SECURITY & PRIVACY

Systematic Review: Comparing zk-SNARK, zk-STARK, and Bulletproof Protocols for Privacy-Preserving Authentication

Bjorn Oude Roelink[1*] | **Mohammed El-Hajj PhD**[1*] | **Dipti Sarmah PhD**[1*]

[1]SCS,EEMCS,University of Twente, Enschede, Netherlands

Correspondence
Mohammed El-Hajj PhD,
SCS,EEMCS,University of Twente,
Enschede, Netherlands
Email: m.elhajj@utwente.nl

Present address
[*]SCS,EEMCS,University of Twente,
Enschede, Netherlands

Funding information

This systematic literature review scrutinizes the implementation and analysis of zk-SNARK, zk-STARK, and Bulletproof non-interactive zero-knowledge proof (NIZKP) protocols in privacy-preserving applications across diverse sectors. Examining 43 research works published from 2015 to April 2023, we categorized findings into financial, medical, business, general, and other domains. Our analysis highlights significant variations in real-world performance across implementations utilizing NIZKP protocols. However, divergent methodologies in security analyses hindered conclusive comparisons. Addressing research gaps, our future endeavors aim to establish a real-world benchmark for these protocols.

KEYWORDS
Zero knowledge, *zk-SNARK*, zk-STARK, Bulletproof, privacy-preserving, Security analysis, Performance

[*]Equally contributing authors.

1 | INTRODUCTION

Zero-knowledge proofs (ZKPs) represent a relatively recent cryptographic innovation, initially introduced by Goldwasser et al. [1]. They enable a prover to demonstrate certain knowledge to a validator without disclosing the specifics of that knowledge. However, traditional ZKPs are interactive, necessitating multiple exchanges between the prover and verifier for trust or rejection. Additionally, these proofs cannot be reverified by other parties without initiating fresh interactions, limiting their practicality. Addressing this limitation, Blum et al. proposed Non-Interactive Zero-Knowledge Proofs (NIZKPs) [2]. NIZKPs empower a verifier to confirm a claim in a single interaction, allowing subsequent verifiers to validate the same claim later.

Notably, ZKPs, especially the non-interactive variants, have gained prominence in cryptocurrencies like ZCash and Ethereum [3]. In these contexts, they facilitate transaction verification without divulging sensitive transaction details, preserving privacy. Although cryptocurrencies have significantly bolstered the visibility of ZKPs due to the surge in blockchain technologies, their utility extends beyond this domain.

Traditional authentication methods, including password-based systems and token-based authentication, have long been the cornerstone of digital security. However, these methods are plagued by significant limitations and vulnerabilities in the face of evolving cyber threats. Password-based authentication [4], despite its widespread use, is inherently vulnerable. Users tend to choose weak passwords or reuse them across multiple accounts, making it easy for attackers to gain unauthorized access through techniques like brute-force attacks. Moreover, passwords can be easily intercepted or stolen through phishing attacks, keyloggers, or data breaches, leading to compromised accounts and sensitive data leaks. Token-based authentication [5], while more secure than simple passwords, is not immune to challenges. Physical tokens can be lost or stolen, compromising the authentication process. Additionally, time-based tokens are susceptible to interception during transmission, allowing attackers to hijack the authentication session.

Cyber-attacks have become increasingly sophisticated, leveraging advanced techniques such as machine learning algorithms and artificial intelligence to bypass traditional security measures. Attackers employ tactics like social engineering, malware, and phishing schemes that specifically target authentication processes. As a result, organizations face a constant struggle to stay one step ahead of malicious actors, requiring innovative and adaptive security solutions. In light of these challenges, there is a pressing need for authentication mechanisms that are not only highly secure but also respect user privacy. Privacy-preserving authentication [6] methods ensure that sensitive user information is not unnecessarily disclosed during the authentication process, safeguarding individuals' privacy rights. Such mechanisms often employ advanced cryptographic techniques, including zero-knowledge proofs, enabling users to prove their identities without revealing sensitive data. Authentication represents another sphere where zero-knowledge proofs can revolutionize practices. Authentication aims to confirm a person's identity without divulging specific details. ZKPs empower users to prove claims without revealing the intricacies of the proof, ensuring privacy during authentication [6]. Furthermore, ZKPs find applications in age verification, enabling users to prove they meet a specific age requirement without disclosing their exact birthdate [7], as well as in the "know your customer" process, where banks need income information without requiring the exact figure.

As the digital landscape continues to evolve, addressing these challenges becomes paramount. The development and adoption of innovative, secure, and privacy-preserving authentication mechanisms are crucial to mitigating the risks posed by sophisticated cyber threats and ensuring a safer digital environment for individuals and organizations alike. Privacy-preserving authentication is an important area of research in cryptography [8], with applications in anonymous credentials, secure voting protocols, and other areas where privacy is a concern. ZKPs are a powerful tool for privacy-preserving authentication, allowing one party to prove to another party that they know a certain piece of information without revealing the information itself. In recent years, several types of zero-knowledge proofs have

emerged as leading contenders for practical use: zk-SNARKs [9], zk-STARKs [10], and bulletproof [11]. These protocols differ in their efficiency, security, and underlying mathematical techniques, making them suitable for different types of applications. In the rapidly evolving landscape of zero-knowledge proofs and privacy-preserving authentication, there exist notable research gaps and challenges that necessitate a comprehensive review. Existing literature, while substantial, often lacks a unified synthesis and critical analysis.

One significant research gap lies in the exploration of practical implementations of zero-knowledge proofs across diverse applications that use zk-SNARKs, zk-STARKs, and bulletproof. While theoretical frameworks abound, there is a scarcity of empirical studies detailing real-world applications and their effectiveness. Additionally, the intersection of zero-knowledge proofs and emerging technologies, such as blockchain and IoT, presents unexplored avenues for research. Understanding the integration challenges and optimizing these technologies for real-time applications is an underexplored area. In the realm of privacy-preserving authentication, the integration of usability and security remains a challenge. Striking a balance between robust security measures and user-friendly experiences is a persistent gap. Furthermore, there is a scarcity of research addressing the vulnerabilities of existing privacy-preserving authentication methods to novel cyber threats. As attackers continuously adapt their tactics, it is crucial to identify potential weaknesses and develop countermeasures.

The motivation behind conducting a systematic literature review about the implementation of zk-SNARKs, zk-STARKs, and bulletproof in the context of privacy-preserving authentication is twofold. Firstly, such a review allows for the consolidation of fragmented knowledge, providing a holistic understanding of the current state of research. By synthesizing existing studies, researchers and practitioners can gain insights into successful methodologies, challenges faced, and lessons learned, paving the way for informed future research directions. Secondly, in the face of technological advancements and evolving cyber threats, staying abreast of emerging trends is imperative. A comprehensive review not only identifies gaps but also sheds light on nascent areas of research and innovative solutions. By understanding the trajectory of recent developments, researchers can align their work with contemporary challenges, ensuring that their contributions are relevant and impactful. This study conducts a Systematic Literature Review (SLR) covering the past decade, with a specific focus on the utilization of zk-SNARK, zk-STARK, and Bulletproof protocols in academic literature. The primary objective of this review is to identify, categorize, and analyze the various applications and methodologies of these cryptographic protocols in the context of privacy-preserving authentication. By undertaking this comprehensive analysis, we aim to contribute valuable insights into the evolving landscape of privacy-enhancing technologies, as evidenced by the literature. This analysis forms the core contribution of this study, offering a deep understanding of the practical implementations and challenges associated with these protocols in ensuring privacy-preserving authentication.

The structure of this article is as follows: Section 2 will design the SLR to discover the recent academic landscape regarding the implementation of zk-SNARKs, zk-STARKs, and bulletproof in the context of privacy-preserving authentication. In Section 3, we will conduct all steps of this SLR, and report their results. Next, Section **??** will summarize all articles that are the result of the SLR in the previous section. Section **??** will discuss the results achieved from the SLR and the benchmark done, and give a number of recommendations on the implementation of zk-SNARKs, zk-STARKs, and bulletproof in the context of privacy-preserving authentication. Finally, Section **??** concludes the work done.

2 | DESIGNING THE SYSTEMATIC LITERATURE REVIEW

A SLR entails a thorough analysis of existing research within a clearly defined domain, employing systematic techniques to identify, select, and evaluate relevant articles while gathering and scrutinizing data from these studies. To

ensure the rigor of an SLR, it is essential to adopt methods that are both reproducible and transparent [12]. While various types of literature reviews, like exploratory reviews, aim to uncover published theories, empirical data, and research methodologies in academic literature [13], our objective extends beyond a surface-level examination. We aim to pinpoint gaps in the current state of the art. Hence, we have opted for an SLR approach in this study. This section outlines the framework used for conducting the systematic literature review. Initially, we will craft a precise search string, employing it to query predetermined online databases. Subsequently, we will sift through articles, discarding irrelevant ones, and analyze the characteristics of the retained corpus. Lastly, we will outline the identified knowledge gaps and propose potential avenues for future research.

2.1 | Methodology

Since we have chosen to undertake a systematic literature review, it is crucial to present a detailed account of our review process to ensure the reproducibility of our results. Our process begins by integrating the research topic, context, aims, and objectives, leading to the formulation of research questions, as detailed in 2.2. In 2.3, we outline our literature collection procedure based on these research questions. Here, we craft precise search queries to locate literature relevant to our inquiries and specify the research databases subjected to these queries. Subsequently, in 2.4, we elucidate the subsequent step involving the filtration of acquired literature. This process includes the removal of duplicate sources, exclusion of materials incongruent with our topic and context, and a manual review process. The manual review involves an initial evaluation of abstracts for eligibility and a subsequent scrutiny of full texts. Only works meeting all these criteria are incorporated. Following this, information retrieval techniques are applied to the selected research. The outcomes are evaluated, and a bibliometric analysis is conducted. The final stage encompasses the creation of a comprehensive report. This document enumerates the research findings, addresses each research question, and delves into the obtained results. For a visual representation of the entire systematic literature review process,it is illustrated in Figure 1.

2.2 | Research Questions

In this subsection, we outline the key research questions that will be addressed as a result of the SLR. These questions serve as the focal points for our investigation into the implementation of zk-SNARKs, zk-STARKs, and bulletproofs in the context of privacy-preserving authentication:

1. What are the existing real-world use case implementations of zk-SNARKs, zk-STARKs, and bulletproofs in privacy-preserving authentication, as documented in the literature? How are these protocols currently being applied in practical scenarios, and what insights can be drawn from these implementations regarding their effectiveness, challenges faced during deployment, and potential improvements for broader adoption?
2. What are the comparative performance and security implications of implementing zk-SNARKs, zk-STARKs, and bulletproofs in privacy-preserving authentication systems? This includes an analysis of authentication speed, computational overhead, and resilience against various types of attacks, as well as potential vulnerabilities.

These research questions guide our systematic exploration of the literature, aiming to provide comprehensive insights into the practical applications, performance, security, user experience, and challenges associated with zk-SNARKs, zk-STARKs, and bulletproofs in the realm of privacy-preserving authentication.

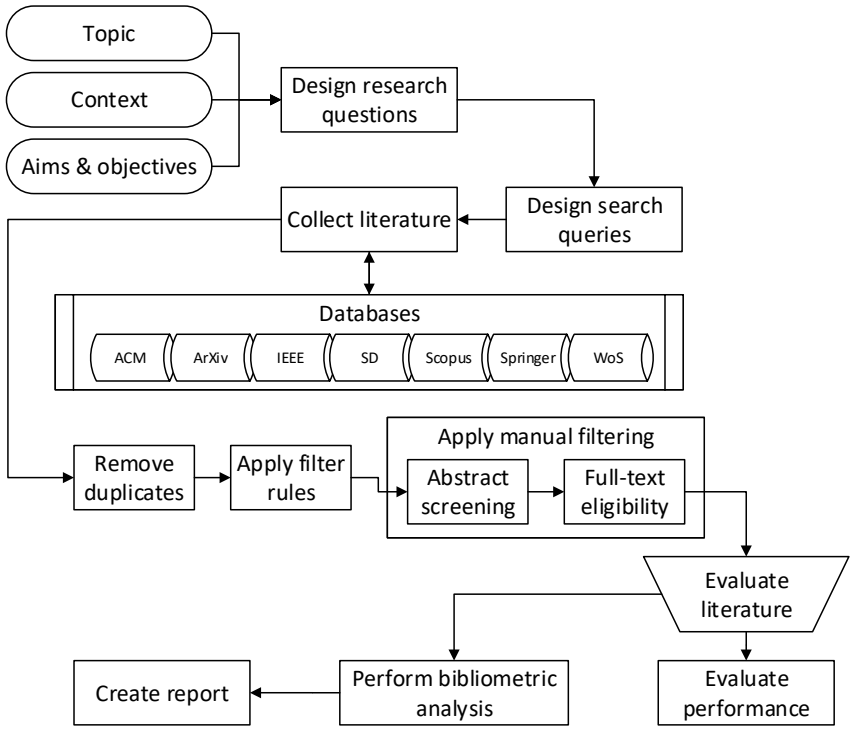

FIGURE 1 Systematic literature review process diagram

2.3 | Collecting literature

The SLR scope consists of two dimensions, namely, publication period and publication venues. Concerning the publication period, this SLR includes papers published from 2013 to 2023. The year 2013 was taken as the starting point since, from this year, research in usage of ZKPs for privacy-preserving authentication started growing. We conducted the literature search in June 2023, accepting only studies until that point. From a publication venue perspective, we searched for studies in the following databases; ScienceDirect, ACM Digital Library, IEEE Xplore, Scopus, ArXiv, Web of Science, and Springer Link. The list of included literature databases and URLs can be found in Table 1.

2.3.1 | Searching query

We seek a comparative analysis among zero-knowledge proof protocols, specifically focusing on zk-STARK, zk-SNARK, and Bulletproof protocols. To achieve this objective, our search query encompasses terms ensuring that each retrieved work discusses at least one of these protocols. We construct our query using three distinct components, combined using the OR operator:

- `("zk-STARK" OR "zk-STARKs" OR "zero-knowledge Scalable Transparent Argument of Knowledge")`

TABLE 1 Included Research Databases

Database	URL
ACM Digital Library	https://dl.acm.org
ArXiv	https://arxiv.org
IEEE Explore	https://ieeexplore.ieee.org
ScienceDirect	https://www.sciencedirect.com
Scopus	https://www.scopus.com
Springer Link	https://link.springer.com
Web of Science	https://www.webofscience.com

- `("zk-SNARK" OR "zk-SNARKs" OR "zero-knowledge Succinct Non-interactive Argument of Knowledge")`
- `("Bulletproof" OR Bulletproofs")`

Additionally, our interest extends to the application of these protocols in the realm of privacy-preserving authentication. To narrow down our search, we require that the following query components align:

- `("privacy-preserving" OR "preserve privacy")`
- `("authentication" OR "identity")`

Combining these elements, our complete query is as follows:

```
(
    ("zk-STARK" OR "zk-STARKs" OR
        "zero-knowledge Scalable Transparent Argument of Knowledge")
    OR ("zk-SNARK" OR "zk-SNARKs" OR
        "zero-knowledge Succinct Non-interactive Argument of Knowledge")
    OR ("Bulletproof" OR "Bulletproofs")
)
AND ("privacy-preserving" OR "preserve privacy")
AND ("authentication" OR "identity")
```

2.4 | Filtering literature

As mentioned in 2.3, we estimate that the collection of literature will comprise hundreds of research publications. Since these works are not yet detailed enough to be evaluated right away, we must first filter them to exclude any publications that have nothing to do with our topic or context. There are two stages to this filtering. Initially, a rule-based filter is applied. 2.4.1 has a description of this procedure. We then apply the second stage of manual filtering on the resulting collection, which is comprised of two stages: full-text eligibility assessment, which is described in 2.4.3, and title and abstract screening, which is described in 2.4.2. Figure 2 shows a PRISMA [14] flow diagram that represents the whole filtering procedure we used for the literature review.

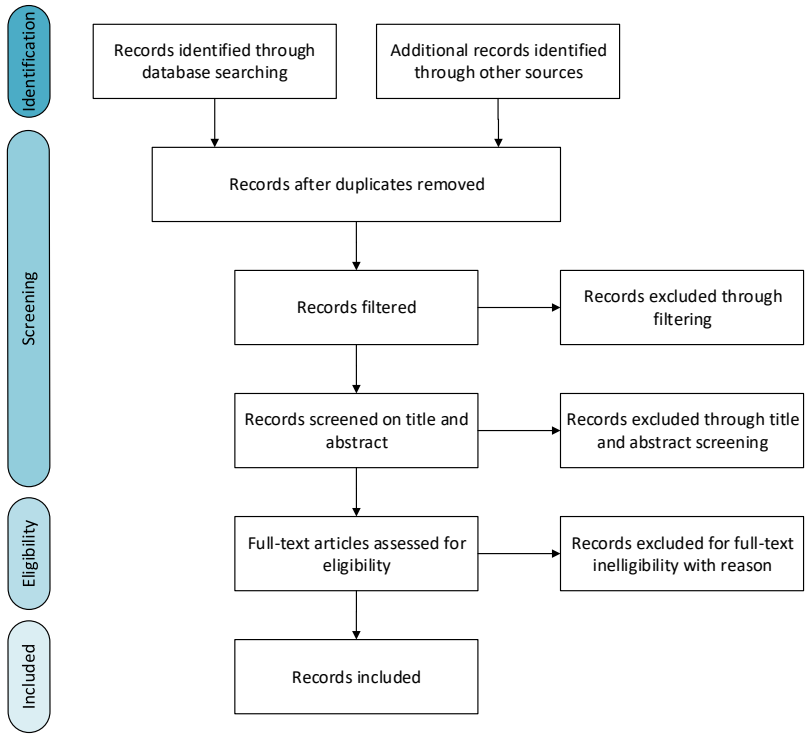

FIGURE 2 Systematic literature review PRISMA flow diagram.

2.4.1 | Rule-based filtering

Our initial filtering process is conducted through a rule-based filter, which functions based on article metadata, including factors such as content type and publication date. The criteria we have applied to this filter are documented in table 2. Any article matching one of the exclusion criteria is removed from the collection, while only articles that do not meet any of the exclusion criteria in this filter are retained.

TABLE 2 Literature filter rules

Filter	Rule
Language	Exclude research written in languages other than English
Content type	Exclude research published in a book or included as a chapter thereof
Publication date	Exclude research published before 2013
Duplicate	Exclude duplicates of a unique research

By implementing these rules, we ensured a refined collection that aligns precisely with our research criteria, enhancing the quality and relevance of the literature under consideration.

2.4.2 | Manual title and abstract screening

Following the application of the rule-based filter detailed in 2.4.1, we proceed with a manual filtering process involving the examination of each article's title and abstract. Articles that meet our predefined inclusion criteria and do not violate any exclusion criteria are retained, while others are excluded.

Our inclusion criteria encompassed the following aspects:

- The article must present or describe a use-case where zero-knowledge proofs find application.
- Privacy preservation should be the primary objective of the article. This focus can extend beyond authentication, covering any privacy-preserving application.
- The title or abstract of the article must indicate the usage or potential usage of zero-knowledge proofs. Articles that imply the use of zero-knowledge proofs, even if not explicitly mentioned, are included for further assessment during the full-text eligibility evaluation.

Conversely, we employed the following exclusion criteria:

- Articles categorized as surveys, literature reviews, or overviews are excluded, as our systematic literature review focuses on original research for evaluation rather than third-party evaluations.
- The main objective of the article should be a privacy-preserving application. Articles lacking this focus are filtered out.
- Articles introducing new zero-knowledge proof schemes are excluded. Our review specifically examines the usage of established protocols, namely zk-STARK, zk-SNARK, and Bulletproof, in privacy-preserving applications. New protocols are irrelevant as they do not pertain to privacy-preserving applications of zero-knowledge proofs.
- Articles proposing concepts (e.g., mathematical ideas) for application in other privacy-preserving techniques are not relevant to our review, as they do not directly demonstrate the application of zero-knowledge proofs in privacy preservation.
- Articles suggesting alternatives to the use of zero-knowledge proofs for specific applications are also excluded. Our review focuses on comparing the usage of zk-SNARK, zk-STARK, and Bulletproof zero-knowledge proof protocols.

These criteria guided our comprehensive evaluation, ensuring the relevance and applicability of the selected articles to our study.

2.4.3 | Manual full-text eligibility assessment

The last filtering step involves a thorough full-text eligibility assessment of the articles shortlisted after the title and abstract screening outlined in 2.4.2. We evaluated each article by examining its entire content to determine its eligibility for inclusion in our analysis, adhering to our predetermined inclusion and exclusion criteria.

Similar to the manual title and abstract screening, articles must meet all eligibility criteria to be retained. For those excluded during this assessment, we provide explicit reasons for their exclusion. We established the following eligibility criteria for articles to be included in our final evaluation:

- **Direct Usage of Zero-Knowledge Proof Protocols:** The article must directly employ one of the three speci-

fied zero-knowledge proof protocols (zk-STARK, zk-SNARK, or Bulletproof). Indirect usage, such as through a blockchain that implements zero-knowledge proofs, is insufficient.

- **In-Depth Application of Zero-Knowledge Proof Protocols:** The usage of zero-knowledge proof protocols should be substantial and profound. Mere surface-level references, like suggesting a possibility using zk-SNARKs, do not meet the criteria.
- **Primary Focus on Privacy Preservation:** The primary objective of the article should be privacy preservation, not just an unintended consequence.

These tight criteria ensure that only articles deeply embedded in the direct application of zk-STARK, zk-SNARK, or Bulletproof protocols, with a strong focus on privacy preservation, are included in our final evaluation, enhancing the relevance and integrity of our study.

2.5 | Presenting knowledge gaps and new research directions

In the final phase, we will have read and analyzed all remaining papers. With this information, we hope to identify knowledge gaps in the literature and possible new research direction.

3 | PERFORMING THE SYSTEMATIC LITERATURE REVIEW

In section 2, we outlined the systematic literature review process. This section delves into the practical execution of the methodology detailed there, presenting the outcomes of each stage. In 3.1, we present the results of our literature collection efforts from various research databases, aligning with the process elucidated in 2.3. Moving forward, in 3.2, we showcase the outcomes of filtering the discovered articles, adhering to the criteria outlined in 2.4. Lastly in 3.3, we assess the articles that remain post-filtering, following the evaluation procedure detailed in **??**. Upon concluding this section, we possess the necessary data to present the results of our systematic literature review and engage in a comprehensive discussion, as outlined in section **??**.

3.1 | Collecting literature

In this section, we outline our approach to literature collection. Our process initiates by querying research databases, following the search parameters detailed in 2.3.1. The outcomes of our search queries for each database are documented in Table 3. The numbers listed in the *Results* column represent the total findings encompassing various forms of references, including conference proceedings. However, for our systematic literature review, we focus solely on related articles and, therefore, exclude collections like conference proceedings. The count presented in the *Articles* column represents the identified records that align with our research scope.

