
[12]	Mixed-methods approach, combining qualitative and quantitative methodologies	Transaction data from Bitcoin, Ethereum, and Hyperledger, focusing on various transaction types and user demographics.
[13]	Case study approach	Different segments of the BFSI sector, focusing on how ZKP can be applied to enhance identity verification processes
[14]	A design science research (DSR) approach to develop and evaluate a holistic software-based CBDC system	experts from various fields, such as regulation, cryptography, central banking, identity, and payments

[15]	Qualitative approach, analyzing existing literature and case studies on blockchain applications	data studied includes healthcare providers, insurance companies, and patients, focusing on their interactions and experiences with traditional insurance processes and the potential benefits of blockchain technology.

5. Data Analysis

The sections cover data analysis in the reviewed literature and revealed findings.

Portuondo *et al.* [6] revealed that zero-knowledge cryptography effectively allows parties to prove the validity of transactions without disclosing sensitive information. This capability supports the hypothesis that zero-knowledge protocols can enhance privacy in blockchain applications. The paper discusses interactive and non-interactive zero-knowledge protocols, emphasizing their practical applications and limitations. Guo *et al.* [7] studied findings indicate that the proposed zk-APC scheme successfully preserves transaction unlinkability, meaning that even if an adversary queries the blockchain, they cannot link transactions to specific parties. The research supports the hypothesis that utilizing zk-SNARKs can effectively enhance privacy in payment channels, demonstrating the potential of this technology to address existing privacy concerns. Vijay and Duvvi [8] funded indicate that ZKPs can significantly enhance privacy and security in blockchain applications. For instance, zk-SNARKs and zk-STARKs have shown promise in reducing proof size and complexity, which can improve scalability. However, challenges such as computational overhead and implementation complexity remain, suggesting that while the hypotheses regarding the benefits of ZKPs are supported, practical deployment may require further optimization. Moreover, Zhang *et al.* [9] revealed that the clustering rate of addresses improved by 9% through refined methods. Additionally, it was found that 87.5% of addresses and 25.7% of transactions could be identified, indicating significant potential for deanonymization. The study also highlighted that a substantial portion of coins sent to shieldedpool were involved in round-trip transactions, suggesting a pattern of behavior that could be exploited for deanonymization. Another article by Albuquerque *et al.* [10] indicates that Zcash has a significantly lower minimum hash rate than Bitcoin, making it a more attractive option for solo miners. Specifically, Zcash's hash rate is about eight orders of magnitude smaller than Bitcoin's across various scenarios. The analysis also reveals that Zcash is the second-best cryptocurrency for solo mining among the top ten cryptocurrencies by market capitalization, primarily due to its unique privacy features and lower capital expenditure requirements. Next, Roy and Tinny [11] funded from the literature indicated that while blockchain technology offers significant improvements in security and efficiency, challenges such as scalability, regulatory compliance, and implementation complexity remain critical hurdles. Studies also highlighted the importance of cryptographic advancements, such as zero-knowledge proofs and homomorphic encryption, in enhancing the privacy and security of blockchain transactions. Joseph [12] studied findings revealed significant trade-offs associated with implementing ZKPs, such as increased transaction times (from 5 to 12 seconds), higher gas fees (from 0.02 ETH to 0.05 ETH), and a 60% rise in computational load. Chi-Square tests indicated algorithmic biases, with low-value accounts receiving fewer transaction approvals and smaller mining pools facing reduced rewards. An article conducted by Akram and Sen [13] indicated that ZKP can effectively validate information without revealing the source, addressing privacy concerns inherent in traditional public blockchain systems. The literature reviewed supports the hypothesis that ZKP enhances identity privacy and security in financial applications. Additionally, the study highlights various use cases of ZKP in the BFSI sector, demonstrating its commercial viability and potential for widespread adoption. Furthermore, the interview findings indicated that while pseudonymization is a step toward privacy, it is insufficient. Experts emphasized the need for perfect unlikability and verifiability in transactions. The research confirmed that a CBDC system based on ZKPs could be designed to support full privacy while addressing regulatory constraints, thus supporting the initial hypothesis that such a system is feasible. In contrast, Samanta *et al.* [15] researched indicates that implementing smart contracts can significantly reduce

processing times and enhance the security of transactions. The hypotheses regarding the efficiency of blockchain in automating claims processing were supported, demonstrating that smart contracts can self-execute based on predefined conditions.