3.2 | Filtering literature

In the previous section 3.1, we discussed our process of collecting literature. Now, we move forward by detailing the filtering phase, a crucial step in refining our research scope. Notably, not all literature records retrieved are equally applicable to our study. To enhance the quality of our research and narrow down our focus, we apply filtering strategies as outlined in 2.4. Our filtering process begins with rule-based filtering, described in 2.4.1. By applying predefined

TABLE 3 Number of Articles identified using the Search Query

Database	Results	Articles
ACM Digital Library	64	60
ArXiv	0	0
IEEE Explore	5	5
ScienceDirect	76	76
Scopus	19	16
Springer Link	256	114
Web of Science	9	9
Total	**429**	**280**

filter rules (as depicted in 2), we reduced the initial pool of 280 records to 245, excluding duplicates, specific content types, outdated publications, and non-English articles as presented in Table 4. Next, we perform manual filtering,

TABLE 4 Number of articles removed through rule-based filtering

Filter	Filtered	Included	Excluded
Duplicate	280	262	18
Content type	262	246	16
Publication date	246	245	1
Language	245	245	0
Total	**280**	**245**	**35**

involving title and abstract screening, followed by a comprehensive full-text eligibility assessment, detailed in 2.4.2 and 2.4.3 respectively. The result of this manual filtering process is presented in 5. The entire filtering process as

TABLE 5 Number of articles removed through manual filtering

Filter	Filtered	Included	Excluded
Title and abstract screening	245	126	119
Full-text eligibility assessment	126	43	83
Total	**245**	**43**	**202**

conducted, including the number of literature articles included and excluded in each step, is illustrated in Figure 3.

Upon completing the filtering process, we were left with 43 included research results. These selected works exhibit a balanced distribution between conference papers (56%) and journal articles (44%), reflecting the diversity in scholarly publications as illustrated in Figure 4a. Further analysis of our included literature reveals interesting patterns in terms of source libraries. Significant contributions stem from ACM Digital Library (30%), Springer Link (28%), and ScienceDirect (23%), signifying their prominence in zero-knowledge proof research for privacy-preserving appli-

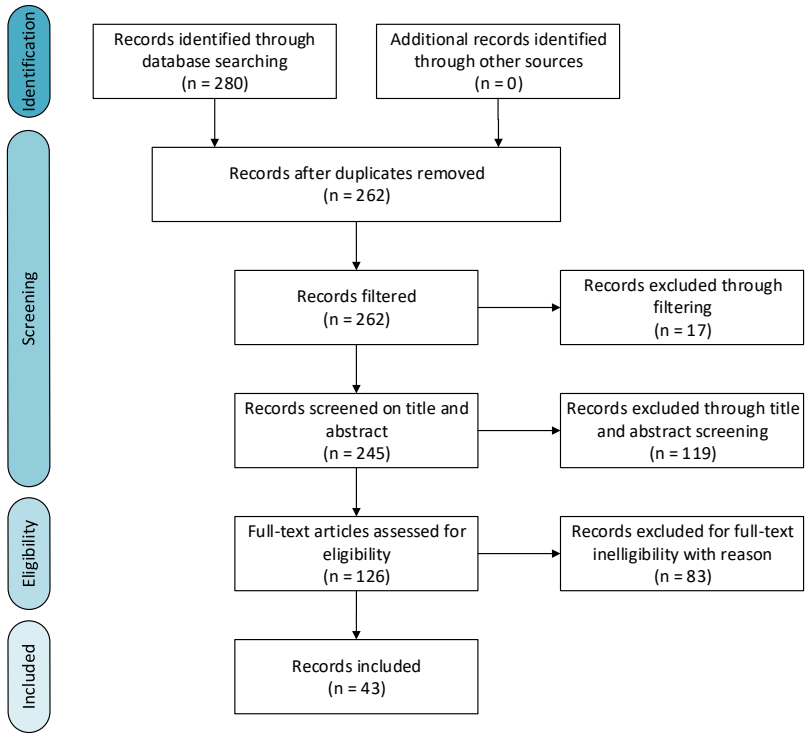

FIGURE 3 Filled systematic literature review PRISMA flow diagram

cations as illustrated in Figure (4b). Notably, the prevalence of certain keywords, such as "blockchain," underscores the evolving landscape of zero-knowledge proofs, primarily within blockchain technologies. Additionally, the dominance of terms like "privacy," "zero-knowledge proof," and "authentication" echoes our research focus as illustrated in 6. Figure 5 shows the number of included research literature, including the type, by year of publication. We must note that the literature collection was performed on March 31, 2023. This means that the year 2023 in the figure only represents research published in the first quarter of that year. The graph shows a clear increasing trend in the total number of published research on the topic of zero-knowledge proofs for privacy-preserving applications, at least for research that meets our inclusion criteria. This trend can be explained by the young mathematical foundation behind the technology that is ZKPs, next to an increasing interest in its application for privacy-preserving uses in an ever more digital society.

Figure 6 shows the co-occurrence graph of keywords that occur at least twice in the included literature. This graph clearly shows that "blockchain" is the most prevalent keyword among the works included in our systematic literature review. We can explain this difference by the main application of zero-knowledge proofs currently being in blockchains, the technology behind cryptocurrencies. The prevalence of this keyword combined with the interest in cryptocurrencies in the past few years also helps explain the rise in the number of research published in the past few years, as seen in 5. The high occurrence of other keywords including "privacy", "zero-knowledge proof", and "authentication", is also logical since these terms are what we searched for when collecting the literature. The three

(a) Research Type Distribution

(b) Included Articles by Library Catalog

FIGURE 4 Distribution of the Included Articles

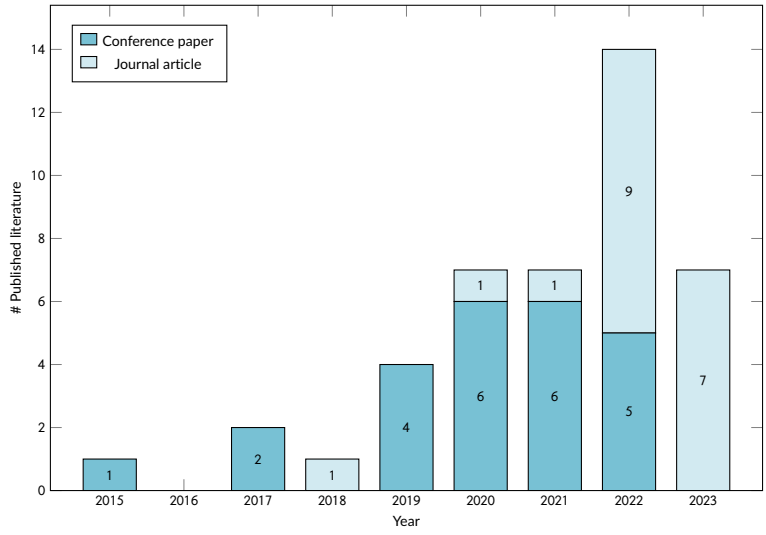

FIGURE 5 Number of research included by year of publication

specific zero-knowledge proof protocols "zk-SNARK", "zk-STARK" and "Bulletproofs" are less prevalent, which we can explain by research proposals using just one of these three protocols. Of the three protocols "zk-SNARK" appears the most, which we can explain by it being the oldest and most popular protocol of the three.

Figure 7 shows the co-authorship graph of authors that collaborated with each other, within the group of authors that authored included research works. This graph has 39 clusters, which means that of the 43 included papers and articles, most authors are only connected to authors of the same paper. This seems to indicate that authors of research within our inclusion criteria do not collaborate often. Combined with the results illustrated in Figure 5 however, it can also show that the relevant research field is young and has not had the time to explore follow-up research. Such follow-up research can combine the knowledge of researchers from different domains interested in the topic of zero-knowledge proofs. This limits the degree of connectivity in the co-authorship graph. A third explanation is that the authors of included papers are not mainly interested in zero-knowledge proofs, but in the different applications in which they apply zero-knowledge proofs to achieve an objective. Applications in entirely separate research domains can in that event be a disincentive for collaboration. The latter explanation seems probable given that our search query

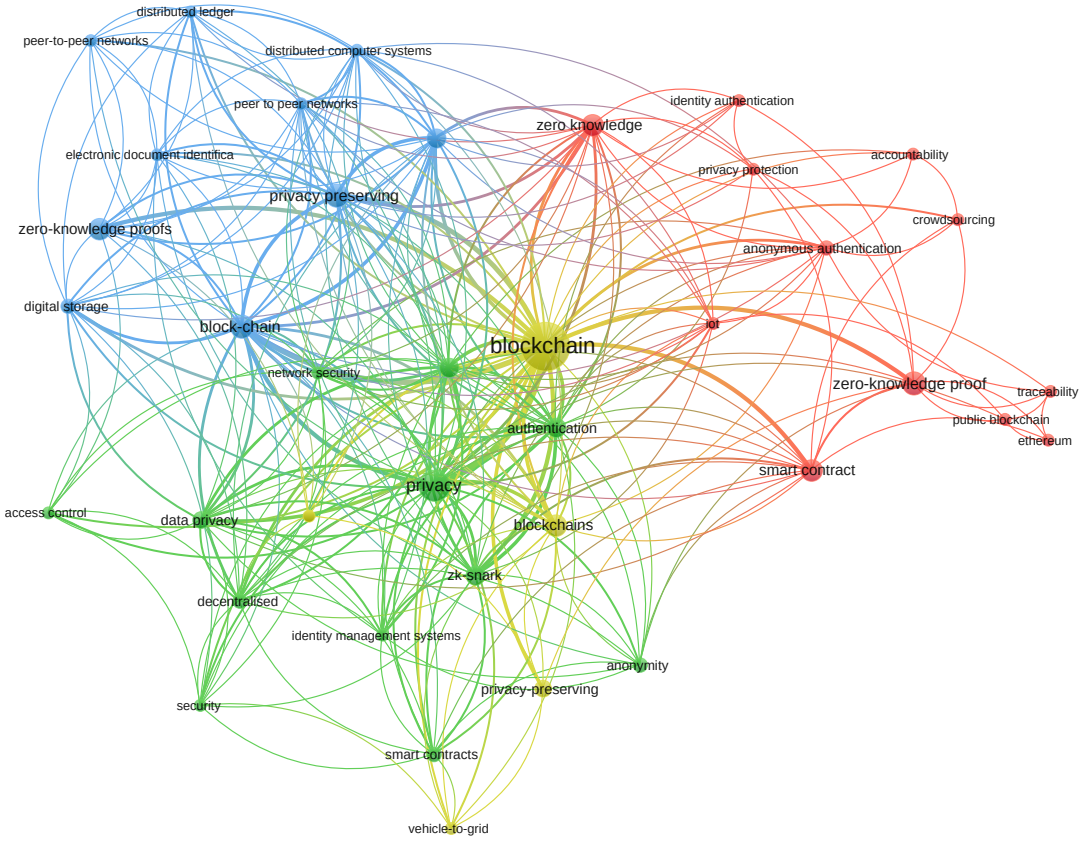

FIGURE 6 Keyword co-occurrence graph of keywords that occur at least twice in the included literature

and filtering criteria look for different privacy-preserving applications that apply zero-knowledge proof protocols for privacy preservation.

3.3 | Evaluating literature

In this section, we outline the process of evaluating the literature included in section3.2. Initially, the literature was categorized broadly, with each category representing a specific use case for the applications included. This categorization aids in organizing the findings within the results and discussion section, linking them to their respective use cases and illustrated in Figure 8. It's worth noting that this categorization is not always precise, as some research works could fit into multiple categories. However, each piece of research is placed in the category we deemed most fitting for the presented solution.

Each category of literature was evaluated based on the methodology described in the following sections, and the findings are summarized in Table 6. The table includes the following abbreviations:

- **Ref.** - Reference; Details and source of the work
- **Application** - The application for which the research work proposed a solution using zero-knowledge proofs

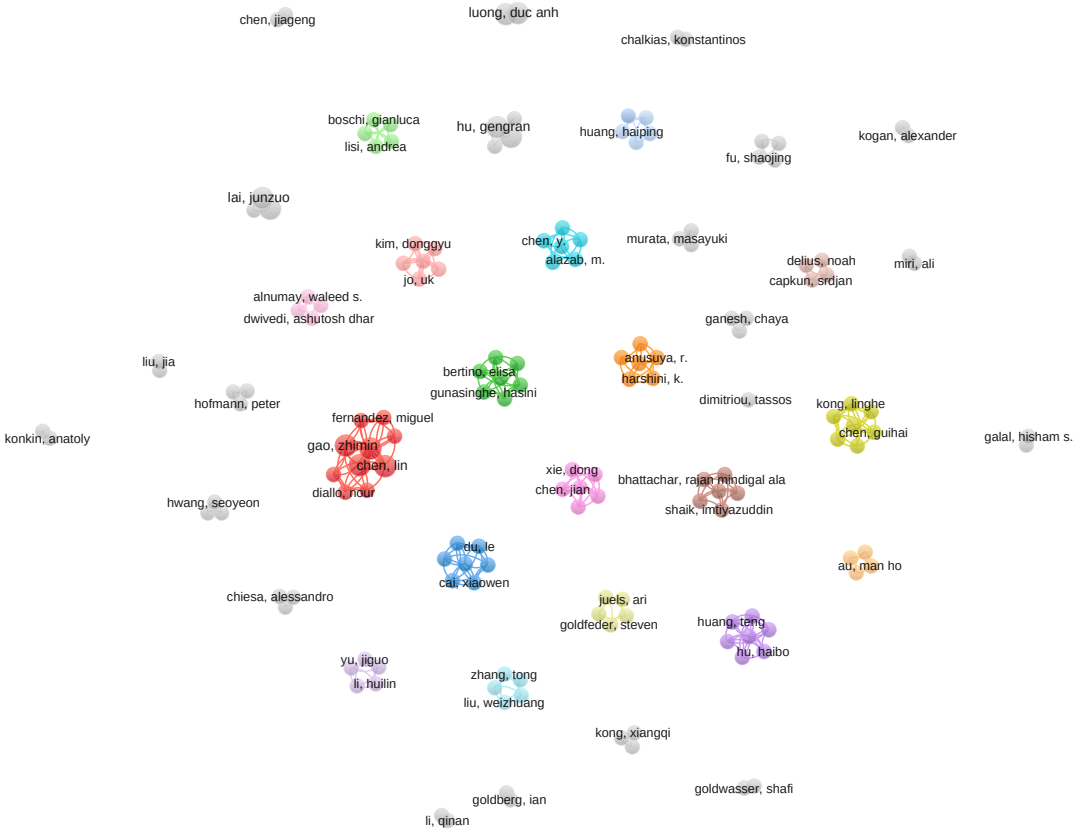

FIGURE 7 Co-authorship graph of included literature

- **Use case** - Our use case grouping of the application
- **Protocol** - The non-interactive zero-knowledge proof protocol used in the proposed solution
- **Analyses** - The types of analyses performed in the work
  1. **S** - Security analysis
  2. **SC** - Security analysis, including a comparison with other works
  3. **P** - Performance analysis
  4. **PC** - Performance analysis, including a comparison with other works
  5. **C** - Cost analysis
  6. **CC** - Cost analysis, including a comparison with other works
- **Strengths & weaknesses** - Our findings on the strengths and weaknesses of the work

In the 'Strengths & weaknesses' column of the literature benchmark pesented in Table 6 we include the following:

- Whether the researchers included an implementation of the proposed solution and whether they published this implementation.
- Whether the authors mentioned the limitations of the proposal.

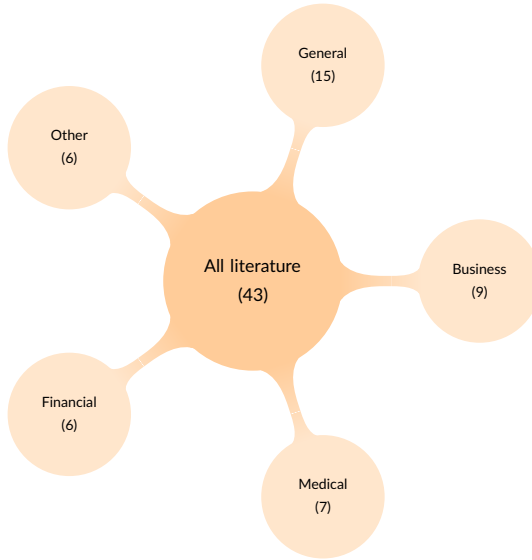

FIGURE 8 Research Use Case Categorisation

- Whether the authors mentioned any future research directions.
- Whether the authors mentioned the quantum resistance of the proposal.

3.4 | Financial

In this section, we thoroughly examine and assess various research papers within the Financial category.

- In [15] the authors proposed PGC (pretty good confidentiality), a standalone cryptocurrency based on a decentralized confidential payment (DCP) system. PGC offers transaction anonymity and confidentiality, while conforming to regulatory compliance requirements by adding auditability. A new public-key encryption called twisted ElGamal is used to add zero-knowledge proofs like Sigma protocols and Bulletproofs to prove transaction correctness while preserving privacy. The generic DCP system uses an integrated signature and encryption (ISE) scheme and non-interactive zero-knowledge proof (NIZKP) systems. Sigma protocols prove linear relations, while Bulletproofs prove value intervals. The twisted ElGamal encryption scheme enables the use of both protocols.
  The authors included a brief performance analysis that included proof size and transaction times for the generation and verification of different policy types in PGC. However, the authors also referred to a full version of their work which included an exceptionally extensive benchmark of the different parts of PGC. This full version also included a comparison of the proposed scheme against two other account-based DCPs, zkLedger [16] and Zether [17]. The full version of this work also included a security analysis of the DCP construction which described the correctness of the generic DCP by first listing a theorem and then proving it. The authors did not conclude the paper with specific benefits or limitations of PGC, and neither did they provide any future directions. However, from the other content in their work, we could conclude that the main benefits of GCP were the security, privacy, and auditability aspects of the scheme.

- In [18] the authors propose a decentralized netting protocol for inter-bank payments, addressing the challenges of traditional RTGS systems due to single point of failure and trust issues. The protocol, combined with ElGamal encryption and zero-knowledge proofs, ensures settlement correctness, prevents permanent gridlocks, and preserves user privacy, thereby enhancing the security of inter-bank payments. The proposal uses ElGamal encryption to encrypt payment instructions, requiring the correct private key for successful decryption. Participants use zero-knowledge proofs like zk-SNARKs to verify submitted instructions and account balances. Blockchain technology, specifically smart contracts, is used for verifications, Merkle trees calculation, and account balance updates. Participants can prove knowledge of incoming payment instructions without disclosing transaction details. The authors conducted a cost analysis of Ethereum Gas for submitting and updating transactions on the Ethereum "Istanbul" fork, indicating that while the protocol is practical for deployment on Ethereum, it may perform better on permissioned blockchains.
  While the main benefit of the proposed protocol was that it could resolve gridlocks in inter-bank payments while being decentralized, confidential, and privacy-preserving, the authors did mention some limitations to the protocol. These limitations included the need for all banks to be online for the settlement and a privacy leak in the protocol that could worst-case be exploited to successfully break anonymity. Resolving the latter limitation required modifications to the zero-knowledge proof in the update transaction, which the authors left for future works. Other suggested future research directions included investigating better proving times and a transparent setup method.

- In [19] the authors propose zkChain, a privacy-preserving model for efficient asset transfer using zk-SNARKs and one-way hash chains. They aim to reduce the proof size and verification times while ensuring the anonymity and privacy of participants. zkChain expresses account balances using one-way hash chains, with the last hash serving as public input and the preimage as private input. Provers can use zero-knowledge proofs to prove ownership, and the blockchain records account balance proofs for traceability.
  An included performance analysis existed of two parts. In the first part, the authors compared the key generation, proof generation, and verification times for two different machines and listed the proving key and proof sizes. Regarding the results, the authors explained that the slower proof generation was not a problem for the system since only a single user performed it. While each participant had to perform the proof verifications, these verifications were much faster to perform than generating said proof. The transaction latency and send rate for an increasing number of participating nodes, along with the transaction delay for an increasing send rate, were displayed in the second part of the performance analysis. The outcomes demonstrated that while a higher send rate had no effect on performance, a higher node count had a negative effect. Additionally, the authors included a security analysis that analysed the privacy and attack resistance aspects of zkChain. This analysis described how zkChain guaranteed the zero-knowledge balance and transaction linkability aspects while being resistant to double-spending and over-spending attacks. In the end, the authors concluded that the performance of zkChain was its main competitive advantage compared to other solutions, while the techniques used in zkChain simultaneously prevented overspending attacks.

- In [20] the authors proposed a blockchain-based transaction processing system (TPS) to improve business communication and trading efficiency. However, they faced concerns about data confidentiality. They proposed a solution using homomorphic encryption and zero-knowledge proofs, ensuring only authorized entities could view private transaction data, addressing the main concern in previous works. The proposal used homomorphic encryption to encrypt transaction information in the Bb-TPS to guarantee confidentiality. As a result of using

homomorphic encryption, the system could still perform mathematical operations, like calculating the new account balance, on the encrypted transactions while the encryption hid the transaction contents. However, since the transactions were encrypted, it was hard to provide transparency as well. To this end, the proposal used zk-SNARKs as zero-knowledge proofs to prove and verify statements on the transaction without revealing any transaction details. These proofs provided the transparency required in the proposal. The accompanying performance analysis, which displayed the computation time and record size for a growing number of completed transactions, assessed the effectiveness of a prototype implementation. For the same quantity of transactions, the writers also included a performance summary for a SQLite database. However, no comparison with other Bb-TPS systems was done.
In conclusion, the main benefit of the proposed system was tamper resistance, data confidentiality, and improvements in accounting and auditing efficiency and effectiveness. These benefits however came with the downside of the computational overhead imposed by the blockchain. Other limitations of the current proposal included that no details were provided on the block mining and reward mechanisms, nor on the zk-SNARK implementation. The authors finally mentioned the development of blockchain-based continuous monitoring systems as a promising future research direction.

- In [21] the authors proposed Platypus, a central bank digital currency (CBDC) designed to offer privacy, scalability, and regulation. It combines e-cash transaction processing with ledger-based fund management, providing privacy guarantees and simple regulatory enforcement. Platypus' CBDC trust model with a central authority eliminates privacy and performance limitations of previous designs. The main enabling technology is zk-SNARKs, which verify transaction validity by the central bank. The security analysis included in the paper analysed transaction integrity, transaction privacy, fund availability, and regulation integrity and privacy. For each of these requirements, the authors first stated a definition, then stated a claim based on that definition, and subsequently proved the claim.
  Additionally, the authors conducted a performance analysis. This analysis listed the trusted setup, proving, and verification times, as well as the number of constraints and the transaction size. These aspects were included for the base transaction and transactions with additional regulations. The proving times of the scheme were three to four orders of magnitude higher than the verification times, while the trusted setup takes an order of magnitude longer than generating a proof. The exact results however differed based on the used devices and elliptic-curve algorithms. To conclude, the authors mentioned the main benefit of Platypus was that, given the trust model of CBDCs, Platypus was able to provide all the desirable CBDC features of privacy, performance, scalability, and regulation using an e-cash-like system.

- In [22] the authors propose PrivateEx, a privacy-preserving scheme for exchanging assets. Unlike centralized platforms, PrivateEx uses zero-knowledge proofs to ensure fairness and correctness without publicly exposing all exchange information. This approach addresses privacy challenges faced by centralized platforms that require trust and expose all exchange information. PrivateEx uses zero-knowledge proofs, specifically zk-SNARKs, to ensure fairness, correctness, and privacy in asset exchanges. These proofs are publicly shared and verified using blockchain technologies, which also store exchanged assets. A security analysis outlines the system requirements and how PrivateEx ensures these requirements.
  Additionally, the authors included a performance analysis that evaluated the performance of different zk-SNARK circuit designs on the number of constraints, proving and verifying key sizes, and proof generation times. The authors additionally remarked the verification times to be constant in the number of constraints. The main ben-

efits of PrivateEx were the fairness, and correctness guarantees of the scheme, combined with the preservation of privacy during asset exchanges. In the conclusion the authors briefly mentioned that using Bulletproofs could have improved performance, however they did not elaborate on this.

3.5 | Medical

This section discusses and reviews case studies under the Medical category.

- In [23] the authors propose a blockchain-based system for securely storing electronic health records (EHRs) to address privacy and security concerns. EHRs are widely used in health institutions for access to accurate information, but they can be hacked, limiting patient access. The proposed solution ensures privacy through zero-knowledge proofs, adding immutability, authenticity, and accountability. The protocol uses the zk-SNARK zero-knowledge proof protocol for authentication, enabling patients to verify their doctor's medical license, insurance, and prescription. This method maintains privacy-sensitive data without revealing the data. Smart contracts are used for functions like adding doctors, inserting EHRs, viewing EHRs, and sending prescriptions. These actions are recorded on the blockchain as events. The system combines the interplanetary file system (IPFS) with blockchain to store encrypted EHRs in a distributed manner.
  The authors evaluated the system performance of the proposed system using a simulated local blockchain called Ganache, while they used a "calliper" to record the performance of the smart contract implementations of Hyperledger Sawtooth and Ethereum. The resulting performance metrics, which demonstrated the latency and throughput figures for different send rates, were included in a performance analysis. Besides the performance figures of the smart contract implementations, however, the authors did not analyse other performance aspects or the security of the system. In conclusion, the authors mentioned that the main benefit of the proposal was that patients had unrestricted access to their EHRs, while the system guaranteed the privacy and consistency of the EHRs. The authors finally suggested research into the application of the proposed paradigm in areas besides healthcare as a future research direction.

- In [24] the authors propose a privacy-preserving data-market platform for medical data, particularly for machine learning and AI research. They use zero-knowledge proofs and blockchain technologies to ensure privacy, verify data validity, and offer monetary incentives for data sharing, addressing patient resistance to data misuse and lack of transparency. The proposed platform uses blockchain technologies to deploy smart contracts that automatically update a machine learning model based on personal data contributions. These contracts also automatically remunerate participants for data contributions, protecting patient privacy. The platform uses zk-SNARKs for zero-knowledge proofs to validate the accuracy of contributed parameters. The smart contracts update the model on the distributed ledger only if the validation succeeds.
  The authors did not include a performance or security analysis according to our definition; however, they instead provided a detailed mathematical description of the quadratic span problem in the zk-SNARKs. In conclusion, the authors mentioned that the main benefit of the proposed solution was the automated way researchers could update their machine-learning models with verified contributed patient data. The ability to do this using real data was partially a result of the main benefit for patients, namely privacy protection and remuneration, which increased the willingness of patients to contribute. The authors finally briefly mentioned the research into the further applicability of blockchain technology as a future research direction but without more details.

- In [25] the authors propose a privacy-preserving blockchain-based scheme for securely sharing medical data between patients and research institutions. They argue that existing systems struggle with patient reluctance and the need for certainty in the usefulness of the information. They propose a solution that combines blockchain technologies with zero-knowledge proofs, aiming to address issues like anonymous secure authentication and uncertainty in the applicability and correctness of received information. This approach aims to create a secure and private medical data-sharing system. The proposed scheme uses zk-SNARKs to generate proofs of data requirements without disclosing them, and for patients and health institutions to verify submitted data conformity. A blockchain smart contract verifies these proofs, and if successful, encrypted data is uploaded to a semi-trusted server for decryption. The transaction is verified and published on the blockchain for finalization and recording. The research conducted a security analysis on the proposed solution, highlighting its ability to achieve confidentiality, availability, integrity, privacy preservation, and traceability, while also preventing single points of failure.
  Next to the security analysis, the research included a performance analysis evaluated on a test implementation. This analysis listed for different numbers of circuit inputs the key generation, proof, and verification times, as well as the proving key, verification key, and proof sizes. The performance analysis additionally compared these performance factors against PGHR [26], which showed favorable results for the proposed solution in the key generating keys and proving phases but unfavorable results for verifications.
  The researchers compared a proposed scheme to three other ones on computation costs, startup nodes, and privacy protection. They concluded that the main benefits were privacy protection and data availability and consistency. They suggested future research should focus on optimizing implementation efficiency and ensuring the scheme can resist conspiracy attacks.

- In [27] the authors propose a secure protocol for genomic range queries between users and testing facilities, aiming to improve privacy and efficiency while preserving security. They use cryptographic commitments, zero-knowledge range proofs, and homomorphic encryption to achieve their desired functionality. Cryptographic commitments involve committing the positions of genome mutations at the sequencing lab, while zero-knowledge range proofs use bulletproofs to prove the positions of the first two mutations outside the queried range. Additionally, homomorphic ElGamal (AH-ElGamal) is used as the most efficient homomorphic encryption scheme for similarity testing, allowing users to decrypt the total value to calculate the similarity score. This approach addresses the tension between privacy and security in genomic range queries.
  The authors evaluated the proposed protocol through performance and security analyses, comparing it to alternative homomorphic encryption schemes AH-ElGamal and Paillier. They also assessed the system's authenticity, completeness, and user privacy requirements, providing proof of how the implementation met these requirements. Some of the limitations of the system included that the used additive homomorphic encryption did not support all types of genomic tests and that the protocol only supported the single-nucleotide polymorphism (SNP) genomic representation. Furthermore, the authors avoided discussing low-level security problems such as side-channel attacks. Contrarily, the main benefit of the proposed protocol was that it was an efficient protocol that accounted for security and privacy requirements. While the proposed protocol focused on revealing plaintext SNP representations of genomes, the protocol was mentioned to be equally applicable to encrypted genomes.

- In [28] the authors propose a blockchain-based privacy-preserving contact tracing system for tracing infectious diseases. Traditionally, in-person interviews were unreliable and time-consuming. Smartphones enable automated contact tracing using location-based or contact-based methods, but these are privacy-sensitive and reduce user privacy. The proposed system aims to solve these issues by generating zero-knowledge range-proofs

to check user contact without revealing their precise locations. The proposed system uses bulletproof zero-knowledge range proofs to prove a user's location range, hashed and stored on the blockchain. Users who are confirmed infected disclose their location range during a specific period. Other users can verify their location ranges using verified ranges. Users without overlaps can submit new range proofs. Blockchain addresses are used as substitutes for real user identities to hide their identities. The proposed system's security analysis outlines assumptions and guarantees for location privacy, anonymous identification, verification information exposure, and false positives. Performance analysis of a test implementation on Hyperledger Fabric reveals that response times increase linearly with the number of apps (users), highlighting the system's security measures.
The system's performance could have been improved by ensuring user privacy and addressing performance issues with large users. Additionally, the system could not verify the validity of location data from sensors on user devices. The authors suggest researching ways to verify this data validity as a future research direction. Despite these limitations, the proposed solution hid user locations and allowed users to prove their distance from infected users using their footprints.

- In [29] the authors propose a privacy-preserving, blockchain-based healthcare system for IoT devices, ensuring secure and private sharing of health data. While cryptographic techniques can implement security, privacy is difficult without a trusted third party. Blockchain-based systems remove the need for a trusted third party and add anonymity, but their public nature introduces new privacy challenges. Zero-knowledge proofs solve these problems, creating private and secure healthcare systems on the blockchain. The proposal solution uses blockchain technology, including smart contracts, to provide a distributed platform with strict data integrity guarantees. Blockchain addresses act as pseudonyms, while smart contracts run computations and verify zero-knowledge proofs, such as zk-SNARKs, for authentication to the HSP and IoT devices. Common cryptographic techniques like digital signatures, hash functions, and Diffie-Hellman key exchange are used. The proposed system met user anonymity, authentication, and confidentiality requirements through a security analysis, which was demonstrated through security theorems and security games. Furthermore, The performance analysis of the system using the Ropsten [30] testnet blockchain network evaluated the initialization, proof, and verification of zk-SNARKs for various user numbers. The authors also conducted a cost analysis of interactions with the smart contract, revealing Ethereum gas costs and conversions.
  In conclusion, the main benefit of the proposed system was that it enabled the secure and private sharing of health data between IoT devices and health service providers, without the need for third parties. The authors did mention some limitations of the current system, including the high computational power requirement and the high costs for device management. To minimize these downsides, the authors proposed research into lower computational power requirements and the usage of non-EMV blockchain networks as future research directions.

- In [31] the authors propose a privacy-preserving medical insurance claim scheme using blockchain technology and zero-knowledge proofs, addressing existing complex, unreliable, and data leaky schemes and addressing fraud concerns in medical insurance purchasing and claiming scenarios. The proposal aims to implement a smart contract system for insurance purchases using blockchain technologies, zk-SNARK zero-knowledge proofs, Schnorr protocol, Fiat-Shamir heuristic method, and homomorphic encryption based on Decisional Bilinear Diffie-Hellman (DBDH). These technologies verify the identity and medical data of patients, initiate insurance claims, generate new medical data, and inform the insurance company to transfer money to the patient. A security analysis of the proposed scheme is also included, providing a security definition and proof for both. The work additionally included a performance analysis of the proposed system, which evaluated the performance using a test imple-

mentation of the system on a locally running private Ethereum test network. This analysis showed the proof generation and verification times for increasing numbers of inputs, message sizes, and ID bit sizes. Also included in the performance analysis was a brief comparison to ADSNARK [26], which showed that the proposed solution had comparatively lower proof generation times. The higher verification times of the proposal on the other hand were justified by the authors because the proposal performed additional verifications not included in ADSNARK. Finally, a brief cost analysis showed the Ethereum transaction fees in gas for deposits, proof requests, and verification requests. In conclusion, the main benefit of the proposed solution was that it included the properties of authentication correctness, completeness, and perfect zero-knowledge. Through these properties, the system protected patients' privacy and guaranteed the legitimacy of user identities.

3.6 | Business

The business category is reviewed and discussed in this section considering the following research papers:

- In [32] The authors propose a record-keeping infrastructure that uses blockchain technology, zk-SNARKs, and commitments to achieve privacy, public auditability of secret data, accountable deletion, and succinctness. This solution addresses the issue of encryption preventing governance and ensuring transparency and accountability in government agencies. The infrastructure preserves privacy by encrypting data and committing to them, which can be opened to prove compliance. The commitments are recorded on the blockchain, making them public and immutable. Zero-knowledge proofs, specifically zk-SNARKs, are used to prove compliance with secret regulations. A commitment is created for each secret regulation, which is then used to prove compliance using the secret regulation commitments. Finally, the authors discussed several ways to utilize or reduce the fees involved in adding records to the blockchain. One of the considered options was to let miners guarantee the correctness of the zk-SNARK in the record before it was appended. In this case, a fee had to be appended to the record for each regulation the record did not comply with, which would act as a penalty for not guaranteeing compliance with those regulations. We inferred from the contents of the proposal that the main benefit was that the system was the first auditable record-keeping system that ensured compliance with secret regulations while preserving the privacy of records in the system.

- In [33] The authors propose AMLChain, a transaction confidentiality and integrity-preserving system for institutions implementing anti-money laundering and know-your-customer practices. This system uses blockchain-based distributed identities and security techniques, including zero-knowledge proofs and digital signatures, to improve the effectiveness of these practices while preserving user privacy, thereby reducing the cost and incompatibility of existing AML solutions. The proposal uses ElGamal asymmetric encryption for transaction signing and verification, uploading information to a public ledger using blockchain technologies. Pedersen commitments hide transaction amounts, while Bulletproofs provide zero-knowledge range proof for transaction validity. These proofs help identify suspicious transactions and ensure funds remain within a certain value range, enabling the identification of suspicious transactions. The included security analysis showed in five lemmas [34] that AMLChain was secure and private when the security assumptions of the used technologies held. Also included in the security analysis was a comparison to several other schemes that compared the sender, receiver, and transaction privacy aspects as well as the efficiency and the support for transaction graphs, transaction identification, and privacy audits.
  While the comparison to other schemes included the scheme efficiency, the performance of the proposed scheme

was not analyzed but only briefly discussed. In this discussion AMLChain was mentioned to perform comparably to FabZK [35], which itself had a throughput several orders of magnitude higher than zkLedger [16]. In conclusion, the main benefit of AMLChain compared to alternatives was that AMLChain included several privacy features and showed improved efficiency.

- In [36] the authors propose DAPOL+, a proof of liability (PoL) scheme that extends the existing DAPOL (distributed auditing proofs of liabilities) protocol to provide provable privacy and security. Traditional liability-proving schemes lack correctness guarantees and allow auditors to learn sensitive information. DAPOL+ adds formal PoL definitions and security proofs to prove its strong privacy and security, improving the overall security of the scheme. The proposal employs sparse Merkle trees (SMTs) alongside homomorphic Pedersen commitments and Bulletproofs as zero-knowledge range proofs. In DAPOL+, the prover commits total liabilities, each user confirms their amount. The SMT accumulates liabilities, allowing the prover to prove total liability by revealing the root node's blinding factor. Bulletproofs ensure validity without overflow. The paper highlights the security of DAPOL+ and provides a separate chapter analyzing its failure probability, focusing on the possibility of the prover manipulating or discarding individual liabilities without detection. The authors developed a proof-of-concept implementation of DAPOL+ and conducted a performance analysis, revealing proving times, verification times, and proof sizes for various aggregated ranges. They suggested optimizations like trading larger proof sizes for faster proof generation.
  According to the authors, the main benefit of DAPOL+ was that it implemented a PoL protocol with provable security and privacy. While a downside of DAPOL+ was that discarded liabilities of users that never verified remained undetected, the authors thoroughly discuss the probability of a system failure caused by such alterations. The authors finally proposed the formal treatment of additional features for particular applications as a future research direction.

- In [37] the authors proposed the usage of zero-knowledge proofs for corporate networks. Private transactions on the blockchain remained an open security concern, even though certain businesses had previously used blockchain technologies to give transaction traceability and to do away with the requirement for a trusted third party. Existing attempts to provide private transactions had limitations in decentralized storing and immutability verifications, both key factors of blockchain. By using zero-knowledge proofs the authors attempted to solve the limitations of private transactions on the blockchain for corporate use. However, the research only shallowly discussed the application of zero-knowledge proofs and otherwise described how previous implementations worked. Given that the authors kept the discussions on the level of a general idea and that the contents did not describe details of a specific application, we should not have included this research according to our filtering rules. Consequently, we have retroactively removed it from our analysis.

- In [38] the authors proposed an advanced zero-knowledge ledger system that was based on zkLedger [16]. Traditional blockchain-based ledgers showed privacy issues, which the previous work zkLedger solved using zero-knowledge proofs. However, the main downside of the zero-knowledge range-proofs used in zkLedger was the resulting slow performance. By replacing the range-proof in the existing zkLedger system, the authors of this proposal made the proof and verification times of zkLedger five times faster and enabled further efficiency improvements by aggregating multiple range-proofs into one. The main enabling technology in the proposal was the Bulletproof zero-knowledge proof protocol, which replaced the previous range-proof scheme in zkLedger based on Borromean ring signatures. Provers used the Bulletproofs to generate proof that their secret data value

lay within a certain range without revealing the value. The prover then submitted the proof to the verifier for verification. The main benefit of the proposed solution was the improved system efficiency achieved through the reduction of the proof size using Bulletproofs. This improvement lowered the required memory and computational power requirements, which was especially useful for resource-constrained devices such as sensors and mobile devices. The authors finally suggested the actual implementation of the proposed improvement in the zkLedger prototype as a research direction for future work.

- In [39] The authors propose a privacy-preserving, traceable supply chain system on the public permissionless blockchain (PPBC), which improves existing PPBC-based systems by concealing private information and preserving privacy. This solution, using encryption and zero-knowledge proofs, addresses the issue of public readable private information in PPBC-based systems.
  The proposal uses elliptic curve ElGamal encryption to encrypt the owner's blockchain address using the manufacturer's public key, allowing tracking of products. Zero-knowledge proofs, zk-SNARKs, are used to ensure product distribution without leaking information. A secret token is shared between the owner and recipient, ensuring correct distribution while keeping blockchain addresses hidden. Smart-contract blockchain technology manages manufacturer information and zero-knowledge proof verification.
  Included in the research was a security analysis, in which the authors verified the traceability and privacy-preserving aspects of the proposal. To do so they first mentioned the possible attack vectors on traceability and privacy and then described why these attacks would fail. One of the attacks, a collusion attack between the owner and recipient, was still able to succeed. The authors proposed to investigate countermeasures to this attack in future research. Additionally, the authors conducted an evaluation of a test implementation on the Ethereum blockchain. Using this evaluation, a cost analysis was included that showed the Ethereum gas costs for different steps in the system for manufacturers and owners/recipients.
  While the main benefits of the systems included that the system achieved privacy preservation, enabled traceability, and prevented unauthorized distribution, there were also some downsides. The relatively high Ethereum gas cost was one, while another downside was that owners could be inferred from the execution of smart-contract execution history. I.e., the proposal did not preserve privacy at a protocol level. To resolve this privacy problem the authors suggested the preservation of privacy at the protocol level as a future research direction. Two other suggested future research directions included a scope increase by reducing transaction fees, and a system extension to deal with product assembly and disassembly.

- In [40] the authors propose PRC, a privacy-respecting contract platform for blockchain-based sharing economy applications. They aim to improve privacy for involved parties while maintaining the desired features of blockchain-based systems. They use three main technologies: commitments, Zk-SNARKs, and blockchain technology. Commitments commit a time-slot reservation or payment with a random value to the blockchain, hiding the committed values. Zk-SNARKs prove a party knows the random number of valid commitments, enabling verification. Blockchain technology validates and records commitments in an immutable and publicly visible manner.
  The use of blockchain technology prevented double usage, i.e. renting a property to multiple users at the same time. Furthermore, proxy agents were used to execute the contracts and remove the connections to real identities. The work included security and performance analyses. In the security analysis, the authors described how double usage attacks were prevented and how the system guaranteed the privacy of users and property owners. The performance analysis existed in two parts, the first of which was a discussion on the blockchain in which the authors stated that the throughput of blockchain could be a problem for the demands of certain sharing econ-

omy applications. The second part showed a performance evaluation of the zk-SNARK scheme, which was the most computationally expensive primitive in the PRC platform. The evaluation showed the key generation, proof generation, and verification times, as well as the proof size, and was performed for a 128-bit security level using a 1-million-gate circuit and 1000-bit inputs.
While the main benefit of the proposal included that the system preserved the privacy of owners and users while functioning on the blockchain, there were also some downsides to the system. These downsides included the fixed contract durations and pricing, as well as the missing support for a privacy-preserving rating and recommendation system. The authors finally proposed to remove one of the downsides of the proposed system by adding a rating and recommendation system as a future research direction. They furthermore proposed to include more operations in the system and to evaluate the possibility of recovering links to actual identities as other future research directions.

- In [41] the authors propose zkrpChain, a privacy-preserving data-auditing solution based on the Hyperledger Fabric consortium blockchain. Unlike existing solutions, zkrpChain keeps transactor identities public while hiding transaction details for privacy. This allows for arbitrary-range audits and joint audits on data from multiple parties, making it suitable for scenarios like food safety supervision. The main difference between arbitrary-range zero-knowledge proofs and standard-range ones is that arbitrary-range proofs prove values within a smaller range.
For the system design the authors used the Hyperledger Fabric and blockchain technologies such as smart contracts to perform distributed tasks including initialization, retrieving range limits, and performing verification of submitted proofs. Bulletproofs, the chosen zero-knowledge range proofs, were used to generate proofs that the underlying data was within a certain value range without revealing the value itself. Contrary to the "one-prover-one-verifier" mode, the "multi-prover-one-verifier" had a dealer peer aggregate proofs from multiple provers before the (combined) proof was uploaded to the public ledger.
The research included a security analysis that first described the threat model for zkrpChain, after which the security mechanisms in zkrpChain that prevented these threats were described. The authors conducted a performance analysis of zkrpChain, a system implemented on Hyperledger Fabric, comparing its execution time and on-chain storage space usage to regular Bulletproofs on standard-range proof sizes. They noted that comparisons to alternative systems were not possible due to the lack of similar functionality in zkrpChain. The comparison to regular Bulletproofs showed that zkrpChain produced larger proof sizes because of the inclusion of intermediate challenges and the usage of a less efficient library implementation. In conclusion, the main benefit of zkrpChain was the support for the generation and verification of arbitrary-range zero-knowledge range proofs, while another great benefit was the aggregation of multiple proofs into one for improved efficiency and system applicability.

- In [42] the authors propose a blockchain-based sealed-bid auction protocol to address issues like collusion, ring bidding, and information leakage. The proposed solution aims to be privacy-preserving and publicly verifiable, but faces challenges like high communication costs, making it difficult to apply to large-scale auctions with multiple bidders. The proposal aims to achieve privacy and public verifiability through Pedersen commitments, blockchain technology, and zero-knowledge proofs. Pedersen commitments enable participants to commit bids, while bulletproofs prove the value within a certain range. Range proofs announce auction winners without leaking other information. Blockchain technology ensures transparent, publicly verifiable, and irreversible transactions without a trusted third party.
The included security analysis consisted of three parts. The first two parts were on correctness and privacy preservation, in which the authors described a theorem and subsequently provided proof of the theorem. The

third part of the analysis described how the proposed scheme met the requirements of public verifiability, fairness, and non-repudiation of bidders and auctioneers. Additionally, the authors conducted a performance analysis for an off-chain implementation, focusing on proving and verifying times of bids with increasing bit-lengths and bid aggregation and win verification times for increasing bidding participants. They also conducted an Ethereum gas cost analysis for each number of bidding participants, finding the scheme's cost acceptable from 512 participants. The practicality for use in real-world applications enabled through the reduced complexity and communication costs of the proposed solution, was also the main benefit of the proposed solution.