Table 4. Data Analysis and Findings in the Reviewed Literature

Ref.	Article Title	Findings
[6]	Application of Zero-Knowledge Cryptography in Blockchain Technology: Guaranteeing Privacy and Data Integrity	Zero-knowledge cryptography effectively allows parties to prove the validity of transactions without disclosing sensitive information
[7]	Zk-SNARKs-Based Anonymous Payment Channel in Blockchain	The proposed zk-APC scheme successfully preserves transaction unlinkability, meaning that even if an adversary queries the blockchain, they cannot link transactions to specific parties.
[8]	Blockchain privacy through Zero-knowledge proofs: A survey of techniques and use cases.	ZKPs (Zcash) can significantly enhance privacy and security in blockchain applications.
[9]	A Refined Analysis of Zcash Anonymity	the clustering rate of addresses improved by 9% through refined methods. Additionally, it was found that 87.5% of addresses and 25.7% of transactions could be identified, indicating significant potential for deanonymization.
[10]	Analyzing the Solo Mining Profitability of Zcash Cryptocurrency in the United States of America	Zcash has a significantly lower minimum hash rate than Bitcoin, making it a more attractive option for solo miners. In addition, Zcash is the second-best cryptocurrency for solo mining among the top ten cryptocurrencies by market capitalization, primarily due to its unique privacy features and lower capital expenditure requirements.
[11]	Cybersecurity and Blockchain for Secure Financial Transactions: Evaluating, Implementing, and Mitigating Risks of Digital Payments.	While blockchain technology significantly improves security and efficiency, challenges and implementation complexity remain critical hurdles.
[12]	Balancing Data Privacy and Compliance in Blockchain-Base Financial Systems	Significant trade-offs associated with implementing ZKPs. Chi-Square tests indicated algorithmic biases, with low-value accounts receiving fewer transaction approvals and smaller mining pools facing reduced rewards.
[13]	A case study Evaluation of Blockchain for digital identity verification and management in BFSI using Zero-Knowledge Proof	ZKP can effectively validate information without revealing the source, addressing privacy concerns inherent in traditional public blockchain systems

[14]	Designing a central bank digital currency with support for cash-like privacy	while pseudonymization is a step toward privacy, it is insufficient. The study confirmed that a CBDC system based on ZKPs could be designed to support full privacy while addressing regulatory constraints, thus supporting the initial hypothesis that such a system is feasible.
[15]	Application of Ethereum Smart Contract in healthcare and health insurance using Zk-SNARKsin Zcash	implementing smart contracts can significantly reduce processing times and enhance the security of transaction.

6. Discussions in the Literature Reviewed

This section covers the insights gained from the reviewed literature on blockchain initiation. Paper resolves that zero-knowledge cryptography can significantly improve privacy and confidentiality in blockchain environments [6]. It emphasizes the importance of developing efficient protocols that can be integrated into existing blockchain systems to address the identified challenges. The insights gained from Guo *et al.* [7] researched highlight the critical importance of privacy in blockchain transactions, particularly in payment channels. The study demonstrates that while scalability can be achieved through payment channels, privacy must not be compromised. This balance is essential for the broader adoption of blockchain technology in various applications. Research conducted by Zhang *et al.* [9] suggested that while Zcash was designed to enhance user privacy, usage patterns reveal vulnerabilities that can be exploited. Albuquerque *et al.* [10] researched indicates a need for ongoing improvements in privacy measures to protect users effectively. The research questions were effectively answered, demonstrating that Zcash offers a viable alternative for solo mining, especially in states with lower electricity costs. The hypotheses regarding Zcash's profitability were supported, indicating its potential as a competitive mining option. According to Ref. [11] article noted, the convergence of cybersecurity measures with blockchain technology presents a promising avenue for creating a fortified digital payment ecosystem. However, the literature reveals a need for regulatory frameworks that balance innovation with security requirements. Future initiatives in blockchain for financial transactions must address identified challenges, ensuring that the technology is viable and effective in enhancing security. The study by Joseph [12] emphasized the need for a carefully considered approach to balance privacy and performance in blockchain systems. It highlights the importance of addressing algorithmic biases to ensure fairness and accountability. Akram and Sen [13] researched suggest that while PETs can enhance privacy, their implementation must be optimized to mitigate scalability challenges. The insights gained from the research suggest that while ZKP presents a promising solution for identity verification, challenges remain in its implementation across different segments of the BFSI sector. The study emphasizes the need to explore ZKP applications further to realize its full benefits. According to Ref. [14], the research highlights the potential for a CBDC that balances privacy and regulatory compliance. Using ZKPs is a promising approach to achieving this balance, as it allows for enforcing limits on private payments without disclosing transaction details. The study also points to the need for future research to explore the practical implementation of such systems and their acceptance by users and regulators alike. Samanta *et al.* [15] suggested that blockchain technology, particularly through Ethereum and Zk-SNARKs, can revolutionize healthcare insurance by providing a transparent, efficient, and secure method for managing claims. This could lead to improved patient outcomes and reduced financial burdens.