3.7 | General (multiple use cases)

In this section, we discuss multiple use cases that can fit into more than one category as suggested.

- In [43] the authors proposed a zero-knowledge proof system for use in cluster computing, with a focus on the MapReduce cluster computing technique. The authors designed the proposal to prove the correctness of an output computed by a cluster node, without leaking the used private input data. By ensuring the zero-knowledge proof itself was also a cluster computation, the proposal solved existing challenges in generating such proofs in parallel in a cluster computing setting. The proposal introduced a bootstrapping theorem that used zk-SNARKs to obtain multi-predicate proof-carrying data (PCD) systems. These PCD systems were subsequently used on compliance predicates to obtain distributed zk-SNARKs. Cluster computing systems could then compute the resulting distributed zk-SNARK using the MapReduce technique. Given however that the proposal focused on the bootstrapping techniques for generating distributed zk-SNARKs, it did not comply with our manual filtering criteria of proposing a direct, privacy-preserving application of zk-SNARKs. We therefore concluded that in hindsight we should not have included this research in the manual filtering step, and consequently, we removed it from this analysis.

- In [44] the authors proposed a new architecture integrating the self-sovereign identity (SSI) model into attribute-based access control (ABAC) systems. The introduced architecture implemented the Extensible Access Control Markup Language (XACML) standard and was proposed as an improvement to centralized ABAC systems where attribute managers managed and disclosed data without control for the user. To achieve their objectives the authors used zk-SNARKs in the proposal to prove the result of a function over an identity attribute, without disclosing the attribute information. The research analyzed the performance of the proving key and circuit, cost analysis, and security analysis of the proposed system. It revealed that deployment and evaluation operations were more expensive on the Ethereum blockchain compared to Polygon or MATIC chains. The study also highlighted potential attacks and their mitigation strategies, demonstrating the system's security.
  Attribute confidentiality, user control, and XACML compliance were the main benefits of the proposed system. Finally, the authors mentioned future research directions which included making further improvements to the performance and compatibility of the proposed system, as well as researching setting attribute disclosure constraints that guarantee a desired level of privacy.

- In [45] the authors propose a privacy-preserving reputation scheme for collaborative systems using pseudonyms to allow private interaction. This prevents reputation reset by using a new pseudonym, addressing issues with malicious users removing bad reputations. The proposal also addresses user reluctance to give negative feedback due to fear of retaliation. By using reputation tokens with blockchain ledgers and zero-knowledge proofs, the

scheme addresses these issues without a trusted third party and includes public verifiability.
The proposed solution uses Pedersen commitments, zk-SNARKs, and blockchain technology to create reputation tokens. The blockchain acts as an append-only ledger, ensuring reputation tokens are only added and not altered. Pedersen commitments create reputation tokens with a user's secret key, serial number, random, and unique identifier. Reputation updates involve creating new tokens with an incremented serial number and a zero-knowledge proof. Zk-SNARKs prove committed attributes and pseudonyms belong to the same person. The scheme also allows peers to prove lower reputation bounds instead of the actual reputation. The research involved a security and performance analysis, with the authors presenting security and privacy theorems and providing proofs. Further details can be found in the full version of the paper. In the performance analysis, the authors showed the performance of the zk-SNARKs for the mint and update statements respectively, which each listed the key generation times, proving and verification times, and proof sizes.
The authors proposed using a trusted platform module (TPM) to replace registration tokens and prevent Sybil attacks. They proposed two methods: bind identities to human beings, which is Sybil-proof but requires personal information access, or bind identities to devices, which is more private but allows attackers to create multiple identities. In conclusion, the main benefit of the system was that it ensured the privacy and forward anonymity of users in the reputation scheme, while it prevented Sybil attacks and other reputation-based attacks. A future research direction proposed by the authors was to research securely combining update transactions without posting these update transactions to the blockchain, which would help increase the efficiency of the scheme.

- In [46] the authors proposed a privacy-preserving version of the proof of stake (PoS) consensus protocol Ouroboros Praos. PoS protocols proved to be a promising alternative to the proof of work (PoW) consensus protocol that induced high computational power and energy usage. However, PoS protocols proposed in existing works came with the downside of disclosing the identity and wealth of the stakeholders. This made PoS protocols unsuitable for privacy-preserving cryptocurrencies. In this research, the authors proposed the notion of an "anonymous verifiable random function" (AVRF) to create a private proof of stake (PPoS) protocol. In short, hiding stakeholder wealth required identity anonymity since otherwise the "win" frequency would have leaked the wealth of that stakeholder.
  The proposal utilized zero-knowledge proofs, sigma protocols, Pedersen commitments, and Merkle trees as main technologies. Participants in the PoS protocol committed a stake using Pedersen commitments. Sigma protocols were used to prove a stake won the lottery, and the winning stake owner had to prove ownership using Merkle trees. The stake used in the winning lottery proof corresponded to the user's signature and AVRF keys, revealing a valid path to claim membership. Zk-SNARK zero-knowledge proofs were generated to validate the path and membership without revealing the leaf node. The proposal did not provide a security analysis.
  The authors furthermore did not include a performance analysis, limitations section, conclusions, or future research directions.

- In [47] the authors proposed PrivIdEx. PrivIdEx used blockchain and zero-knowledge proofs to enable private identity information exchange between service providers in a secure and privacy-preserving manner, all without a centralized broker. The proposed solution reduced the number of costly user verifications, currently performed by each service provider separately for the same user, through the reuse of verifications performed by other services. PrivIdEx used zk-SNARKs as zero-knowledge proofs to prove that an identity satisfied the verification requirements while guaranteeing privacy and security. The Hyperledger Fabric was then used to perform such verification without a central broker.

The authors included a security analysis for the protocol and the users' privacy, which included proof that the stated security and privacy requirements hold. Also included was a performance analysis that analyzed circuit size, runtime, and storage requirements for varying identity asset and nonce sizes. The authors listed different versions of PrivIdEx with incremental security and privacy guarantees, each using a different circuit. Performance results for the different circuits were included in the analysis. The proposed PrivIdEx system offers anonymity and unlinkability guarantees, ensuring the confidentiality of party identities. To enhance its applicability, the authors propose two future research directions: integrating PrivIdEx with Hyperledger Fabric's identity-mixer-based certificate authority to prevent collusion attacks, and generalizing PrivIdEx for other confidential assets.

- In [48] the authors proposed a biometric identification scheme based on zk-SNARKs that prevented biometric template information leakage. The proposed scheme was a solution to schemes that stored biometrics templates directly, which were insecure and schemes that applied feature transformations or biometric encryption, which showed reduced identification accuracy. By using zk-SNARKs the proposed scheme could create proofs that collected fingerprint features matched a known biometric template without leaking said biometric template. Blockchain technology was additionally used to provide transparency on access policy evaluations and to prevent tampering. The security analysis included in the research described the security aspects of the system and showed the correctness of the proposed solution regarding the security aspects. The performance analysis of the proposed scheme demonstrated that the threshold size and number of fingerprint features impact accuracy and false rejection rate. The scheme's execution times increased linearly with the number of fingerprints, while accuracy remained constant.
  The efficiency and privacy protection aspects of the proposed scheme were seen as its main benefits. However, to improve the usefulness of the scheme the authors mentioned some future research directions including designing protocols based on the proposed scheme, further improving the scheme's efficiency, and designing application scenarios.

- In [49] the authors conceptualized accountable attribute-based authentication with fine-grained access control (AccABA). Subsequently, they proposed an attribute-based, fair, anonymous, and publicly traceable crowdsourcing scheme on the blockchain using AccABA. With the introduction of AccABA the authors solved the privacy problems posed by regular authentication schemes, as well as the accountability and trusted third parties problems in anonymous authentication schemes. To ensure that a ciphertext could be decrypted only for users matching the access policy, AccABA used Ciphertext-policy attribute-based encryption (CP-ABE). Then using zk-SNARKs a match with the access policy could be proven without disclosure of the user attribute values.
  A security analysis was included which described security properties that the system had to conform to, as well as proofs on how these security properties were fulfilled. The security analysis included a comparison of the properties (e.g. anonymous, fair, accountable) of the proposed system with several other crowdsourcing systems [50] [51] [52] [53] [54]. Aside from the security analysis, the authors did not include other analyses including the performance analysis. Such analysis was likely not included because the researchers did not implement an experimental system implementation to conduct the performance analysis. The authors mentioned the combination of privacy, accountability, and fairness as the main benefits of the system.

- In [55] the authors proposed LaT-Voting, an anonymous and traceable decentralized voting scheme that is based on the blockchain. Traditional e-voting systems were dependent on a centralized platform which introduced the risk of tampering. Blockchain-based solutions contrarily aimed to solve this problem but were in turn unable to

detect double-voting. The introduced notion of "prefix-based linkable-and-traceable anonymous authentication" used in LaT-Voting aimed to solve both the tampering and double-voting, while the scheme preserved user privacy and did not require a trusted third-party. The proposed solution uses zk-SNARK zero-knowledge proofs and smart contracts in blockchain technology to implement functionality. Smart contracts collect cast ballots, verify their validity, and detect double-voters. Blockchain addresses serve as pseudonyms for user identities, enabling vote immutability and public verification of the voting process. Voters register with a certificate authority, obtain a certificate with keys, and generate an authentication token using a zk-SNARK. The generated tokens are verified for validity, and if two tokens have a common prefix, they are considered double-votes. The public key is derived from the secret key obtained from combining two different authentications from a single voter.
The research included a security analysis in which the authors described the correctness of the proposed solution. The authors also explained how the scheme obtained the desired privacy, anonymity, unforgeability, public verifiability, and traceability features. They further proved the correctness and security of the scheme. For the security, they did so by first describing a theorem for unforgeability, anonymity, linkability, and accountability, after which they proved the four theorems and concluded the security of the proposed scheme. In conclusion, the main benefit of the LaT-Voting scheme was that it enabled decentralized and anonymous voting, while it was able to detect double-votes and trace them back to a malicious voter.

- In [56] the authors introduced a privacy-protecting authorization system that leveraged blockchain technology and the zk-SNARK protocol. By ensuring that sensitive attribute data remained undisclosed the proposal addressed a critical concern with existing authorization solutions for blockchain resources. The system employed zk-SNARKs to generate authorization proofs based on identity attributes, ensuring that attribute values were not revealed. Ethereum smart contracts then verified the correspondence between the blockchain address used during proof creation and the proof user, thereby limiting authorization usage to the proof generator.
  The authors conducted a cost analysis that demonstrated the relatively higher expense of their proposed system compared to alternative solutions such as UPort [57] and EverSSDI [58]. Additionally, a security analysis was included which outlined potential attacks on the proposed solution including tampering with credentials and smart contracts. However, the authors proved these attacks to be computationally or practically infeasible. While the primary advantage of the proposal highlighted by the authors was privacy protection, its major drawback was the substantial operational cost. To mitigate this expense, the authors suggested future research directions involving the utilization of alliance chains instead of the main Ethereum blockchain.

- In [59] the authors propose BIMP, a blockchain-based incentive mechanism for location proofs, to address privacy concerns in location-based services. Current systems, such as GPS or centralized parties, can cheat, leak location information, and be vulnerable to attacks. BIMP aims to generate privacy-preserving location proofs, include an incentive mechanism for witnesses, and detect collusion attacks, making nearby nodes more willing to participate. BIMP implemented functionality using hash-based commitments and ring signatures to generate location proofs (LPs) between a witness and a prover. Blockchain technology addressed scalability, rewards, and synchronization issues. Zero-knowledge proofs, specifically zk-SNARKs, were used by provers to prove ownership without revealing their identity. The traceable-detectable-prefix structure prevents prover-witness collusion attacks by using simple hashes to detect attacks while hiding the identities of the prover and witness.
  The authors conducted a security analysis on BIMP, demonstrating its ability to resist attacks, achieve unforgeability, privacy, proof of ownership, and unlinkability, and its effectiveness in collusion detection. Also included was a comparison with two alternative schemes, STAMP [60] and PROPS [61]. For this comparison, the authors

used a "coefficient of satisfaction (CS)" formula based on five features: "privacy protection", "collusion prevention", "safety employing", "data backup", and "incentive mechanism". The results of this comparison showed that independent of the number of LPs, BIMP reached a higher "CS" than both STAMP and PROPS because of its greater level of privacy and security.
The authors concluded with some benefits of BIMP, namely that it effectively incentivized witnesses to generate LPs and effectively protected user privacy. In the end, the authors suggested an investigation into the storage problem of LPs in the generation phase as a future research direction, however, the authors did not seem to elaborate on this suggestion.

- In [62] the authors proposed pRate, a reputation management scheme that provided strong privacy and security guarantees. Reputation systems in online platforms were an important measure of trustworthiness. However, in traditional reputation schemes, there were no integrity guarantees, and neither guarantee was user privacy. On top of that some users did not want to leave a bad rating in fear of receiving a low rating in retaliation. While previous schemes attempted to solve these problems, none of them also hid the reputation from the reputation manager. To that end, pRate was proposed to solve the problems with previous schemes while also hiding the reputation from the reputation manager. The reputation manager could however still learn the user identities of transacting parties such that users could report misbehaving parties. The pRate scheme utilizes technologies like BBS+ signatures, Chaum-Pedersen-signed ElGamal (CPS-EG) encryption, and zero-knowledge proofs, including Bulletproofs, to create user reputation credentials. These credentials can be used to disclose messages or create zero-knowledge proofs. The scheme also uses Bulletproof zero-knowledge proofs to prove interval-based statements on user reputation. CPS-EG is used to ensure the secrecy of rating tokens and ratings. The research conducted a theoretical performance analysis of a scheme, providing formulas for calculating proof size and computational duration of various protocol operations. The exact values were inferred by comparing the parameters of the formula with those in the system. Additionally, The research conducted a security analysis on pRate, identifying five security theorems, which were proven to be true.
  The main benefit of pRate was that it comprised a reputation system that hid identities from participants in the transaction and rating phases, and additionally did not allow the reputation manager to learn the reputation scores either. While the reputation manager knew the identities of transaction participants, this benefited the scheme because it enabled users to report misbehaving participants. Finally, the authors mentioned that the pRate scheme functioned independently from the actual transactions, and as such pRate could be used with other approaches for anonymous transaction and payment schemes.

- In [63] the authors proposed an attribute-based privacy-preserving identity management system on the blockchain. This identity management system revealed real identities upon consensus of a system policy violation, which solved the need to always disclose identity attributes to central identity providers. Other identity management systems require this identity attribute disclosure for verification and traceability purposes. The proposal used blockchain technology, zk-SNARKs, ElGamal encryption, and hash-based commitments to achieve selective attribute disclosure, anonymity, and unforgeability. The same technologies also prevented collusion attacks, while the system's traceability requirement was instead satisfied using Shamir's secret sharing together with blockchain technology.
  The authors conducted a security analysis, proving unforgeability, anonymity, and traceability. They also conducted performance and cost analyses using an off-chain simulation of their proposed system. The performance analysis assessed the system's time and space complexity, while the cost analysis compared it to Ethereum's basic

transactions, finding that transactions were 1.24 to 189.42 times more expensive in the proposed system. The authors highlight the benefits of anonymity and traceability in their proposed system but also acknowledge its limitations, such as high computational power, potential collusion attacks, and reduced system functionality. They suggest future research on efficiency improvements and malicious off-chain validator detection techniques.

- In [64] the authors propose a blockchain-based federated learning system that prioritizes fair incentives, integrity, and privacy. This system enhances existing federated learning systems by preventing data leakage, adding plausibility checks on contributed models, and preventing data-poisoning and free-riding attacks. The proposal utilized Local Differential Privacy (LDP), zk-SNARKs, and blockchain technologies to create plausible deniability, verify model updates on real private data, and distribute the federated learning system, ensuring neutrality, transaction immutability, and transparency. These technologies prevent leaks of private data through pattern information.
  The performance analysis showed that key generation times, proof generation times, and circuit size scale linearly with the number of constraints, while verification duration, verification key size, and proof size remain constant. Although a security analysis was not included, the authors acknowledged that attacks on integrity could occur if the learning task was known beforehand. The authors analyzed the cost of on-chain operations on the Ethereum blockchain, stating it was prohibitively expensive, and suggested using permissioned blockchains like Quorum for lower costs and higher throughput.
  The main benefits of the proposed solution were its confidentiality, fairness, and tamper-resistance, while the solution was also scalable and decentralized. In the end, the authors mentioned some future research directions including improving the performance and scalability by using zk-STARKs and a recursive verification system, as well as researching alternative incentive mechanisms, and ensuring system applicability in practice.

- In [65] the authors proposed a privacy-preserving biometric authentication scheme for authenticating to a server without a trusted third party. To this end, they proposed and compared three proof of decryption techniques based on HMAC, blinding techniques, and verifiable computing (VC). These techniques were an alternative to the use of trusted execution engines (TEEs) to obtain the required trust for biometric authentication. The proposed scheme used Pinocchio, a practical zk-SNARK, in the verifiable computing technique to verify a secret key without exposing it. A conducted performance analysis compared the proposed VC scheme with the matrix-vector multiplication and determinant-based blinding alternatives. Memory consumption of the VC scheme was shown to be relatively low. On the contrary, execution times were orders of magnitude higher than those of the other two techniques.
  The authors additionally mentioned the security level of the scheme in bits, together with the brute-force success probability. However, no comprehensive security analysis was performed. The elimination of the TEE or trusted third party was the main benefit of the proposed method. Suggested future research directions included the implementation of HMAC-based schemes, as well as testing alternative VC techniques for use in the scheme.

- In [66] the authors proposed the DECO (DECentralized Oracle) system. DECO allowed a user to prove statements, such as that a piece of data came from a particular website, about data accessed from a TLS-protected website, without revealing the data itself. By enabling a user to prove such statements, the user could securely access their data, export it, and then prove the data origin to another service. By doing so DECO removes the need for help from the origin service and solves limitations of existing solutions with similar ideas that require deprecated TLS versions or server-side installation to function. The functionality of DECO was enabled by using zk-SNARKs and a three-party handshake protocol. The zk-SNARKs were used to prove the statements on retrieved data without

disclosing the data to the verifier, while the three-party handshake protocol let the prover and verifier from a joint TLS client. This joint TLS client provided authenticity and prevented the prover from secretly encrypting additional messages using the TLS session keys. Security analysis was provided that included simulation-based proofs of the stated security theorem.
Additionally, a performance analysis was performed using a demo implementation of three different applications. The analysis showed the run duration of the different protocols on LAN and WAN, offline and online, and showed the time and memory costs of generating and verifying the zero-knowledge proof steps. At the end of the performance analysis, the authors compared the end-to-end performance of DECO to Town Crier [67], which was approximately twenty times faster than DECO but required more trust assumptions. The compatibility of the proposed system was mentioned as its main benefit. While DECO showed reduced performance compared to Town Crier, the ever-so-often usage of DECO made the authors mention that this trade-off was acceptable for the security gain. Though the authors did not provide specific future research directions, they did mention that DECO could with some adaptations use Bulletproofs to remove the trusted setup requirement. However, using Bulletproofs would have come at the cost of increased proof creation and verification times.

3.8 | Other

We review different use cases in this section that do not fall under any of the mentioned categories:

- In [68] the authors proposed an efficient, privacy-preserving data-sharing framework for vehicles using multi-sharding blockchain. This solution was proposed to solve performance, security, and privacy concerns in vehicular data sharing schemes that included: a single point of failure, identity disclosure, and requirement for a trusted third party. The main enabling technologies in the proposal were zk-SNARK and blockchain technology. zk-SNARKs were used to enable auditable data sharing without disclosure of vehicle identities. To enable said data sharing when scaling to many vehicles, the proposal used blockchain technology for a multi-sharding blockchain protocol that increased performance and scalability. The included security analysis first described three attack types, and then the authors proved that the proposed system was secure against the described attacks.
  Additionally, the proposal included a performance analysis on theoretical (big-O notation) and practical performance. The practical performance was evaluated for both sharding and multi-sharding proof-of-concept implementations and showed the bandwidth consumption and throughput for different numbers of blockchain nodes in the system. The practical performance analysis also showed run durations of the proposed scheme in comparison to ring and group signature-based schemes. The main benefits of the proposed framework are its security, privacy, and performance aspects. The authors concluded by suggesting research on the block sorting mechanism as a future research direction.

- In [69] the authors proposed a privacy-preserving fair payment (PPFP) protocol for use in vehicle-to-grid (V2G) networks. V2G, where electric vehicles exchange electricity with a smart grid, raises privacy concerns due to the transmission of private information. Existing solutions have limitations like high computational complexity and communication overhead. PPFP, using blockchain technologies and zero-knowledge proofs, aims to address these limitations, providing lower computational complexity and stronger privacy without relying on a trusted third party. PPFP uses nested commitment schemes to hide transaction amounts and participants, unlike Bitcoin-based timed commitments (BBTCs). PPFP prevents identity leaks using zk-SNARKs. The authors found PPFP to satisfy privacy, fair payment, and untraceability properties, describing two theorems on privacy and untraceability

and fairness, which were proven to hold.
The main benefits of PPFP were that it allowed EVs and the smart grid to exchange services and electricity without relying on trusted hardware or a central authority. PPFP also satisfied the three properties of privacy, fairness, and untraceability. In contrast to these benefits was the downside of the time-consuming Bitcoin transactions, however the authors diminished this downside by mentioning that PPFP could use alternative consortium blockchains without the loss of security.

- In [70] the authors proposed Eunomia, a blockchain-based vehicular digital forensics (VDF) scheme that was secure and privacy-preserving. Gathering evidence for VDF was of great importance for investigations into vehicular accidents and crimes. It was therefore a major problem when witnesses withheld evidence for fear of retaliation, data leaks, and data misuse. By setting requirements on privacy (anonymity and unlinkability) and security (confidentiality, authentication, fine-grained access control, accountability, and traceability) for Eunomia, the authors aimed to resolve privacy concerns in witnesses and thereby improve the effectiveness of VDF. The proposal in Eunomia aimed to meet privacy and security requirements using technologies like zero-knowledge proofs, Pedersen commitments, ciphertext-policy attribute-based encryption (CP-ABE), and blockchain technologies. Bulletproof was used for warrant validity, while smart contracts validated these proofs. CP-ABE ensured only encrypted data requests were acknowledged. Pedersen commitments were used in an oblivious transfer protocol to embed the investigator's private key in data, providing traceability and embedding the investigator's private key.
  A security analysis in the research showed that the anonymity, unlinkability, confidentiality, and authentication requirements of the scheme were met. To prove them, the authors described a theorem for each of the requirements and subsequently proved this theorem. For the fine-grained access control, accountability, and traceability requirements the authors instead provided an explanation of how they were achieved. Furthermore, the authors included a comparison of the privacy and security properties of the proposed solution compared to previous works, including DiaLOG [71], DFAV [72], B4F [73], and BB-VDF [74]. Only Eunomia was able to achieve all the compared security and privacy properties in this comparison. The authors conducted a security analysis and performance evaluation of Eunomia, a prototype on a Wi-Fi-based Ethereum test network. They found unfavorable results, possibly due to improved privacy and security. They also included a cost analysis on Ethereum gas costs. To conclude, the authors mentioned that the main benefit of Eunomia was that data providers could participate in VDF without privacy concerns. At the same time investigation tasks were not disclosed, data could not easily be altered, and data leaks could be traced. A downside of Eunomia was that the crowdsourcing of data enabled false information to be uploaded to the system. However, the authors described that the effects of this downside were mitigated because data providers would be asked to testify in court, as would have been the case for witnesses in justice systems throughout the world.

- In [75] the authors proposed ZXAD, an abuse detection system for private Tor exit nodes that did not reveal any information apart from a high traffic volume. The problem with Tor was that while it could be used for legitimate purposes, it was also abused for high-traffic attacks including denial of service (DoS) attacks. This led to services blocking Tor exit node IPs, which in turn hindered the legitimate use of Tor from that exit node. Existing solutions were either challenging to implement for Tor because of its unlinkability trait or posed a privacy risk to Tor users. The proposed solution instead implemented a privacy-preserving connection identification system which allowed the detection of high-volume attacks. The detected attacks could then be blocked, which would mean that services could unblock Tor access for legitimate users without the fear of high-volume attacks from the same origin. Zero-knowledge proofs, specifically zk-SNARKs, were the main enabling technology in ZXAD.

A client used these proofs to prove their unique ID to obtain a long-term key, without revealing the ID itself. The obtained key was then used to generate periodic keys for generating the circuit and stream tokens. Zero-knowledge proofs were then generated on these tokens again to prove that they were well formed. The tokens allowed to rate limit the number of connections in a period while preserving the user privacy. BLS signatures additionally guaranteed the validity of key distribution messages. Furthermore, Shamir's secret sharing was used to extend ZXAD for Tor's t-out-of-n threshold threat model. This threat model guaranteed the security of ZXAD if a majority of the Tor DirAuths were honest.

The research conducted a security analysis to verify the accuracy of zero-knowledge proofs used to verify circuit and stream tokens. It also evaluated the performance of the ZXAD protocol using Kyber and Libsnark libraries, focusing on execution and verification times, blind signature transfer, circuit token generation phases, and load for DirAuths, exits, and clients. The authors identified several limitations in the ZXAD protocol, including the need for appropriate unlinkable connections, stream tokens sent to destination servers, destruction of a common reference string initial secret, and potential DoS attacks by clients. However, the main advantage of ZXAD was its ability to limit high-volume traffic attacks while maintaining strong privacy guarantees.

- In [76] the authors proposed V2GEx, a privacy-preserving fair vehicle-to-grid (V2G) exchange scheme based on blockchain technology. By reducing the privacy-preservation aspect to only one party the authors then also proposed Uni-V2GEx, an alternative scheme that offered better efficiency than regular V2GEx. V2G solutions allow electric vehicles (EVs) to improve grid stability by exchanging electricity and serving as grid regulators. A critical issue for this service however was the required constant monitoring of EVs for service regulation and rewards that led to the identity and location information of EV owners being compromised. The two proposed schemes solved this issue by using blockchain technology combined with zero-knowledge proofs to preserve privacy while achieving fair exchange in V2G. The two proposals utilized blockchain technology, specifically smart contracts, as a distributed broker for micro-payments, replacing third-party intermediaries. Zk-SNARKs were used to verify transaction accuracy and maintain privacy. Uni-V2GEx, unlike V2GEx, only used zk-SNARKs for the EV side, reducing privacy for the smart grid. This improved efficiency by eliminating zk-SNARK proof computations for the smart grid side. The authors provided a formal security proof for V2GE, a privacy analysis that explained how it thwarted traffic analysis, de-anonymization attacks, and attacks on payment, identity, and location privacy. They also implemented a prototype on Ethereum, conducted a performance analysis of zk-SNARKs, micropayments, and transaction processing, and added a cost analysis of the prototype.

  To conclude, the authors mentioned that the main benefit of V2GEx was that it simultaneously provided fairness and bi-directional privacy, while Uni-V2G provided improved efficiency compared to V2GEx for situations where unidirectional privacy was adequate.

- In [77] the authors proposed a hybrid identity authentication scheme for blockchain-based mobile crowd sensing (MCS). By including a hierarchical authentication model to perform computation off-chain and verification on-chain, the proposed solution increased the privacy and efficiency of the system. In contrast, existing blockchain-based systems exposed node identities leading to reduced privacy, or had low verification efficiency and failed to scale with the blockchain. The proposal used zk-SNARKs to perform proof-generating computations for authentications off-chain, which were then verified on-chain in an efficient and privacy-preserving manner. Additionally, blockchain technology was used to decentralize the MCS system while smart contracts on the blockchain authenticated nodes within a cluster. An included security analysis of the proposed system started with a threat model with potential attacks and risks for the system and then described how the system prevented these threats.

Afterward, the security of the proposed solution was favorably compared against other schemes [78] [79] [80] [81].

Additionally, a performance analysis was included, which listed the performance of registration, witness generation, proof generation, and proof verification. The proof verification performance was then favorably compared against that of an electric vehicle verification scheme [79]. Next to the performance analysis, a cost analysis showed the costs of performing the operations for registering nodes on the Ethereum blockchain. The authors remarked on the privacy and security aspects of the system as its main benefits and suggested mechanisms for managing MCS participant reputation and methods for sharing collected data as future research directions.

TABLE 6 Benchmark of the systematic literature review

Ref.	Application	Use case	Protocol	Analyses	Strengths & weaknesses
[15]	Digital currency	Financial	Bulletproofs	S, PC	+ Full implementation included and made publicly available + Quantum resistance briefly mentioned in discussing commitments - Limitations not mentioned - Future research directions not mentioned
[18]	Inter-bank settlements	Financial	zk-SNARK	C	+ Limitations mentioned + Future research directions mentioned - Experimental implementation not included - Quantum resistance not mentioned
[19]	Asset exchange	Financial	zk-SNARK	S, P	+ Test implementation included - Limitations not mentioned - Future research directions not mentioned - Quantum resistance not mentioned
[20]	Transaction processing	Financial	zk-SNARK	P	+ Prototype implementation included + Limitations mentioned + Future research directions mentioned - Quantum resistance not mentioned
[21]	Digital currency	Financial	zk-SNARK	S, P	+ Experimental implementation included - Limitations not mentioned - Future research directions not mentioned - Quantum resistance not mentioned
[22]	Asset exchange	Financial	zk-SNARK	S, P	+ Experimental implementation included - Limitations not mentioned - Future research directions not mentioned - Quantum resistance not mentioned

[23]	Medical record sharing	Medical	zk-SNARK	P	+ Simulated test implementation included + Future research direction mentioned - Limitations not mentioned - Quantum resistance not mentioned
[24]	Medical research data sharing	Medical	zk-SNARK	-	+ Future research direction mentioned - Non-theoretical implementation not included - Limitations not mentioned - Quantum resistance not mentioned
[25]	Medical record sharing	Medical	zk-SNARK	S, PC	+ Test implementation included + Future research direction mentioned - Limitations not mentioned - Quantum resistance not mentioned
[27]	Business transaction tracing	Medical	Bulletproofs	S, P	+ Test implementation included and made publicly available + Limitations mentioned - Future research directions not mentioned - Quantum resistance not mentioned
[28]	Contact tracing	Medical	Bulletproofs	S, P	+ Test implementation included + Limitations mentioned + Future research direction mentioned - Quantum resistance not mentioned
[29]	Health monitoring	Medical	zk-SNARK	S, P, C	+ Test implementation included + Limitations mentioned + Future research directions mentioned - Quantum resistance not mentioned
[31]	Medical insurance claiming	Medical	zk-SNARK	S, PC, C	+ Test implementation included - Limitations not mentioned - Future research directions not mentioned - Quantum resistance not mentioned

[32]	Record keeping & auditing	Business	zk-SNARK	-	- Non-theoretical implementation not included - Limitations not mentioned - Future research directions not mentioned - Quantum resistance not mentioned
[33]	Transaction auditing	Business	Bulletproofs	SC	- Non-theoretical implementation not included - Limitations not mentioned - Future research directions not mentioned - Quantum resistance not mentioned
[36]	Liability auditing	Business	Bulletproofs	S, P	+ Experimental implementation included + Limitations mentioned + Future research direction mentioned + "Post quantum friendliness" very briefly mentioned
[38]	Record keeping & auditing	Business	Bulletproofs	-	+ Future research direction mentioned - Non-theoretical implementation not included - Limitations not mentioned - Quantum resistance not mentioned
[39]	Supply chain tracing	Business	zk-SNARK	S, C	+ Test implementation included + Limitations mentioned + Future research directions mentioned - Quantum resistance not mentioned
[40]	Property sharing contracts	Business	zk-SNARK	S, P	+ Future research directions mentioned - Non-theoretical implementation not included - Limitations not mentioned - Quantum resistance not mentioned
[41]	Data auditing	Business	Bulletproofs	S, P	+ Test implementation included - Limitations not mentioned - Future research directions not mentioned - Quantum resistance not mentioned

[42]	Sealed-bid auctions	Business	Bulletproofs	S, P, C	+ Experimental implementation included - Limitations not mentioned - Future research directions not mentioned - Quantum resistance not mentioned
[44]	Attribute-based access control	General	zk-SNARK	S, P, C	+ Proof of concept implementation included + Future research directions mentioned - Limitations not mentioned - Quantum resistance not mentioned
[45]	Reputation system	General	zk-SNARK	S, P	+ Test implementation included + Future research direction mentioned - Limitations not mentioned - Quantum resistance not mentioned
[46]	Consensus system	General	zk-SNARK	-	- Non-theoretical implementation not included - Limitations not mentioned - Future research directions not mentioned - Quantum resistance not mentioned
[47]	Identity exchange	General	zk-SNARK	S, P	+ Test implementation of main building blocks included + Future research directions mentioned - Limitations not mentioned - Quantum resistance not mentioned
[48]	Biometric authentication	General	zk-SNARK	S, P	+ Experimental implementation included + Limitations mentioned + Future research directions mentioned - Quantum resistance not mentioned
[55]	Voting	General	zk-SNARK	S	- Non-theoretical implementation not included - Limitations not mentioned - Future research directions not mentioned - Quantum resistance not mentioned

[49]	Attribute-based access control	General	zk-SNARK	SC	- Non-theoretical implementation not included - Limitations not mentioned - Future research directions not mentioned - Quantum resistance not mentioned
[56]	Authorization system	General	zk-SNARK	S, CC	+ Test implementation included + Future research directions mentioned - Limitations not mentioned - Quantum resistance not mentioned
[59]	Location-based incentives	General	zk-SNARK	S, PC	+ Implementation simulation included + Future research direction mentioned - Limitations not mentioned - Quantum resistance not mentioned
[62]	Reputation system	General	Bulletproofs	S, P	- Non-theoretical implementation not included - Limitations not mentioned - Future research directions not mentioned - Quantum resistance not mentioned
[63]	Identity management	General	zk-SNARK	S, P, C	+ Implementation simulation included + Limitations mentioned + Future research directions mentioned - Quantum resistance not mentioned
[64]	Federated learning	General	zk-SNARK	P, C	+ Experimental implementation included + Limitations mentioned + Future research directions mentioned - Quantum resistance not mentioned
[65]	Biometric authentication	General	zk-SNARK	PC	+ Experimental implementation included + Future research directions mentioned - Limitations not mentioned - Quantum resistance not mentioned

[66]	Data federation	General	zk-SNARK	S, PC	+ Experimental implementation included - Limitations not mentioned - Future research directions not mentioned - Quantum resistance not mentioned
[68]	Vehicular data sharing	Other	zk-SNARK	S, PC	+ Proof of concept implementation included and made publicly available + Future research directions mentioned - Limitations not mentioned - Quantum resistance not mentioned
[69]	Vehicle-to-grid exchange	Other	zk-SNARK	S	- Non-theoretical implementation not included - Limitations not mentioned - Future research directions not mentioned - Quantum resistance not mentioned
[70]	Vehicular digital forensics	Other	Bulletproofs	SC, PC, C	+ Test implementation included + Limitation mentioned - Future research directions not mentioned - Quantum resistance not mentioned
[75]	Tor abuse detection	Other	zk-SNARK	S, P	+ Test implementation included + Limitations mentioned - Future research directions not mentioned - Quantum resistance not mentioned
[76]	Vehicle-to-grid exchange	Other	zk-SNARK	S, P, C	+ Prototype implementation included - Limitations not mentioned - Future research directions not mentioned - Quantum resistance not mentioned
[77]	Mobile crowd sensing	Other	zk-SNARK	SC, PC, C	+ Experimental implementation included + Future research directions mentioned - Limitations not mentioned - Quantum resistance not mentioned

4 | RESULTS

In this section, we delve into the outcomes of the literature review. The subsection 4.1 discusses the results derived from the evaluation of the research works included, as conducted in section 3.3. Subsequently, we present a performance assessment in section 4.2, and a security evaluation for those that carried out a security analysis in section 4.3, respectively. In the end, we revisit the research questions proposed in section 2.2, incorporating all our findings and providing answers in section 4.4.

4.1 | General Findings

Out of the 41 research papers reviewed, 31 employed zk-SNARKs, and 10 made use of Bulletproofs. Notably, none of the research included in our systematic literature review utilized zk-STARKs. Although we cannot draw overarching conclusions about the comparative usage of zk-STARKs versus zk-SNARKs and Bulletproofs, it is evident that zk-STARKs are not commonly employed in privacy-preserving applications research that adheres to our search and filtering criteria. The Bulletproof protocol's security relies on the discrete logarithm problem, which makes it vulnerable to quantum attacks, as Shor's algorithm [82] has demonstrated the ability to solve discrete logarithm problems efficiently using quantum gates [83]. Similarly, homomorphic public-key cryptography is not quantum-resistant, which means that the zk-SNARK protocol also lacks quantum resistance. In our systematic literature review, all the analyzed works utilize one of these two protocols, leading us to the conclusion that none of these solutions can be considered post-quantum secure without additional protective measures. Surprisingly, with the exception of two research, none of the studies included in our review made any mention of the quantum resistance of their proposed solutions.

Furthermore, these mentions were brief and lacked in-depth exploration. Although a few research papers acknowledged their dependency on the discrete logarithm problem for security in their security analysis, none of the authors related this to quantum resistance. Only research papers [15] and [36] briefly acknowledged and considered the quantum resistance of their proposed solutions, but even these works did not delve into the potential impact on solution security or provide insights into how to approach quantum resistance.

We will continue our findings with a comparison of the real-world performance and security of the proposed solutions.

4.2 | Performance Comparison

In this section, we explore the performance aspects of the NIZKP protocol implementations in the reviewed research papers and conduct a comparative analysis of performance metrics, provided by the authors in their performance assessments. Our goal is to reach conclusions regarding performance disparities among the different protocols. The performance analysis results are listed in Table 8.
The table uses the following abbreviations for column names to make it fit on a single page:

- **Paper** - The literature source in the corresponding use case grouping
  - **Fin.** Financial
  - **Med.** Medical
  - **Bus.** Business
  - **Oth.** Other
  - **Gen.** General

- **Pr.** - Protocol; The protocol used in the research
  - **B** Bulletproof (rows coloured grey)
  - **SN** ZK-SNARK
- **Type** Defines how the performance metrics were obtained. Includes system component, parameter configuration, and test machine specifications
- **ST (ms)** Setup Time; The time required to set up the system in milliseconds
- **KT (ms)** Keygen Time; The time required for generating the keys in milliseconds
- **PKS (B)** Proving Key Size; The storage size of the proving key in bytes
- **VKS (B)** Verification Key Size; The storage size of the verification key in bytes
- **PS (B)** Proof Size; The storage size of the generated proof in bytes
- **TxS (B)** Transaction Size; The size of a generated transaction in bytes
- **PT (ms)** Proof Time; The time required to generate a proof in milliseconds
- **VT (ms)** Verification Time; The time required to verify a proof in milliseconds

To keep this concise, we did not include every performance result from each work. Instead, we selected the most pertinent results, including multiple types when they were substantially different (e.g., different system components). When the work examined a single component with multiple parameters, we chose the parameters with detailed descriptions in the text, or we estimated the results from graphs if necessary. In cases where parameters overlapped among different system components, we incorporated the performance values for both the lowest and highest parameters tested for each component. The research works furthermore conducted performance analyses on differing hardware. In Table 7, we list for each work the specifications of the system the researchers used to conduct the performance analysis as indicated by the authors of the work. One work used two different machines, for each of those machines we defined a type which we also referenced in the type column of Table 5.

Financial use case: Out of the six research works within the financial use case category, five conducted a performance analysis. Among these, four employed the zk-SNARK protocol, while only one utilized Bulletproofs. It's important to note that the performance analysis in reference [20] is excluded from our comparison because it assessed the computational overhead of blockchain versus a traditional database, rather than comparing zero-knowledge proof protocols. Consequently, we had four performance analyses in total for comparison: three based on the zk-SNARK protocol and one using the Bulletproof protocol. As can be seen in Table 8, the proof size of the Bulletproof in [15] is more than twice as large as the proof size in [19]. Similarly, the Bulletproof transaction size is somewhere from slightly larger to more than three times larger than the transaction size generated by the zk-SNARKs in [21]. The proof generation times of the Bulletproof in [15] are anywhere from just under three times as fast compared to the fastest zk-SNARKs results in [21], to over 20000 times as fast compared to the slowest zk-SNARKs results from [22]. The opposite is true for proof verification times, though the differences are much smaller. For this metric, the Bulletproof proof results from [15] were anywhere from slightly slower compared to the zk-SNARK results in [19], to just over 15 times slower compared to the fastest zk-SNARK result in [21]. From this small sample size, we can inconclusively say that Bulletproofs generate larger proof and transaction sizes than zk-SNARKs. The same can be seen for the verification times of Bulletproofs, where Bulletproof proofs are slower to verify than proofs generated using zk-SNARKs. In contrast, Bulletproofs are up to several orders of magnitude faster in generating the proofs than zk-SNARKs.

Medical use case: Of the seven research works included in the medical use case category, six included a performance analysis. Four of these six works used zk-SNARK as the protocol while two used Bulletproofs. However, the performance analysis in [23] is not usable in our comparison since it analyses the performance of deploying smart contracts instead of the zero-knowledge proofs. Similarly, [28] only performed an analysis on the response times of the

TABLE 7 Machine Specification

Paper	Type	System specifications
Financial		
[15]		i7-4870HQ, 16GB RAM
[19]	i7	i7-8750, 12GB RAM
	i5	i5-4200H, 12GB RAM
[21]		i7-7700, 16GB RAM
[22]		AWS t2.large, 8GB RAM
Medical		
[25]		i7-4770M, 8GB RAM
[27]		64x E5-4610 v2, 128GB RAM
[29]		i7-8700k, 32GB RAM
[31]		i5-11400H, 16GB RAM
Business		
[36]		M1, 16GB RAM
[40]		unspecified "common computer"
[41]		Xeon Silver 4210, 16GB RAM
[42]		i7-9750H, 8GB RAM
Other		
[75]		i7-6700k (single thread), ? RAM
[76]		i7-8700, 16GB RAM
[77]		i5-1135G7, 8GB RAM
General		
[44]		i7-8750H, 16GB RAM
[45]		i7-3632QM, 16GB RAM
[47]		i7-4790, 16GB RAM
[48]		unspecified i5, 8GB RAM
[63]		i5-4210M, 4GB RAM
[64]		AWS 16vCPU, 64GB RAM
[66]		AWS c5.2large 8vCPU, 16GB RAM

system and did not provide performance numbers for the zero-knowledge proofs which we could compare here. This means that in total we had four performance analyses to compare, three using the zk-SNARK protocol and one using

the Bulletproof protocol. As listed in Table 8, there were only two aspects on which we can compare the Bulletproof in [27] to the zk-SNARK in the other research works, namely on proof generation time and proof verification time. Both times show that Bulletproofs are somewhere in the middle regarding speed compared to the zk-SNARKs in the other works in the category. The proof generation time of the Bulletproof is more than 18 times slower than the fastest result in [31], but equally more than 198 times slower than the result in [25]. The proof verification times show comparable results, where the Bulletproof is more than 16 times slower and five times faster than the fastest and slowest zk-SNARK results respectively, both from [31]. The results from the small sample size in this category show mixed results, with the Bulletproof protocol being faster than the zk-SNARK protocol for some application types while being slower for others. These results can have many reasons, which we will discuss in section **??**. In short, though, we suspect the difference in protocol application to be the main differing factor.

Business use case: The business use case category included eight research works, of which only four included a performance analysis. Of the four works that did include such performance analysis, one used zk-SNARK as the protocol while three used Bulletproofs instead. From the results in Table 8 we can see that a single research work used zk-SNARKs as opposed to the Bulletproofs used by other works. The proof size generated by Bulletproof in [40] was less than half the size of the smallest zk-SNARK proof in the category. The proof generation time of the zk-SNARK proof however was at least 42 times slower than that of the slowest Bulletproof in [42]. Finally, the proof verification times of the only zk-SNARK in this category were listed as below 10ms, so we cannot compare this value exactly. The value however is comparable to the fastest Bulletproof proof generation time of 2ms from [36], while up to about two orders of magnitude slower than the slowest Bulletproof proofs in [36] and [41].

The results from the small sample size in this category show that the zk-SNARK has a smaller proof size and about equal or lower verification times than the Bulletproofs. The zk-SNARK proof generation time however was much slower than the Bulletproof proof generation times from other works in this category.