7. Conclusion

The sections cover the conclusion and future work derived from the reviewed literature. The research concluded that zero-knowledge cryptography is a viable solution for addressing privacy and confidentiality issues in blockchain technology. The research questions were answered affirmatively, supporting the hypothesis that

these cryptographic methods can significantly improve transaction privacy. The paper suggests that as blockchain technology evolves, the integration of zero-knowledge cryptography will be crucial for enhancing user privacy and security. This initiative is deemed viable, with potential for further research and development in the field to address ongoing challenges such as computational efficiency and scalability. The research questions were effectively answered, and the hypotheses regarding the effectiveness of zk-SNARKs in enhancing privacy were supported. The study shows that the zk-APC initiative is a viable solution for addressing privacy issues in blockchain payment channels. Future initiatives suggest that the zk-APC initiative has the potential to significantly improve the privacy of blockchain transactions, making it a promising avenue for future research and application in the cryptocurrency space. The similarities with existing privacy-focused initiatives lie in their goals, while the differences are in the specific methodologies employed to achieve those goals. This initiative could pave the way for more secure and private blockchain transactions in the future. The reviewed literature of Ref. [8] suggested that integrating ZKPs into blockchain technology can effectively address privacy and scalability challenges. Research questions regarding the balance between transparency and confidentiality have been partially answered, indicating a viable path forward for blockchain initiatives. Also, future directions emphasize the need for optimized protocols and standardization to facilitate broader adoption of ZKPs in blockchain systems. The similarities across various studies highlight a consensus on the potential of ZKPs, while differences may arise in the specific applications and challenges faced. The initiative to incorporate ZKPs into blockchain technology appears promising, potentially revolutionizing privacy-preserving applications across multiple industries. Albuquerque and Rodrigues [10] concluded that while Zcash shows promise, future work should enhance the analytical model by incorporating variables like cryptocurrency price fluctuations and mining difficulty over time. This initiative appears viable, especially as the demand for privacy-focused cryptocurrencies grows in the blockchain landscape. The research questions posed in the literature by Ref. [11] were largely addressed, with findings supporting the hypothesis that blockchain can significantly improve the security of digital payments. However, the complexities of implementation and regulatory compliance were noted as areas requiring further exploration. While blockchain initiatives show promise, their success will depend on overcoming existing challenges and ensuring a collaborative approach among stakeholders in the financial ecosystem. Similarly, the research questions by Ref. [12] were effectively addressed, revealing the complexities of achieving optimal privacy in blockchain systems. The study concluded that ZKPs and MPCs offer substantial privacy benefits but also introduce significant trade-offs that must be managed. Future research should focus on hybrid privacy solutions and quantum-resistant cryptographic methods to enhance the viability of blockchain initiatives in financial systems. The research conducted by Ref. [13] concludes that the questions posed regarding identity privacy and the effectiveness of ZKP were adequately addressed. The findings support the hypothesis that ZKP can significantly enhance identity verification processes in the BFSI sector. Additionally, Comparatively, the literature reveals both similarities and differences in applying ZKP across various studies, indicating a growing consensus on its potential while highlighting the need for tailored solutions in different contexts. The paper stated that future initiatives to integrate blockchain and ZKP in identity verification appear viable, with the potential for significant advancements in security and user privacy in the BFSI sector. Another research question posed by Ref. [14] was effectively answered, demonstrating that a CBDC system can be designed to support full privacy while complying with regulatory requirements. The findings suggest that ZKPs can play a crucial role in this process. The study noted that compared to existing literature, this study offers a more integrated approach to privacy in CBDCs, addressing both technological and regulatory aspects. The future of this blockchain initiative appears viable, particularly as the demand for privacy-oriented digital payment solutions continues to grow. Further exploration of user acceptance and regulatory frameworks will be essential for successful implementation. The research questions by Ref. [15] were effectively answered, showing that smart contracts can streamline insurance processes and enhance data privacy. The similarities across literature highlight a consensus on the potential of blockchain in healthcare, while differences may arise in the specific implementations and technologies used. The future of this blockchain initiative appears promising, as it offers a viable solution to longstanding issues in healthcare insurance, paving the way for broader adoption and innovation