General use case (multiple use cases): In the general use case category, there were 14 research works of which 10 included a performance analysis. Of the works that included such performance analysis, nine used zk-SNARK as the NIZKP protocol while only one used Bulletproofs. However, the performance analysis in [59] focuses on the performance of the collision detection, not on the performance of the zero-knowledge proof protocol as we want to compare here. The authors of [62] did not concentrate on the NIZKP protocol's performance either, providing only theoretical performance formulas rather than actual numerical values. As a result, we were unable to compare these two research works' performance analyses. Additionally, we are unable to properly evaluate [65] because it appears to cover more ground than only ZKP performance and primarily concentrates on completely homomorphic encryption in the performance analysis. As such, we were unable to appropriately compare the performance analysis's findings. This indicates that we used the zk-SNARK technique for all seven performance studies that we had to compare. As a result, we are unable to compare the variations among the protocols in this use case group. However, we can use the same approach to examine the differences between works, with wildly differing outcomes. For the key generation time, proof generation times, and verification key size, we see differences of around 40000, 3000, and 30 times between the lowest values from [45] and highest values from [64] respectively. Furthermore, the largest proving key size from [63] is nearly 60000 times larger than the smallest proving key size from [45]. Finally, the longest proof verification time from [64] is about 134 times larger than the shortest time from [48], while the smallest proof size from [47] is about 6 times smaller than the largest proof size from [66]. In short, the verification key sizes, proof sizes, and even the verification times show a reasonable deviation in our opinion, while the other values have a variance that is much higher than we would expect.

Other use case: The six research works in the other use case category included five works with performance analysis. Of the works that included such performance analysis, four used the zk-SNARK NIZKP protocol while only

one used the Bulletproof protocol. However, the performance analysis in [68] focuses mostly on the blockchain. While a running time comparison that showed the running time of various parts of the system was included, these were the numbers for the general scheme and not specifically the zero-knowledge proof protocol. Similarly, [70] included a thorough performance analysis that focused on the computation performance and communication overhead of the entire system, the results of which mostly speak to complete actions in the system which include too much interaction with Ethereum for us to compare the performance. This means that in total we had three performance analyses to compare, all using the zk-SNARK protocol. Therefore, we could not compare the differences between protocols within this use case category. However, we investigated the difference between works using the same protocol, and we compared two criteria, i.e., proof generation and verification times. These numbers show that the proof generation times between [77], [75], and [76] are within the same order of magnitude. The same cannot be said about the proof verification times, where the times from [75] are about three orders of magnitude lower than [76], while the numbers in [76] were already up to five times slower than the proof verification times in [77].

Overview: In our systematic literature review, we examined 41 research works, with 30 of them including a performance analysis. Among these 30 works, 22 utilized the zk-SNARK NIZKP protocol, while the remaining 8 works employed the Bulletproof protocol. We were able to compare the performance of zero-knowledge proof protocols in 22 research works across different use case categories. Out of these, 5 research works analyzed the performance of the Bulletproof protocol, while the other 17 works focused on the zk-SNARK protocol. Based on the available performance analyses, we can compare the proof size, transaction size, proof time, and verification time of the Bulletproof and zk-SNARK protocols. In terms of transaction size, Bulletproof generates larger transactions than zk-SNARKs. The Bulletproof transaction is approximately 17% larger than the largest zk-SNARK transaction and more than three times larger than the smallest zk-SNARK transaction. However, these results are inconclusive due to limited data. Multiple works provide metrics for proof size, proof time, and verification time. The smallest proof size generated by Bulletproof is 622 bytes, while zk-SNARK produces proofs around half this size. Some zk-SNARK works generate larger proofs, but they are still smaller than the largest Bulletproof proof size. One zk-SNARK work stands out as an outlier with a significantly larger proof size. Overall, zk-SNARK tends to generate smaller proofs than Bulletproof. In terms of proof time, Bulletproof generally has shorter proving times, but the results vary significantly. The verification time is even more inconclusive, with both protocols showing varying results. Some zk-SNARK proofs have verification times below 2ms, while others take longer than Bulletproof. Based on the results obtained from our sample, the zk-SNARK and Bulletproof protocols exhibit similar proof verification times. However, it is important to note that the results vary significantly across different studies, making it difficult to draw definitive conclusions.

4.3 | Security Comparison

This section examines security aspects in 41 research works, comparing results to determine differences in protocols. 32 included security analysis, categorized into financial, medical, business, general, and other categories. Works are grouped based on analysis type, with some performing multiple types. The first grouping we define includes works that provided security definitions in theorems or lemmas and then proved these. In this grouping, we define three subgroupings based on the type of the provided proofs. The first subgroup proved the theorems or lemmas by describing a proof in natural language and includes [47] and [62]. The second subgroup proved the theorems or lemmas by (additionally) providing a more mathematical proof. This includes proofs where a mathematical description was an important part of the proof, or where the authors provided a formal mathematical proof. This included [15], [31], [33], [42], [45], [66], [69], [70], and [76]. The final subgroup proved the theorems or lemmas not just through mathematical proofs, but specifically through what are called security games. This group includes [21], [29], and [63].

The second group we designate consists of publications that list certain security specifications or security features of the offered solution, followed by an explanation of how these specifications or system features were satisfied. We may classify the majority of the works in this category into a single subgroup where the descriptions of how the requirements or aspects were satisfied were primarily written in everyday language. [19], [25], [28], [39], [40], [55], [49], [59], [70], and [76] are members of this subgroup. A second grouping used mathematical formulas to explain how the security standards or aspects were partially or completely met. The members of this subgroup are [22], [27], and [42].

A third group we define includes publications that listed a number of attacks on the proposed solution, and subsequently described the security measures in place to prevent these attacks or how these attacks could otherwise be mitigated. We define two subgroups in this group as well. The first provided just general descriptions of the attacks and the security measures using mostly natural language. This includes [19], [40], [44], [68], and [77]. The other subgroup consists of publications that give these descriptions partly or fully in a mathematical way. This subgroup includes [56] and [75].

A fourth group we define includes works that separately defined a threat model in the security analysis of their work. This group includes [33] and [41].

In conclusion, two publications offered a security analysis that other papers did not. A group provided an overview of the system's security. Only the work of Guo et al. [48] is included here, wherein they used mathematics to characterize the soundness and completeness of the zk-SNARK and demonstrate the security of their suggested fix. An additional group computed the likelihood of the suggested solution's security failing. Ji and Chalkias [36] computed the failure probability of their suggested solution by mathematical means in their lone study that is included in this category. Despite the fact that we detailed multiple methods by which the security analyses of the included works were carried out, some works carried out the security analysis in a comparable manner. However, as the security studies were conducted on entire solution systems or significant portions of them, we are unable to accurately evaluate the security even between the works that carried out the security study in an equivalent manner. This indicates that we were unable to compare the security analyses of the included works in a way that would have been beneficial, as we shall address in more detail in section **??**

4.4 | Answering the research questions

Our systematic literature research attempts to address the research issues we outlined in section 2.2. In this section, we restate the questions and provide an answer.

- **What are the existing real-world use case implementations of zk-SNARKs, zk-STARKs, and bulletproofs in privacy-preserving authentication, as documented in the literature? How are these protocols currently being applied in practical scenarios, and what insights can be drawn from these implementations regarding their effectiveness, challenges faced during deployment, and potential improvements for broader adoption?**

In this systematic literature review work, we included 41 research works that implement at least one of the zk-SNARK, zk-STARK, or Bulletproof protocols in a privacy-preserving solution. We found these works using the search query defined in subsection 2.3.1 and narrowed them down to include only those that seek to protect privacy. The search query that needed either "authentication" or "identity," even if our filtering did not contain any filtering rules on the authentication components, ensured that the application was at least connected to authentication. In section 3.3 we analyze each work and provide a use case description. In Table 6 we also provide the column **Application** which is

further summarised in a few words for which the solution using NIZKPs is used.

- **What are the comparative performance and security implications of implementing zk-SNARKs, zk-STARKs, and bulletproofs in privacy-preserving authentication systems? This includes an analysis of authentication speed, computational overhead, and resilience against various types of attacks, as well as potential vulnerabilities.**

The real-world performance of the NIZKP protocol implementations in the included works and suggested solutions were compared in subsection 4.2. Once more, since we were unable to include any works that employed zk-STARKs in our SLR, we are unable to discuss their performance in real life here. As previously mentioned, although there was a considerable to extremely big fluctuation in the outcomes, we discovered that the real-world performance of the Bulletproof protocol and zk-SNARK protocol was comparable. With the exception of one extreme outlier, the most trustworthy finding indicates that proofs produced by the Bulletproof protocol were often larger than those produced by the zk-SNARK protocol. The result is that the Bulletproof protocol generates a proof faster than the zk-SNARK protocol is less trustworthy. works that employed zk-STARKs in our SLR, we are unable to discuss their performance in real life here. As previously mentioned, although there was a considerable to extremely big fluctuation in the outcomes, we discovered that the real-world performance of the Bulletproof protocol and zk-SNARK protocol was comparable. With the exception of one extreme outlier, the most trustworthy finding indicates that proofs produced by the Bulletproof protocol were often larger than those produced by the zk-SNARK protocol. The result is that the Bulletproof protocol generates proof faster than the zk-SNARK protocol is less trustworthy.

Verification time results are the least dependable because they vary the most. Overall, it appears that both protocols require roughly the same amount of time to validate a proof; but, because of their significant differences, different applications may require different times for the two protocols to prove to be faster than the other. To put it briefly, we are unable to come to a definitive conclusion about which protocol performs better in actual situations. In section 5, we go into further detail on the significance of these findings and our next moves. Furthermore, we were unable to offer any real-world results on the implementations' security. The security studies in the included publications vary too much from one another, as described in subsection 4.3, to allow any conclusions about the security differences between the Bulletproof and zk-SNARK protocols to be made. The one security conclusion we could draw—that neither zk-SNARKs nor Bulletproofs are quantum resistant—is covered in further detail in section 5. This implies that if quantum security is a concern, zk-STARKs are still the sole choice available among the three protocols. The choice of zk-SNARK, zk-STARK, or Bulletproof protocol in an application involves two main trade-offs: performance, security, and applicability. The theoretical performance of these protocols is vastly different, but real-world performance does not show clear differences. Security differences are not clear due to mutual differences between security analyses. The zk-SNARK and Bulletproof protocols are not quantum resistant, introducing an implicit vulnerability to quantum computer attacks. They also do not require a trusted setup, which is another security aspect to consider. The applicability trade-off is more important for applications involving value ranges. The Bulletproof protocol is a range protocol, making it more desirable for applications involving value ranges. Other trade-offs include the availability of libraries that implement each NIZKP protocol, but these are not discussed in this work.

5 | DISCUSSION

In this section, we discuss the results of our systematic literature review (SLR). We first, investigate the strengths and limitations of our work in subsection 5.1. We provide an overview of the aspects our SLR did well and where other

researchers could use our work. Then to contrast these strengths we mention some of the limitations that we ran into with our work, where our work is not that useful for researchers, and where other research can expand further on our work. Furthermore, we show that our SLR work provides a novel contribution in subsection 5.2 through a comparison with related SLR works. Finally, subsection 5.3 details some potential future research directions that we either observed from the included works or that we formed ourselves based on the results and conclusions of our work.

5.1 | Strengths and limitations

Our systematic literature review as performed in this work has several strengths and weaknesses. In this section, we list what we conceive to be the main strengths and limitations of our work.

Strengths

- In this work, we provided, through means of a systematic literature review, an elaborate overview of current research into applications that use non-interactive zero-knowledge proof to preserve privacy. We conceive this to be the main strength of our work since it provides a good overview of the different applications of the main NIZKP protocols for privacy-preserving applications. Such an overview is beneficial to see the big picture of the possibilities enabled by NIZKPs.
- More importantly, this work provides an overview of applications such that researchers can see immediately whether a solution to their problem using NIZKPs already exists, which allows these researchers to build upon and improve previous works.
- Our work is also beneficial in case any researchers want to perform research on NIZKPs but do not know where to start. In that case, the overview of the applications using zero-knowledge proofs for their devised solution can give researchers innovative ideas.
- More specifically, the future research directions given by most works allow researchers to immediately find a concrete research topic and goal.
- Our work is furthermore valuable in providing an overall picture of the status of non-interactive zero-knowledge proofs, including how often each of the three included zero-knowledge proof protocols is used and for which general applications. For the same applications, our work also provides the typical performance to expect from the solution using ZKPs if the original research provided these figures.
- Finally, our systematic literature review gives an idea of the status of research on using NIZKPs for privacy-preserving authentication applications. For example, we noted that comparisons between the different applications and NIZKP protocols are difficult because there currently does not seem to be a standardized way to conduct performance analyses. And while for the performance analysis at least the type of the recorded metrics at corresponds, e.g., proving key size, proof generation time, etc., the security analyses do not show such correspondence. The way the authors analyzed the security of the application, and which security aspects they analysed, are vastly different between different research works. This makes it hard for researchers to compare the security of the different research works, even if the applications themselves are comparable.

Limitations Aside from the strengths, our work also has several limitations.

- The main limitation of our work is that the used search query, combined with our filter rules and inclusion criteria did not lead to the inclusion of any works using the zk-STARK protocol. This is arguably a huge downside for

a systematic literature review that aimed to compare three NIZKP protocols since it means that we could not compare 60 or conclude any results on the zk-STARK protocol.

- The study conducted an additional literature search on 10 October 2023, adjusting the search query to exclude zk-SNARK and Bulletproof terms. After filtering and removing duplicates, six new works were found, all published after the initial search. However, none of these works were included in the systematic literature review based on inclusion criteria. The additional search did not lead to the inclusion of any new works using the zk-STARK protocol, making the systematic literature review its biggest limitation. Table 10 in the Appendix 6 details the reasons for not including the six new works.
- While also a strength for giving a global overview, another limitation of our systematic literature review is that the difference in applications makes it harder to compare the use of zero-knowledge proofs in different works. Different applications require different solutions and technical approaches to create these solutions. This means that the way researchers applied the NIZKP protocols is vastly different, and therefore results drawn from the use of ZKPs in these different works may not always be representative of other works, limiting the usefulness of these results.
- Additionally, not all works include a performance or security analysis and those that do perform these analyses in vastly diverse ways. For the performance analyses, this means that there are differences in the types of measured metrics, as well as differences in the parts of the implementation that are measured. Especially which parts of the systems the authors measured they often did not describe in detail, so the performance differences may be caused by differences in what is included in the measurements.
- For the security analyses, the differences in the analyses were mostly diverse ways of assessing the security, as well as which parts of the system were included. For example, some of the works describe the security mostly in the security assumptions that were made, and then the authors proved that these assumptions held. Other works went more into the mathematical details of the implementation and proved that it was computationally infeasible to break the implementation under some computational hardness assumption.
- Even between papers that performed a similar security analysis though, the security analyses were performed on different parts of the system. This was partly caused again by the difference in the applications of the ZKPs, where each solution had differing aspects that were important to perform a security analysis on. This does not mean however that the descriptions of the performed security analyses are redundant in this systematic literature review, as these descriptions give a good overview of diverse ways in which the security analyses were performed in the included works.
- Furthermore, the explanation of the security analyses of individual works as described in section 3.3 can give researchers a quick reference to works that provide a solution similar or related to their proposed solution to which they could compare the security.
- A final limitation in our comparison was that, even when the application was the same or just the zero-knowledge proof was evaluated, the machine on which each work evaluated the performance was different. This means that the results would not be directly comparable because of a difference in the computational speed of the machine skewing the results.

5.2 | Related systematic literature review Research

In this section, we compare our systematic literature review (SLR) with the works of other authors addressing related topics involving various types of reviews. Through this comparison, we discuss the differences in our approach, thereby highlighting the unique contribution of our SLR. To start off we compare our SLR with one of the works re-

jected for inclusion in this work since it did not propose an application that used NIZKPs [84]. This work instead compared the zk-SNARK and zk-STARK protocols including an overview of implementing libraries. The authors then described how zk-SNARKs could be used for identity management on the blockchain, provided examples of an identity attribute compliance use case, and evaluated some performance measurements on the examples. In short, we can conclude that while the work also aimed at the privacy-preserving authentication/identity topic, there are several differences with our SLR. First, this work only compared the zk-SNARK and zk-STARK protocols and did not include the Bulletproof protocol. On top of this, the authors only compared the protocols on the technical aspects and libraries that implement them, not on the performance. Finally, our work includes many different applications in the privacy-preserving authentication/identity space, while this work only includes an individual use case of an identity system on the blockchain. As described, our SLR differentiates itself from this work through the inclusion of three ZKP protocols and comparing these on the performance and security for multiple privacy-preserving authentication/identity use cases. During our research, we only found a single work that performed some kind of systematic literature review of zero-knowledge proofs, we sought and included more similar systematic literature review works using the following two search queries:

("zero-knowledge" AND "literature review")

and

("zero-knowledge" AND "survey")

Subsequently, we examined outcomes from works closely aligned with our work for meaningful comparisons. It's important to highlight that not all results are comparable in this section; rather, we selectively incorporated the most pertinent findings. To the best of our knowledge, the systematic literature reviews presented in this section are the most akin to our work in terms of comparability. Numerous located works, such as [85] and one by Li et al. [86], delved into zero-knowledge proofs comprehensively, providing historical context and detailed mathematical insights. These works proceeded to examine potential applications of zero-knowledge proofs. Chen et al.'s [87] work centered on IoT applications, while Gowravaram's [88] focused on ZKP applications in financial regulation. The key distinction between these works and ours lies in our specific focus on three Non-Interactive Zero-Knowledge Proof (NIZKP) protocols: zk-SNARKs, zk-STARKs, and Bulletproofs. Our emphasis then shifted to comparing the real-world performance disparities of these protocols in applications with a privacy-preserving authentication use case. Although works like Kurmi et al.'s [89] and a work by Pathak et al. [90] shared a similar setup by focusing on authentication use cases, they diverged from our approach by not comparing the three specific protocols and their respective performance metrics.

Within Cerulli's work [91], a literature review explored the mechanics of zero-knowledge proofs and group signatures. Subsequently, the study proceeded to formulate zero-knowledge proofs tailored for various applications. In contrast, our systematic literature review (SLR) distinguished itself by evaluating three specific zero-knowledge proof protocols, analyzing their real-world application scenarios, and assessing their implementation performance based on insights derived from other works. Subsequently, two research works diverged from zero-knowledge proof reviews: Herbowo's [92], which delved into self-sovereign identity systems, and Herskind et al.'s [93], which explored privacy-preserving approaches for electronic cryptocurrencies. While these works incorporated zero-knowledge proofs, unlike our systematic literature review (SLR), these proofs were not the primary focus. Consequently, the authors did not engage in a comparative analysis of the three specific Non-Interactive Zero-Knowledge Proof (NIZKP) protocols concerning real-world performance.

Two of the reviewed works we encountered focused on a singular Non-Interactive Zero-Knowledge Proof (NIZKP) protocol. Specifically, Chen et al.'s [94] work centered on zk-SNARK, while Morais et al.'s [95] delved into Bulletproofs. These reviews delved more extensively into the intricacies of their respective protocols compared to our work, providing insights into potential applications. However, in contrast to our approach, these works did not undertake a

comparative analysis of multiple protocols regarding their real-world performance in applications. Additionally, the applications discussed in both works diverged from our emphasis on privacy-preserving authentication. There were also studies that, like our systematic literature review (SLR), compared multiple Non-Interactive Zero-Knowledge Proof (NIZKP) protocols. For instance, Sun et al.'s [96] work delved into both the zk-SNARK and Bulletproof protocols, providing insights into their theoretical performance using big-O notation. However, unlike our work, they did not delve into real-world performance. The applications discussed in their study were exclusively related to blockchain use, whereas our focus on privacy-preserving authentication extended beyond the blockchain. Similarly, Partala et al. [97] conducted a comparison of various Zero-Knowledge Proof (ZKP) protocols, including zk-STARKs and Bulletproofs, assessing both theoretical and practical performance. However, their performance comparison focused directly on the protocols rather than evaluating the real-world performance of solutions, as our SLR does. Additionally, their emphasis was on applications in blockchain, in contrast to our broader scope.

In another study, Panait et al. [84] compared zk-SNARK and zk-STARK protocols but omitted the comparison of the Bulletproof protocol, which is a distinctive feature of our work. Their investigation centered on libraries implementing these Zero-Knowledge Proof (ZKP) protocols, a facet not covered in our study. Conversely, our work extensively compares the application use cases for ZKP protocols and evaluates the real-world performance of these solutions, aspects not explored in their work.

Finally, two studies closely aligned with ours were an analysis by Gong et al. [98] and an investigation incorporated in a work by Sanchez Ortiz [99]. Gong et al.'s analysis meticulously examined the zk-SNARK, zk-STARK, and Bulletproof protocols, providing an in-depth exploration of their mathematical underpinnings and big-O performance. Furthermore, the analysis delved into the quantum resistance of the protocols. Nonetheless, it did not compile or contrast applications for these Non-Interactive Zero-Knowledge Proof (NIZKP) protocols. Additionally, their study omitted a comparison of real-world performance—a key objective of our systematic literature review (SLR). In the literature review within Sanchez Ortiz's work, there was an exploration of the general workings and cryptographic fundamentals of Zero-Knowledge Proofs (ZKPs). It also drew comparisons between the zk-SNARK and Bulletproof protocols, particularly in finance use cases, with a discussion on the zk-STARKs protocol as well. The primary distinction from our study is that our focus is on privacy-preserving authentication, whereas their emphasis is on financial applications. Moreover, our research goes a step further by comparing solutions utilizing Non-Interactive Zero-Knowledge Proofs (NIZKPs) in other works based on real-world performance. In contrast, their approach involves using existing literature to explore the application of Zero-Knowledge Proofs (ZKPs) for guidance in developing their own use case implementations. We intended to incorporate a comparison with Khandekar's work [100]; however, due to the unavailability of the full text, we were unable to access it and, consequently, could not include their work in this comparison.

Based on the aforementioned comparison with other works, we infer that our systematic literature review stands out as distinct from previous studies, to the best of our knowledge. Consequently, we assert that our work represents a novel contribution to the research on the application of non-interactive zero-knowledge proofs, particularly within the domain of privacy-preserving authentication.

5.3 | Future research directions

While not all the works included in our analysis offered insights into future research directions, among those that did, one of the most frequently mentioned focuses was the optimization of proposed solutions for enhanced efficiency and speed. Notably, a common aspect identified as a source of slow performance was zero-knowledge proofs, particularly in scenarios where faster alternatives using traditional cryptographic methods could achieve similar functionality. Some works that were excluded during the systematic literature review filtering process did not leverage

zero-knowledge proofs (ZKPs) and instead opted for more conventional cryptographic methods for performance reasons. The authors of works choosing ZKPs defended this decision by highlighting the additional privacy-preserving aspects that zero-knowledge proofs bring to their proposed solutions. The observed lower performance and efficiency of zero-knowledge proofs (ZKPs) emerge as a deliberate trade-off for the enhanced privacy-preserving aspects they offer in a solution. Consequently, delving into ways to enhance the performance and efficiency of non-interactive zero-knowledge proofs (NIZKPs) emerges as a promising avenue for future research. This exploration has the potential to ameliorate the performance of NIZKPs, rendering the trade-off more acceptable and thereby increasing the attractiveness of choosing NIZKPs for the enhanced privacy they provide. Noteworthy works advocating for this future research direction include [18], [25], [29], [44], [48], [63], and [64].

Another avenue for future research, as proposed by [23], [36], and [47], involves exploring the applicability of the proposed solution in different domains or for alternative applications. These authors advocated for such investigations, believing that a solution employing zero-knowledge proofs could offer significant privacy benefits, potentially extending its usefulness beyond the specific subject explored in their respective works. Moreover, nearly all the reviewed works suggested, or at least implied, that subsequent research on their solutions would be beneficial, especially if limitations were identified. This may include implementing alternative options for specific components of the system or modifying the solution to mitigate potential attacks that were discovered.

In addition to the future research directions outlined in the reviewed works, our systematic literature review led us to identify another potential avenue. In the realm of quantum-resistant cryptography, also known as post-quantum cryptography [101], significant developments have occurred. The American National Institute of Standards and Technology (NIST) initiated a call for proposals in 2016 to standardize post-quantum cryptographic algorithms, ultimately revealing four quantum-resistant cryptographic algorithms in 2022 for general encryption or digital signature applications [102].

Considering these advancements, we propose that researching the quantum resistance of Non-Interactive Zero-Knowledge Proof (NIZKP) protocols is a prudent undertaking. This entails understanding how quantum resistance alters the dynamics of NIZKPs and its implications for applications, as described in the works included in our systematic literature review. One such example of a quantum-resistant NIZKP protocol is the zk-STARK protocol [103]. However, it is noteworthy that despite its quantum resistance, the zk-STARK protocol is not widely utilized, as none of the works in our review incorporated it into their solutions.

Given this observation, we posit that exploring the integration of quantum-resistant NIZKP protocols as a replacement for non-quantum-resistant protocols, aimed at achieving post-quantum security, represents a valuable future research direction.

5.4 | Conclusion

In this work, we looked at the use of the zk-SNARK, zk-STARK, and Bulletproof non-interactive zero-knowledge proof protocols for preserving privacy authentication use cases in several applications. To do so, we performed a systematic literature review and ended up including and analysing 41 different research works that applied at least one of the three NIZKP protocols to a privacy-preserving application. We established and described our findings from the analyses of these works and additionally performed a comparison of the real-world performance and security of the implementations on the works that included performance or security analyses, respectively. Our results showed that the real-world performance of implementations using the NIZKP protocols varies widely. For the comparison of the security analyses, we were unable to come to a conclusion because of the vast differences in how the security analyses were performed. To conclude our research, we discussed our work. First, we included a discussion on the

strengths and limitations of our work. Then we included a comparison to other literature reviews on zero-knowledge proofs, which showed our contribution by showing that our work is significantly different from other works. Finally, we discussed some future research directions proposed in the included works, and additionally, we proposed some future research directions that we found important. In the upcoming research, we aim to fill a research gap by implementing a real-world benchmark for the three NIZKP protocols and provide answers to questions that we could not answer with the results from this systematic literature review.

TABLE 8 Performance analysis results

Paper	Pr.	Type	ST (ms)	KT (ms)	PKS (B)	VKS (B)	PS (B)	TxS (B)	PT (ms)	VT (ms)
Fin.										
[15]	B	Confidential transaction						1310,00	40,00	14,00
	B	Auditing policies Limit policy					622,00		21,50	7,50
[19]	SN	zkChain, i7		5931,78	12193219,20	573,25	286,75		1789,68	5,21
	SN	zkChain, i5		8966,48	12193219,20	573,25	286,75		2788,52	6,77
[21]	SN	BN256, Base Tx	730,00					418,00	110,00	0,89
	SN	BN256, Tx both limits	3400,00					802,00	430,00	0,92
	SN	BLS12-381, Base Tx	1300,00					546,00	180,00	1,50
	SN	BLS12-381, Tx both limits	6200,00					1122,00	730,00	1,60
[22]	SN	Commitment			6140000,00	511,80			10000,00	
	SN	First claim, MerkleTreeDepth=16			103660000,00	511,80			131000,00	
	SN	First claim, MerkleTreeDepth=64			447480000,00	511,80			466000,00	
Med.										
[25]	SN	1000 circuit inputs		16300,00	15300000,00	31500,00	125400,00		52000,00	614,00
[27]	B	FES-SPH-PSM Bulletproofs							262,20	168,00
[29]	SN	1000 users		3148,00					2018,00	219,00
	SN	20000 users		99026,00					18257,00	181,00
[31]	SN	FAD phase 10 inputs							1757,00	133,10
	SN	FAD phase 60 inputs							4920,00	988,10
	SN	PPT phase, 2^{10} message space							41,10	22,20
	SN	PPT phase, 2^{60} message space							83,20	40,50
	SN	IPP phase 16-bit ID							14,00	10,00

Table 8 continued from previous page

	SN	IPP phase 512-bit ID							810,00	611,00
Bus.										
[36]	B	Inclusion proofs, 1 aggregated range					672,00		8,00	2,00
	B	Inclusion proofs, 256 aggregated ranges					1184,00		2005,00	381,00
[40]	SN	128-bit security, 1M-gate-circuit, 1000-bit input		117000 to 123000			288,00		147000 to 784000	< 10
[41]	B	Standard range 1-p-1-v mode, 8-bit data size					1088,00		28,00	14,00
	B	Standard range 1-p-1-v mode, 64-bit data size					1568,00		197,00	91,00
	B	Arbitrary range 1-p-1-v mode, 8-bit data size					1312,00		52,00	25,00
	B	Arbitrary range 1-p-1-v mode, 64-bit data size					1792,00		388,00	175,00
[42]	B	Bidding, 128-bit bidlength							642,11	4,74
	B	Aggregation and winner verification, 512 bidders							3480,00	11,18
Oth.										
[75]	SN	Libsnark implementation zk-SNARK proof					169,00		3270 ± 20	8,4 ± 0,1
[76]	SN	Convert	18000		63000000,00	633,00			6000	30000
	SN	Commit	23000		85000000,00	596,00			7000	24000

Table 8 continued from previous page

	SN	Claim/Refund	11000		32000000,00	559,00			3000	31000
	SN	Deposit	11000		115000000,00	670,00			3000	31000
	SN	Pour(Zerocash)	31000		898000000,00	749,00			8000	22000
[77]	SN	100 circuit inputs							5000	10840,00
	SN	600 circuit inputs							9000	10840,00
Gen.										
[44]	SN	Modular approach			11000000		700		3000	
[45]	SN	Mint statement		34,40	3230,00	820,00	287,00		25,20	22,40
	SN	Update statement		42600,00	49240000,00	1849,00	287,00		22100,00	21,00
[47]	SN	Circuit 2, 64-bit nonce		12865,90	32903000,00	3285,60	280,00		3380,00	4,50
	SN	Circuit 2, 128-bit nonce		12872,90	32938000,00	3597,00	280,00		3382,70	4,50
[48]	SN	9 fingerprints	26,79						46,92	1,82
	SN	54 fingerprints	186,95						318,77	23,78
[63]	SN	Generate PKc, VKc		106240,00	192005879,00	6497,00				
	SN	Generate PKd, VKd		2830,00	3896140,00	3381,00				
	SN	Generate π_C					566,00		36620,00	
	SN	Generate π_D					566,00		1580,00	
[64]	SN	π_W, k=4, n=100		177000,00		25000,00	708,00		8641,00	236,00
	SN	π_W, k=4, n=1000		1360000,00		25000,00	705,00		74945,00	232,00
	SN	π_K, k=4, n=100		174000,00		4200,00	705,00		8152,00	244,00
	SN	π_K, k=4, n=1000		1380000,00		4200,00	705,00		73696,00	243,00
[66]	SN	Binary option phase					861,00		12970 ± 40	10,00
	SN	Age proof phase					574,00		3670 ± 20	10,00
	SN	Price discrimination phase					1722,00		12680 ± 20	50,00

references

[1] Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof systems;18(1):186–208. http://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Proof%20Systems/The_Knowledge_Complexity_Of_Interactive_Proof_Systems.pdf.

[2] Blum M, Feldman P, Micali S. Non-interactive zero-knowledge and its applications. In: Proceedings of the twentieth annual ACM symposium on Theory of computing STOC '88, Association for Computing Machinery;. p. 103–112. https://dl.acm.org/doi/10.1145/62212.62222.

[3] Akcora CG, Gel YR, Kantarcioglu M. Blockchain networks: Data structures of bitcoin, monero, zcash, ethereum, ripple, and iota. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery 2022;12(1):e1436.

[4] Conklin A, Dietrich G, Walz D. Password-based authentication: a system perspective. In: 37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the IEEE; 2004. p. 10–pp.

[5] Dammak M, Boudia ORM, Messous MA, Senouci SM, Gransart C. Token-based lightweight authentication to secure IoT networks. In: 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC) IEEE; 2019. p. 1–4.

[6] Zhong Y, Hovanes J, Guin U. On-Demand Device Authentication Using Zero-Knowledge Proofs for Smart Systems. In: Proceedings of the Great Lakes Symposium on VLSI 2023 GLSVLSI '23, New York, NY, USA: Association for Computing Machinery; 2023. p. 569–574. https://doi.org/10.1145/3583781.3590275.

[7] Rajamanickam R, Chaturvedi S. Strengthening the Privacy of Blockchain with Zero Knowledge Proof Case Study: Online Exam Student Verification. In: International Conference on ICT for Sustainable Development Springer; 2023. p. 159–168.

[8] Lu Z, Wang Q, Qu G, Zhang H, Liu Z. A blockchain-based privacy-preserving authentication scheme for VANETs. IEEE Transactions on Very Large Scale Integration (VLSI) Systems 2019;27(12):2792–2801.

[9] Chen T, Lu H, Kunpittaya T, Luo A. A review of zk-snarks. arXiv preprint arXiv:220206877 2022;.

[10] Panait AE, Olimid RF. On using zk-SNARKs and zk-STARKs in blockchain-based identity management. In: Innovative Security Solutions for Information Technology and Communications: 13th International Conference, SecITC 2020, Bucharest, Romania, November 19–20, 2020, Revised Selected Papers 13 Springer; 2021. p. 130–145.

[11] Bünz B, Bootle J, Boneh D, Poelstra A, Wuille P, Maxwell G. Bulletproofs: Short proofs for confidential transactions and more. In: 2018 IEEE symposium on security and privacy (SP) IEEE; 2018. p. 315–334.

[12] Paul J, Lim WM, O'Cass A, Hao AW, Bresciani S. Scientific procedures and rationales for systematic literature reviews (SPAR-4-SLR). International Journal of Consumer Studies 2021;45(4):O1–O16.

[13] Adams CJ, Khan HTA, Raeside R, White DI. Research methods for graduate business and social science students. Thousand Oaks, CA: SAGE Publications; 2007.

[14] Moher D, Shamseer L, Clarke M, Ghersi D, Liberati A, Petticrew M, et al. Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement. Systematic reviews 2015;4:1–9.

[15] Chen Y, Ma X, Tang C, Au MH. PGC: Decentralized Confidential Payment System with Auditability. In: Chen L, Li N, Liang K, Schneider S, editors. Computer Security – ESORICS 2020 Lecture Notes in Computer Science, Springer International Publishing;. p. 591–610.

[16] Narula N, Vasquez W, Virza M. zkLedger: Privacy-Preserving Auditing for Distributed Ledgers;. p. 65–80. https://www.usenix.org/conference/nsdi18/presentation/narula.

[17] Bünz B, Agrawal S, Zamani M, Boneh D. Zether: Towards Privacy in a Smart Contract World. In: Bonneau J, Heninger N, editors. Financial Cryptography and Data Security Lecture Notes in Computer Science, Springer International Publishing;. p. 423–443.

[18] Galal HS, Youssef AM. Privacy Preserving Netting Protocol for Inter-bank Payments. In: Garcia-Alfaro J, Navarro-Arribas G, Herrera-Joancomarti J, editors. Data Privacy Management, Cryptocurrencies and Blockchain Technology Lecture Notes in Computer Science, Springer International Publishing;. p. 319–334.

[19] Huang J, Huang T, Wei H, Zhang J, Yan H, Wong DS, et al. zkChain: A privacy-preserving model based on zk-SNARKs and hash chain for efficient transfer of assets;https://www.webofscience.com/wos/woscc/summary/052c1a81-5308-4536-ae9a-494037700028-7e0eaa1c/relevance/1, place: Hoboken Publisher: Wiley WOS:000898714700001.

[20] Wang Y, Kogan A. Designing confidentiality-preserving Blockchain-based transaction processing systems;30:1–18. https://www.sciencedirect.com/science/article/pii/S1467089518300794.

[21] Wüst K, Kostiainen K, Delius N, Capkun S. Platypus: A Central Bank Digital Currency with Unlinkable Transactions and Privacy-Preserving Regulation. In: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security CCS '22, Association for Computing Machinery;. p. 2947–2960. https://dl.acm.org/doi/10.1145/3548606.3560617.

[22] Xu L, Chen L, Gao Z, Kasichainula K, Fernandez M, Carbunar B, et al. PrivateEx: privacy preserving exchange of crypto-assets on blockchain. In: Proceedings of the 35th Annual ACM Symposium on Applied Computing SAC '20, Association for Computing Machinery;. p. 316–323. https://dl.acm.org/doi/10.1145/3341105.3373901.

[23] Anusuya R, Karthika Renuka D, Ghanasiyaa S, Harshini K, Mounika K, Naveena KS. Privacy-Preserving Blockchain-Based EHR Using ZK-Snarks. In: Raman I, Ganesan P, Sureshkumar V, Ranganathan L, editors. Computational Intelligence, Cyber Security and Computational Models. Recent Trends in Computational Models, Intelligent and Secure Systems Communications in Computer and Information Science, Springer International Publishing;. p. 109–123.

[24] Ghaffaripour S, Miri A. Enabling Medical Research Through Privacy-Preserving Data Markets. In: Moallem A, editor. HCI for Cybersecurity, Privacy and Trust Lecture Notes in Computer Science, Springer International Publishing;. p. 367–380.

[25] Huang H, Zhu P, Xiao F, Sun X, Huang Q. A blockchain-based scheme for privacy-preserving and secure sharing of medical data;99:102010. https://www.sciencedirect.com/science/article/pii/S0167404820302832.

[26] Backes M, Barbosa M, Fiore D, Reischuk RM. ADSNARK: Nearly Practical and Privacy-Preserving Proofs on Authenticated Data. In: 2015 IEEE Symposium on Security and Privacy;. p. 271–286. ISSN: 2375-1207.

[27] Hwang S, Ozturk E, Tsudik G. Balancing Security and Privacy in Genomic Range Queries;26(3):23:1–23:28. https://dl.acm.org/doi/10.1145/3575796.

[28] Jo U, Oktian YE, Kim D, Oh S, Lee H, Kim H. A Zero-Knowledge-Range-Proof-based Privacy-Preserving Blockchain Platform for COVID-19 Contact Tracing. In: 2022 International Conference on Platform Technology and Service (PlatCon);. p. 53–58. https://www.webofscience.com/wos/woscc/summary/052c1a81-5308-4536-ae9a-494037700028-7e0eaa1c/relevance/1.

[29] Luong DA, Park JH. Privacy-Preserving Blockchain-Based Healthcare System for IoT Devices Using zk-SNARK;10:55739–55752. Conference Name: IEEE Access.

[30] Mohanty D, Mohanty D. Deploying smart contracts. Ethereum for Architects and Developers: With Case Studies and Code Samples in Solidity 2018;p. 105–138.

[31] Zheng H, You L, Hu G. A novel insurance claim blockchain scheme based on zero-knowledge proof technology;195:207–216. https://www.sciencedirect.com/science/article/pii/S0140366422003152.

[32] Goldwasser S, Park S. Public Accountability vs. Secret Laws: Can They Coexist? A Cryptographic Proposal. In: Proceedings of the 2017 on Workshop on Privacy in the Electronic Society WPES '17, Association for Computing Machinery;. p. 99–110. https://dl.acm.org/doi/10.1145/3139550.3139565.

[33] He Y, Chen J. AMLChain: Supporting Anti-money Laundering, Privacy-Preserving, Auditable Distributed Ledger. In: Meng W, Katsikas SK, editors. Emerging Information Security and Applications Communications in Computer and Information Science, Springer International Publishing;. p. 50–67.

[34] Gennaro R, Minelli M, Nitulescu A, Orrù M. Lattice-based zk-SNARKs from square span programs. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security; 2018. p. 556–573.

[35] Kang H, Dai T, Jean-Louis N, Tao S, Gu X. FabZK: Supporting Privacy-Preserving, Auditable Smart Contracts in Hyperledger Fabric. In: 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN);. p. 543–555. ISSN: 1530-0889.

[36] Ji Y, Chalkias K. Generalized Proof of Liabilities. In: Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security CCS '21, Association for Computing Machinery;. p. 3465–3486. https://dl.acm.org/doi/10.1145/3460120.3484802.

[37] Konkin A, Zapechnikov S. Privacy methods and zero-knowledge poof for corporate blockchain;190:471–478. https://www.sciencedirect.com/science/article/pii/S1877050921013004.

[38] Singh R, Dwivedi AD, Mukkamala RR, Alnumay WS. Privacy-preserving ledger for blockchain and Internet of Things-enabled cyber-physical systems;103:108290. https://www.sciencedirect.com/science/article/pii/S0045790622005183.

[39] Uesugi T, Shijo Y, Murata M. Design and Evaluation of a Privacy-preserving Supply Chain System Based on Public Permissionless Blockchain. In: 2021 International Symposium on Electrical, Electronics and Information Engineering ISEEIE 2021, Association for Computing Machinery;. p. 312–321. https://dl.acm.org/doi/10.1145/3459104.3459155.

[40] Xu L, Shah N, Chen L, Diallo N, Gao Z, Lu Y, et al. Enabling the Sharing Economy: Privacy Respecting Contract based on Public Blockchain. In: Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts BCC '17, Association for Computing Machinery;. p. 15–21. https://dl.acm.org/doi/10.1145/3055518.3055527.

[41] Xu S, Cai X, Zhao Y, Ren Z, Du L, Wang Q, et al. zkrpChain: Towards multi-party privacy-preserving data auditing for consortium blockchains based on zero-knowledge range proofs;128:490–504. https://www.sciencedirect.com/science/article/pii/S0167739X21003800.

[42] Zhang Q, Yu Y, Li H, Yu J, Wang L. Trustworthy sealed-bid auction with low communication cost atop blockchain;631:202–217. https://www.sciencedirect.com/science/article/pii/S0020025523002633.

[43] Chiesa A, Tromer E, Virza M. Cluster Computing in Zero Knowledge. In: Oswald E, Fischlin M, editors. Advances in Cryptology - EUROCRYPT 2015 Lecture Notes in Computer Science, Springer;. p. 371–403.

[44] Di Francesco Maesa D, Lisi A, Mori P, Ricci L, Boschi G. Self sovereign and blockchain based access control: Supporting attributes privacy with zero knowledge;212:103577. https://www.sciencedirect.com/science/article/pii/S1084804522002181.

[45] Dimitriou T. Decentralized Reputation. In: Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy CODASPY '21, Association for Computing Machinery;. p. 119–130. https://dl.acm.org/doi/10.1145/3422337.3447839.

[46] Ganesh C, Orlandi C, Tschudi D. Proof-of-Stake Protocols for Privacy-Aware Blockchains. In: Ishai Y, Rijmen V, editors. Advances in Cryptology – EUROCRYPT 2019 Lecture Notes in Computer Science, Springer International Publishing;. p. 690–719.

[47] Gunasinghe H, Kundu A, Bertino E, Krawczyk H, Chari S, Singh K, et al. PrivIdEx: Privacy Preserving and Secure Exchange of Digital Identity Assets. In: The World Wide Web Conference WWW '19, Association for Computing Machinery;. p. 594–604. https://dl.acm.org/doi/10.1145/3308558.3313574.

[48] Guo C, You L, Hu G. A Novel Biometric Identification Scheme Based on Zero-Knowledge Succinct Noninteractive Argument of Knowledge;2022:2791058. https://www.webofscience.com/wos/woscc/summary/052c1a81-5308-4536-ae9a-494037700028-7e0eaa1c/relevance/1, place: London Publisher: Wiley-Hindawi WOS:000864451000002.

[49] Li P, Lai J, Wu Y. Accountable attribute-based authentication with fine-grained access control and its application to crowdsourcing;17(1):171802. https://doi.org/10.1007/s11704-021-0593-4.

[50] Li M, Weng J, Yang A, Lu W, Zhang Y, Hou L, et al. CrowdBC: A Blockchain-Based Decentralized Framework for Crowdsourcing;30(6):1251–1266. Conference Name: IEEE Transactions on Parallel and Distributed Systems.

[51] Lu Y, Tang Q, Wang G. ZebraLancer: Private and Anonymous Crowdsourcing System atop Open Blockchain. In: 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS);. p. 853–865. ISSN: 2575-8411.

[52] Chen J, Chen J, He K, Du R. SeCrowd: Efficient secure interactive crowdsourcing via permission-based signatures;115:448–458. https://www.sciencedirect.com/science/article/pii/S0167739X20305264.

[53] Shu J, Liu X, Jia X, Yang K, Deng RH. Anonymous Privacy-Preserving Task Matching in Crowdsourcing;5(4):3068–3078. Conference Name: IEEE Internet of Things Journal.

[54] Yang M, Zhu T, Liang K, Zhou W, Deng RH. A blockchain-based location privacy-preserving crowdsensing system;94:408–418. https://www.sciencedirect.com/science/article/pii/S0167739X18320909.

[55] Li P, Lai J. LaT-Voting: Traceable Anonymous E-Voting on Blockchain. In: Liu JK, Huang X, editors. Network and System Security Lecture Notes in Computer Science, Springer International Publishing;. p. 234–254.

[56] Li Q, Xue Z. A Privacy-Protecting Authorization System Based on Blockchain and zk-SNARK. In: Proceedings of the 2020 International Conference on Cyberspace Innovation of Advanced Technologies CIAT 2020, Association for Computing Machinery;. p. 439–444. https://dl.acm.org/doi/10.1145/3444370.3444610.

[57] Lundkvist DC, Heck R, Torstensson J, Mitton Z, Sena M. UPORT: A PLATFORM FOR SELF-SOVEREIGN IDENTITY;.

[58] Zhou T, Li X, Zhao H. EverSSDI: blockchain-based framework for verification, authorisation and recovery of self-sovereign identity using smart contracts;60(3):281–295. https://www.inderscienceonline.com/doi/abs/10.1504/IJCAT.2019.100300, publisher: Inderscience Publishers.

[59] Lin Z, Luo Y, Fu S, Xie T. BIMP: Blockchain-Based Incentive Mechanism with Privacy Preserving in Location Proof. In: Qiu M, editor. Algorithms and Architectures for Parallel Processing Lecture Notes in Computer Science, Springer International Publishing;. p. 520–536.