in the industry

The reviewed literature demonstrates a strong consensus on the viability of Zero-Knowledge Proofs (ZKPs), which Zcash is an example of, and related cryptographic methods in enhancing privacy and security across various blockchain applications, including financial transactions, identity verification, and digital payments. Studies by various researchers affirm the effectiveness of ZKPs and zk-SNARKs in addressing privacy challenges, supporting their potential for broader adoption in blockchain systems. Even with their potential, there are still a lot of obstacles to overcome, like scalability, regulatory compliance, and computing efficiency. To overcome these obstacles, future studies should concentrate on creating hybrid privacy solutions, optimizing protocols, and investigating quantum-resistant cryptography. Additionally, standardization and customized solutions are needed to address the distinct requirements of many industries, especially in the healthcare, BFSI, and Central Bank Digital Currencies (CBDCs) sectors. Ultimately, the studies underscore the importance of collaborative efforts between stakeholders and further innovation to ensure blockchain's continued growth as a secure, privacy-preserving technology across various sectors.

Limitations: Recent research papers on Zcash are few; other initiatives were combined.

Conflict of Interest

The author declares no conflict of interest.

References

[1] T. V. Le *et al*., "A systematic literature review of blockchain technology: Security properties, applications and challenges," *Journal of Internet Technology*, *22*(4), 789–801, 2021.

[2] K. Doshi, "The impact of blockchain technology on the financial services industry," *International Journal of Computer* Science *and* Information *Technology*, vol. 16, no. 3, 2024.

[3] W. Fan *et al*., "The application of blockchain technology in the financial field," *Advances in* Economics*, Management and Political Sciences*, vol. 92, no. 1, pp. 388–401, 2024.

[4] E. P. E. George *et al*., "Blockchain technology in financial services: Enhancing security, transparency, and efficiency in transactions and services," *Open Access Research Journal of Multidisciplinary Studies*, vol. 8, no. 1, 2024.

[5] P. Sharma, S. Gupta, and D. Kapoor, "Blockchain technology in the stock market: A deep dive into enhancing efficiency and security," *Revolutionizing the Global Stock Market*, pp. 44–59, 204.

[6] A. C. Portuondo *et al*. (2024). Application of zero-knowledge cryptography in blockchain technology: Guaranteeing privacy and data integrity. Opastpublishers.com. [Online]. Available: https://www.opastpublishers.com/open-access-articles/application-of-zeroknowledge-cryptography-in-blockchain-technology-guaranteeing-privacy-and-data-integrity.pdf

[7] Y. Guo *et al*., "Zk-SNARKs-based anonymous payment channel in blockchain," *Blockchains*, vol. 2, no. 1, pp. 20–39, 2024.

[8] M. V. B. Reddy and S. Duvvi, "Blockchain privacy through Zero-knowledge proofs: A survey of techniques and use cases," *Frontiers in Health Informatics*, pp. 8457–8469, 2024.

[9] Z. Zhang *et al*., "A refined analysis of zcash anonymity," *IEEE Access: Practical Innovations, Open* Solutions, pp. 31845−31853, 2020.

[10] G. Albuquerque and C. K. Rodrigues, "Analyzing the solo mining profitability of Zcash cryptocurrency in the United States of America," *Journal of Internet Services and Applications*, vol. 14, no. 1, pp. 21–31, 2023.

[11] A. Roy and S. S. Tinny, "Cybersecurity and blockchain for secure financial transactions: Evaluating, implementing, and mitigating risks of digital payments," *International Journal of Applied and Natural Sciences*, vol. 1, no. 2, pp. 38–48, 2024.

[12] S. A. Joseph, "Balancing data privacy and compliance in blockchain-based financial systems," *Journal of Engineering* Research *and Reports*, vol. 26, no. 9, pp. 169–189, 2024.

[13] M. Akram and A. Sen, "A case study evaluation of blockchain for digital identity verification and management in BFSI using Zero-Knowledge proof," in *Proc. 2022 International Conference on Decision Aid Sciences and Applications*, 2022, pp. 1295–1299.

[14] J. Gross, J. Sedlmeir, M. Babel, A. Bechtel, and B. Schellinger, "Designing a central bank digital currency with support for cash-like privacy," *SSRN Electronic Journal*, 2021.

[15] M. Samanta, C. Bisht, and P. Singh, "Application of Ethereum Smart Contract in healthcare and health insurance using Zk-SNARKs in Zcash," in *Proc. 2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI)*, 2024, pp. 1–6.