[60] Wang X, Pande A, Zhu J, Mohapatra P. STAMP: Enabling Privacy-Preserving Location Proofs for Mobile Users;24(6):3276–3289. https://dl.acm.org/doi/10.1109/TNET.2016.2515119.

[61] Gambs S, Killijian MO, Roy M, Traoré M. PROPS: A PRivacy-Preserving Location Proof System. In: 2014 IEEE 33rd International Symposium on Reliable Distributed Systems;. p. 1–10. ISSN: 1060-9857.

[62] Liu J, Manulis M. pRate: Anonymous Star Rating with Rating Secrecy. In: Deng RH, Gauthier-Umaña V, Ochoa M, Yung M, editors. Applied Cryptography and Network Security Lecture Notes in Computer Science, Springer International Publishing;. p. 550–570.

[63] Luong DA, Park JH. Privacy-Preserving Identity Management System on Blockchain Using Zk-SNARK;11:1840–1853. Conference Name: IEEE Access.

[64] Rückel T, Sedlmeir J, Hofmann P. Fairness, integrity, and privacy in a scalable blockchain-based federated learning system;202:108621. https://www.sciencedirect.com/science/article/pii/S1389128621005132.

[65] Syed H, Shaik I, Emmadi N, Narumanchi H, Thakur MSD, Bhattachar RMA. WiP: Privacy Enabled Biometric Authentication Based on Proof of Decryption Techniques. In: Tripathy S, Shyamasundar RK, Ranjan R, editors. Information Systems Security Lecture Notes in Computer Science, Springer International Publishing;. p. 185–197.

[66] Zhang F, Maram D, Malvai H, Goldfeder S, Juels A. DECO: Liberating Web Data Using Decentralized Oracles for TLS. In: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security CCS '20, Association for Computing Machinery;. p. 1919–1938. https://dl.acm.org/doi/10.1145/3372297.3417239.

[67] Zhang F, Cecchetti E, Croman K, Juels A, Shi E. Town Crier: An Authenticated Data Feed for Smart Contracts. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security CCS '16, Association for Computing Machinery;. p. 270–282. https://dl.acm.org/doi/10.1145/2976749.2978326.

[68] Huang J, Kong L, Wang J, Chen G, Gao J, Huang G, et al. Secure Data Sharing over Vehicular Networks Based on Multi-Sharding Blockchain;https://dl.acm.org/doi/10.1145/3579035, just Accepted.

[69] Kong X, Zeng P, Li C. PPFP: An Efficient Privacy-Preserving Fair Payment Protocol for V2G Based on Blockchain. In: 2022 IEEE 8th International Conference on Computer and Communications (ICCC);. p. 1308–1313.

[70] Li M, Chen Y, Lal C, Conti M, Alazab M, Hu D. Eunomia: Anonymous and Secure Vehicular Digital Forensics Based on Blockchain;20(1):225–241. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85120542083&doi=10.1109%2fTDSC.2021.3130583&partnerID=40&md5=9298a87f2289c06a67bda351dea5b274, publisher: Institute of Electrical and Electronics Engineers Inc.

[71] Mansor H, Markantonakis K, Akram RN, Mayes K, Gurulian I. Log Your Car: The Non-invasive Vehicle Forensics. In: 2016 IEEE Trustcom/BigDataSE/ISPA;. p. 974–982. ISSN: 2324-9013.

[72] Feng X, Dawam ES, Amin S. A New Digital Forensics Model of Smart City Automated Vehicles. In: 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData);. p. 274–279.

[73] Cebe M, Erdin E, Akkaya K, Aksu H, Uluagac S. Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles;56(10):50–57. Conference Name: IEEE Communications Magazine.

[74] Li M, Weng J, Liu JN, Lin X, Obimbo C. Toward Vehicular Digital Forensics From Decentralized Trust: An Accountable, Privacy-Preserving, and Secure Realization;9(9):7009–7024. Conference Name: IEEE Internet of Things Journal.

[75] Mani A, Goldberg I. ZXAD: High-volume Attack Mitigation for Tor. In: Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society WPES '21, Association for Computing Machinery;. p. 1–16. https://dl.acm.org/doi/10.1145/3463676.3485609.

[76] Wan Z, Zhang T, Liu W, Wang M, Zhu L. Decentralized Privacy-Preserving Fair Exchange Scheme for V2G Based on Blockchain;19(4):2442–2456. https://www.webofscience.com/wos/woscc/summary/052c1a81-5308-4536-ae9a-494037700028-7e0eaa1c/relevance/1, place: Los Alamitos Publisher: Ieee Computer Soc WOS:000822381200001.

[77] Wang T, Shen H, Chen J, Chen F, Wu Q, Xie D. A hybrid blockchain-based identity authentication scheme for Mobile Crowd Sensing;143:40–50. https://www.sciencedirect.com/science/article/pii/S0167739X23000201.

[78] Cui Z, Xue F, Zhang S, Cai X, Cao Y, Zhang W, et al. A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN;13(2):241–251.

[79] Gabay D, Akkaya K, Cebe M. Privacy-Preserving Authentication Scheme for Connected Electric Vehicles Using Blockchain and Zero Knowledge Proofs;69(6):5760–5772. Conference Name: IEEE Transactions on Vehicular Technology.

[80] Ren Y, Li X, Sun SF, Yuan X, Zhang X. Privacy-preserving batch verification signature scheme based on blockchain for Vehicular Ad-Hoc Networks;58:102698. https://www.sciencedirect.com/science/article/pii/S2214212620308450.

[81] Jenefa J, Anita EAM. Identity-based message authentication scheme using proxy vehicles for vehicular ad hoc networks;27(5):3093–3108. https://doi.org/10.1007/s11276-021-02655-6.

[82] Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science;. p. 124–134.

[83] Aono Y, Liu S, Tanaka T, Uno S, Van Meter R, Shinohara N, et al. The Present and Future of Discrete Logarithm Problems on Noisy Quantum Computers;3:1–21. http://arxiv.org/abs/2111.06102.

[84] Panait AE, Olimid RF. On Using zk-SNARKs and zk-STARKs in Blockchain-Based Identity Management. In: Maimut D, Oprina AG, Sauveron D, editors. Innovative Security Solutions for Information Technology and Communications Lecture Notes in Computer Science, Springer International Publishing;. p. 130–145.

[85] Rottoo SK. A survey of zero-knowledge techniques and their applications;http://hdl.handle.net/1993/17404.

[86] Li F, McMillin B. Chapter Two - A Survey on Zero-Knowledge Proofs. In: Hurson A, editor. Advances in Computers, vol. 94 Elsevier;.p. 25–69. https://www.sciencedirect.com/science/article/pii/B9780128001615000025.

[87] Chen Z, Jiang Y, Song X, Chen L. A Survey on Zero-Knowledge Authentication for Internet of Things;12(5):1145. https://www.mdpi.com/2079-9292/12/5/1145, number: 5 Publisher: Multidisciplinary Digital Publishing Institute.

[88] Gowravaram NR. Zero Knowledge Proofs and Applications to Financial Regulation;https://dash.harvard.edu/handle/1/38811528, accepted: 2019-03-26T11:07:42Z.

[89] Kurmi J, Sodhi A. A Survey of Zero-Knowledge Proof for Authentication;5.

[90] Pathak A, Patil T, Pawar S, Raut P, Khairnar S. Secure Authentication using Zero Knowledge Proof. In: 2021 Asian Conference on Innovation in Technology (ASIANCON);. p. 1–8.

[91] Cerulli A, Efficient Zero-Knowledge Proofs and their Applications;. https://discovery.ucl.ac.uk/id/eprint/10073525/, conference Name: UCL (University College London) Meeting Name: UCL (University College London) Pages: 1-1 Publication Title: Doctoral thesis, UCL (University College London).

[92] Herbowo KN, Comparing Zero-Knowledge Proof Protocols for Practical Open Source Self-Sovereign Identity Systems;. https://essay.utwente.nl/89761/, publisher: University of Twente.

[93] Herskind L, Katsikouli P, Dragoni N. Privacy and Cryptocurrencies—A Systematic Literature Review;8:54044–54059. Conference Name: IEEE Access.

[94] Chen T, Lu A, Kunpittaya J, Luo A. A Review of Zero Knowledge Proofs;.

[95] Morais E, Koens T, van Wijk C, Koren A, A Survey on Zero Knowledge Range Proofs and Applications. arXiv;. http://arxiv.org/abs/1907.06381.

[96] Sun X, Yu FR, Zhang P, Sun Z, Xie W, Peng X. A Survey on Zero-Knowledge Proof in Blockchain;35(4):198–205. Conference Name: IEEE Network.

[97] Partala J, Nguyen TH, Pirttikangas S. Non-Interactive Zero-Knowledge for Blockchain: A Survey;8:227945–227961. Conference Name: IEEE Access.

[98] Gong Y, Jin Y, Li Y, Liu Z, Zhu Z. Analysis and comparison of the main zero-knowledge proof scheme. In: 2022 International Conference on Big Data, Information and Computer Network (BDICN);. p. 366–372.

[99] Sánchez Ortiz E, Zero-Knowledge Proofs applied to finance;. https://essay.utwente.nl/83802/, publisher: University of Twente.

[100] Khandekar PAS Aayush P. Literature review on zero-knowledge proof and its applications. In: AI-Based Metaheuristics for Information Security and Digital Media Chapman and Hall/CRC;.Num Pages: 8.

[101] Computer Security Division ITL, Post-Quantum Cryptography | CSRC | CSRC;. https://csrc.nist.gov/projects/post-quantum-cryptography.

[102] NIST Asks Public to Help Future-Proof Electronic Information;https://www.nist.gov/news-events/news/2016/12/nist-asks-public-help-future-proof-electronic-information, last Modified: 2018-01-08T16:08-05:00.

[103] Ben-Sasson E, Bentov I, Horesh Y, Riabzev M, Scalable, transparent, and post-quantum secure computational integrity;. https://eprint.iacr.org/2018/046, report Number: 046.

6 | APPENDIX

TABLE 9 Excluded research literature

Title	DOI	Reason
A Privacy-Preserving Payment Model for EV Charging	10.1007/978-3-030-89432-0_21	No protocol usage
AMVchain: authority management mechanism on blockchain-based voting systems	10.1007/s12083-021-01100-x	No protocol usage
An Efficient Group Signature Based Digital Currency System	10.1007/978-981-15-2767-8_34	No protocol usage
An efficient identity tracing scheme for blockchain-based systems	10.1016/j.ins.2021.01.081	No protocol usage
An organization-friendly blockchain system	10.1016/j.cose.2019.101598	No protocol usage
Anonymous Traceability protocol based on Group Signature for Blockchain	10.1016/j.future.2021.09.020	No protocol usage
Blockchain based privacy-preserving software updates with proof-of-delivery for Internet of Things	10.1016/j.jpdc.2019.06.001	No protocol usage
Blockchain-Based Self-Sovereign Identity System with Attribute-Based Issuance	10.1007/978-3-031-21280-2_2	No protocol usage
Casper: a blockchain-based system for efficient and secure customer credential verification	10.1007/s42786-021-00036-3	No protocol usage
Computing Neural Networks with Homomorphic Encryption and Verifiable Computing	10.1007/978-3-030-61638-0_17	No protocol usage
Decentralized Access Control Encryption in Public Blockchain	10.1007/978-981-15-2777-7_20	No protocol usage
Decentralized Privacy-Preserving Netting Protocol on Blockchain for Payment Systems	10.1007/978-3-030-51280-4_9	No protocol usage
DECOUPLES: a decentralized, unlinkable and privacy-preserving traceability system for the supply chain	10.1145/3297280.3297318	No protocol usage
DEPLEST: A blockchain-based privacy-preserving distributed database toward user behaviors in social networks	10.1016/j.ins.2019.05.092	No protocol usage

Dynamic pricing in industrial internet of things: Blockchain application for energy management in smart cities	10.1016/j.jisa.2020.102615	No protocol usage
Efficient Novel Privacy Preserving PoS Protocol Proof-of-concept with Algorand	10.1145/3475992.3475999	No protocol usage
EIFFeL: Ensuring Integrity for Federated Learning	10.1145/3548606.3560611	No protocol usage
ElearnChain: A privacy-preserving consortium blockchain system for e-learning educational records	10.1016/j.jisa.2021.103013	No protocol usage
emmy - Trust-Enhancing Authentication Library	10.1007/978-3-030-33716-2_11	No protocol usage
FAST: Fair Auctions via Secret Transactions	10.1007/978-3-031-09234-3_36	No protocol usage
hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design	10.1016/j.ipm.2021.102535	No protocol usage
HyperNet: A conditional k-anonymous and censorship resistant decentralized hypermedia architecture	10.1016/j.eswa.2022.118079	No protocol usage
Kicking-the-Bucket: Fast Privacy-Preserving Trading Using Buckets	10.1007/978-3-031-18283-9_2	No protocol usage
KPH: A Novel Blockchain Privacy Preserving Scheme Based on Paillier and FO Commitment	10.1007/978-981-19-5209-8_7	No protocol usage
Lattice-Based Zero-Knowledge Proofs: New Techniques for Shorter and Faster Constructions and Applications	10.1007/978-3-030-26948-7_5	No protocol usage
Lockmix: a secure and privacy-preserving mix service for Bitcoin anonymity	10.1007/s10207-019-00459-6	No protocol usage
MiniLedger: Compact-Sized Anonymous and Auditable Distributed Payments	10.1007/978-3-030-88418-5_20	No protocol usage
NECTAR: non-interactive smart contract protocol using blockchain technology	10.1145/3194113.3194116	No protocol usage
Nummatus: A Privacy Preserving Proof of Reserves Protocol for Quisquis	10.1007/978-3-030-35423-7_10	No protocol usage

Oblivious Message Retrieval	10.1007/978-3-031-15802-5_26	No protocol usage
PAChain: Private, authenticated & auditable consortium blockchain and its implementation	10.1016/j.future.2020.05.011	No protocol usage
PAChain: Private, Authenticated and Auditable Consortium Blockchain	10.1007/978-3-030-31578-8_12	No protocol usage
PASTRAMI: Privacy-preserving, Auditable, Scalable & Trustworthy Auctions for Multiple Items	10.1145/3423211.3425669	No protocol usage
PPCA: privacy-preserving conditional actions for IoT environments using smart contracts	10.1145/3360774.3360794	No protocol usage
Privacy and information sharing in a judicial setting: a wicked problem	10.1145/2757401.2757425	No protocol usage
Privacy Preserving Biometric Authentication on the blockchain for smart healthcare	10.1016/j.pmcj.2022.101683	No protocol usage
Privacy-Enhancing Decentralized Anonymous Credential in Smart Grids	10.1016/j.csi.2020.103505	No protocol usage
Privacy-preserving energy storage sharing with blockchain and secure multi-party computation	10.1145/3508467.3508471	No protocol usage
Privacy-Preserving Incentive Systems with Highly Efficient Point-Collection	10.1145/3320269.3384769	No protocol usage
Private and Trustworthy Distributed Lending Model Using Hyperledger Besu	10.1007/s42979-021-00500-3	No protocol usage
QHSE: An efficient privacy-preserving scheme for blockchain-based transactions	10.1016/j.future.2020.06.025	No protocol usage
Quantifying location privacy in permissioned blockchain-based internet of things (IoT)	10.1145/3360774.3360800	No protocol usage
Random-Value Payment Tokens for On-Chain Privacy-Preserving Payments	10.1007/978-3-031-17834-4_13	No protocol usage

SecTEP: Enabling secure tender evaluation with sealed prices and quality evaluation in procurement bidding systems over blockchain	10.1016/j.cose.2021.102188	No protocol usage
Simple and scalable blockchain with privacy	10.1016/j.jisa.2020.102700	No protocol usage
Sunspot: A Decentralized Framework Enabling Privacy for Authorizable Data Sharing on Transparent Public Blockchains	10.1007/978-3-030-95384-3_43	No protocol usage
Towards a privacy-preserving smart contract-based data aggregation and quality-driven incentive mechanism for mobile crowdsensing	10.1016/j.jnca.2022.103483	No protocol usage
TPPSUPPLY : A traceable and privacy-preserving blockchain system architecture for the supply chain	10.1016/j.jisa.2022.103116	No protocol usage
VERICONDOR: End-to-End Verifiable Condorcet Voting without Tallying Authorities	10.1145/3488932.3497758	No protocol usage
Verifiable Computation in Multiparty Protocols with Honest Majority	10.1007/978-3-319-12475-9_11	No protocol usage
Vulnerability market as a public-good auction with privacy preservation	10.1016/j.cose.2020.101807	No protocol usage
ZeroLender: Trustless Peer-to-Peer Bitcoin Lending Platform	10.1145/3374664.3375735	No protocol usage
zksk: A Library for Composable Zero-Knowledge Proofs	10.1145/3338498.3358653	No protocol usage
A Group Signature Based Digital Currency System	10.1007/978-981-15-2777-7_1	Indirect protocol usage
A Privacy-Preserving Framework for Endorsement Process in Hyperledger Fabric	10.1016/j.cose.2022.102637	Indirect protocol usage
An E-Voting System Based on Tornado Cash	10.1007/978-3-031-25467-3_8	Indirect protocol usage
Succinct Attribute-Based Signatures for Bounded-Size Circuits by Combining Algebraic and Arithmetic Proofs	10.1007/978-3-031-14791-3_31	Indirect protocol usage
Zero-Knowledge Proofs for Set Membership: Efficient, Succinct, Modular	10.1007/978-3-662-64322-8_19	Indirect protocol usage

RingCT 3.0 for Blockchain Confidential Transaction: Shorter Size and Stronger Security	10.1007/978-3-030-51280-4_25	Optional protocol usage
Zero-Knowledge for Homomorphic Key-Value Commitments with Applications to Privacy-Preserving Ledgers	10.1007/978-3-031-14791-3_33	Optional protocol usage
Accountable Privacy for Decentralized Anonymous Payments	10.1007/978-3-662-54970-4_5	Indirect protocol usage, adapts zk-SNARKs for their application
An access control model for the Internet of Things based on zero-knowledge token and blockchain	10.1186/s13638-021-01986-4	Privacy preservation not a (direct) main goal, describes improving IoT access control using Blockchain
Blockchain-Based Confidential Payment System with Controllable Regulation	10.1007/978-3-031-21280-2_3	No detailed usage, only evaluation mentions Bulletproofs
Circuitree: A Datalog Reasoner in Zero-Knowledge	10.1109/ACCESS.2022.3153366	Application to more easily write zk-proofs, not use them
DBS: Blockchain-Based Privacy-Preserving RBAC in IoT	10.1007/978-3-030-91424-0_6	No detailed usage
Designing a blockchain-enabled privacy-preserving energy theft detection system for smart grid neighborhood area network	10.1016/j.epsr.2022.107884	No detailed usage
Efficient Verifiable Image Redacting based on zk-SNARKs	10.1145/3433210.3453110	Indirect protocol usage, uses CP- and CC-SNARK
Efficient Zero-Knowledge Proofs on Signed Data with Applications to Verifiable Computation on Data Streams	10.1145/3548606.3560630	Indirect protocol usage, uses CP-SNARK
Non-Interactive Zero-Knowledge Proofs for Composite Statements	10.1007/978-3-319-96878-0_22	Indirect protocol usage, proposes a new protocol
Offline Authentication Scheme based on Blockchain Technology for Smart Lock	10.1145/3291842.3291893	No detailed usage, just mentions zk-SNARK can be used
On Using zk-SNARKs and zk-STARKs in Blockchain-Based Identity Management	10.1007/978-3-030-69255-1_9	No proposed application, compares zk-SNARK and zk-STARK
Privacy-Preserving Analytics for Data Markets Using MPC	10.1007/978-3-030-72465-8_13	No detailed usage

Provisions: Privacy-preserving Proofs of Solvency for Bitcoin Exchanges	10.1145/2810103.2813674	No protocol usage, uses sigma-protocols. Full version uses zk-SNARK, but no detailed usage
Public Verifiable Private Decision Tree Prediction	10.1007/978-3-030-71852-7_16	Indirect protocol usage, proposes a new NIZKP
RZee: Cryptographic and statistical model for adversary detection and filtration to preserve blockchain privacy	10.1016/j.jksuci.2022.07.007	Indirect protocol usage, proposes improvements on zk-SNARK
Zapper: Smart Contracts with Data and Identity Privacy	10.1145/3548606.3560622	Indirect protocol usage, uses SE-SNARK
ZeroCross: A sidechain-based privacy-preserving Cross-chain solution for Monero	10.1016/j.jpdc.2022.07.008	Indirect protocol usage, uses CP-SNARK
ZeroMT: Multi-transfer Protocol for Enabling Privacy in Off-Chain Payments	10.1007/978-3-030-99587-4_52	No detailed usage
Zether: Towards Privacy in a Smart Contract World	10.1007/978-3-030-51280-4_23	Indirect protocol usage, proposes new protocol based on sigma-protocols and Bulletproofs
Zk-AuthFeed: How to feed authenticated data into smart contract with zero knowledge	10.1109/Blockchain.2019.00020	Indirect protocol usage, uses zk-DASNARK
zkCNN: Zero Knowledge Proofs for Convolutional Neural Network Predictions and Accuracy	10.1145/3460120.3485379	Indirect protocol usage, uses CP-SNARK
ZkrpChain: Privacy-preserving data auditing for consortium blockchains based on zero-knowledge range proofs	10.1109/TrustCom50675.2020.00092	Less complete version of included full paper "zkrpChain: Towards multi-party privacy-preserving data auditing for consortium blockchains based on zero-knowledge range proofs"
ZPiE: Zero-Knowledge Proofs in Embedded Systems	10.3390/math9202569	Privacy preservation not a (direct) main goal, shows usage in low-power IoT

TABLE 10 Extra zk-STARK literature search; Found and excluded research literature

Title	DOI	Reason
A regulated anonymous cryptocurrency with batch linkability	10.1016/j.csi.2023.103770	No protocol usage for a privacy-preserving application
A Review of Privacy-Preserving Cryptographic Techniques Used in Blockchain Platforms	10.1007/978-3-031-29857-8_23	No protocol usage
BV-ICVs: A privacy-preserving and verifiable federated learning framework for V2X environments using blockchain and zkSNARKs	10.1016/j.jksuci.2023.03.020	No protocol usage, used zk-SNARKs but we only looked for zk-STARK in this extra search
Privacy-Preserving Post-quantum Credentials for Digital Payments	10.1007/978-3-031-32415-4_10	No protocol usage, only compares to zk-STARK
Queer In AI: A Case Study in Community-Led Participatory AI	10.1145/3593013.3594134	No protocol usage
Towards verifiable and privacy-preserving account model on a consortium blockchain based on zk-SNARKs	10.1007/s12083-023-01497-7	No protocol usage, used zk-SNARKs but we only looked for zk-STARK in this extra search